Jihočeská univerzita v Českých Budějovicích
Přírodovědecká Fakulta

Bezpečnost OTP zasílaného formou SMS, autentizačního a autorizačního nástroje a nebezpečí zneužití služeb elektronického bankovnictví ovládnutím počítače a chytrého telefonu klienta

Bakalářská práce

Holub Petr

Školitel: Jan Doubek, MBA

České Budějovice 2017

Bibliografické údaje

Holub, P., 2017: Bezpečnost OTP zasílaného formou SMS, autentizačního a autorizačního nástroje a nebezpečí zneužití služeb elektronického bankovnictví ovládnutím počítače a chytrého telefonu klienta. [Safety OTP consigned via SMS, authentication and authorization tool and the danger of misuse of electronic banking services mastering computer and smartphone of client. Bc. Thesis, in Czech.] - 74p, Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Abstrakt

Tato bakalářská práce se zabývá bezpečností autentizačního a autorizačního nástroje OTP, který je zasílán SMS zprávami při potvrzování platebních příkazů prováděných prostřednictvím služeb internetového bankovnictví. Práce se zabývá metodologií útoku využívající škodlivý kód k získání přístupu k bankovnímu účtu napadaného klienta a posouzením bezpečnosti aktuálně používaného nástroje OTP jako metody dvoufaktorové autentizace.

Abstract

This bachelor thesis deals with the safety authentication and authorization tool OTP which is sent by SMS when confirm payment orders make through internet banking services. The work deals with the methodology of attack using malicious code to gain access to a bank account client fallen and safety assessment tool currently used by OTP as a method for two-factor authentication.

Klíčová slova

Internetové bankovnictví, bankovní malware, chytrý telefon, OTP, SMS.

Key words

Internet banking, banking malware, smartphone, OTP, SMS.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne……

Podpis: ……

Holub Petr

Poděkování

Tímto bych rád poděkoval školiteli mé bakalářské práce Janu Doubkovi, MBA za pomoc a podnětné připomínky při zpracovávání.

Dále chci poděkovat Ing. Luďku Raškovi za užitečné postřehy v oblasti OTP mechanismů a biometrické identifikace.

Jako poslední chci poděkovat své rodině a přátelům za podporu a pochopení během studií.

Obsah

1. Úvod

Rozvoj informačních a komunikačních technologií umožnil lidem usnadnit práci v mnoha aspektech jejich života. S počítači se v dnešní době mohou lidé setkat při mnoha životních situacích. Přes jejich využívání v práci až po zábavu ve volném čase. Bylo tedy jen otázkou času, kdy se tento trend začne rozšiřovat i do oblasti bankovnictví. Elektronické, zvláště pak internetové bankovnictví usnadnilo lidem v mnoha ohledech život. Možnost platit při nákupu platební kartou či provádět platební příkazy bez nutnosti navštívit banku během několika minut z pohodlí domova jsou toho příkladem. Co ovšem pro jednoho znamená ulehčení běžných povinností, představuje pro druhého způsob jak připravit majitele účtu, kteří využívají služeb internetového bankovnictví o peníze. S nástupem chytrých telefonů se začaly objevovat útoky na tato zařízení v podobě trojských koňů a jiného škodlivého kódu, které mají za úkol získat citlivá data jejich majitelů. Včetně dat a přístupových údajů týkajících se internetového bankovnictví.

Tématem této práce je přiblížit způsob, jakým se kyberzločinci snaží o získání finančních prostředků klientů bank za pomoci ovládnutí jejich počítače a chytrého telefonu. Zároveň se pozastavuje nad bezpečností autorizačního nástroje OTP, jenž je využíván jako prostředek dvoufaktorové autentizace během provádění platebních transakcí prostřednictvím internetového bankovnictví. OTP byl jako prostředek autentizace dlouhou dobu považován za bezpečnou metodu, jak potvrzovat transakce prováděné přes internet. Stále větší množství vyskytujících se útoků cílených na uživatele chytrých telefonů, jejichž bankovní odnož je popsána v této práci, dokládá skutečnost, že je tento způsob autorizace již nedostačující. Z tohoto důvodu je také hledána vhodná náhrada. Alternativy, jimiž lze tento autentizační a autorizační nástroj nahradit, z nichž některé jsou v reálném světě již používány, práce rovněž přibližuje.

2. Cíle a metodika práce

2.1. Cíle práce

Jedním z cílů práce je definování pojmů elektronického bankovnictví a zaměření na oblast zabezpečení internetového bankovnictví velkých bank v ČR a to při používání autentizačního a autorizačního nástroje OTP zasílaném prostřednictvím SMS.

Druhým bodem je provedení rozboru módu operandi útoku na služby internetového bankovnictví, s cílem infikovat počítač a chytrý telefon škodlivým kódem. Zjištění, jak útok probíhá, jaké jsou jeho následky a jak se lze proti tomuto typu útoku bránit.

Posledním bodem je poukázání na silné a slabé stránky používaného autentizačního a autorizačního nástroje OTP zasílaném prostřednictvím SMS a to zejména v případě, kdy klient používá chytrý telefon.

2.2. Metodika práce

Obsahově je práce rozdělena do tří částí. V první části je definován pojem přímé bankovnictví, jaké existují formy přímého bankovnictví a co umožňují. Podrobněji bude rozebrána forma internetového bankovnictví.

Druhá část se zabývá metodologií útoku proti službám internetového bankovnictví, pomocí nichž se útočníci snaží oklamat klienty bank a získat tak jejich přihlašovací údaje. V této části jsou kromě metodologie útoku uvedeny také informace a doporučení, kterými je možno se zcizení přihlašovacích údajů vyvarovat.

V poslední části je zhodnocena bezpečnost autentizačního nástroje OTP, jenž je používán jako nástroj dvoufaktorové autentizace k potvrzování transakcí prováděných právě za pomoci služeb internetového bankovnictví. Dále jsou uvedeny možnosti, jakými lze tento, z dnešního pohledu již zastaralý, způsob autorizace online platebních transakcí nahradit.

3. Přímé bankovnictví

3.1. Co znamená pojem přímé bankovnictví?

Pro definování pojmu přímého bankovnictví je nejdříve nutné říci, co určuje slovo bankovnictví samo o sobě. Pro tuto definici je nejprve potřeba vysvětlit pojem banka, který s bankovnictvím souvisí. Banka je instituce, jež poskytuje účastníkům trhu služby spojené s peněžním kapitálem. Bankovnictví je pak definováno jako souhrn peněžních služeb, které banky poskytují. Tyto peněžní služby jsou tvořeny službami spojovanými nejen s hotovostními a bezhotovostními transakcemi, ale i úvěrovými či spořicími službami. Mezi ně rovněž patří platební styk. Platební styk představuje peněžní vztah mezi plátcem a příjemcem, který je prováděn za pomoci k tomu určených prostředků. Zjednodušeně lze říci, že plátce zaplatí za službu, kterou pro něho příjemce vykoná.

S rozvojem informačních a komunikačních technologií, začalo vznikat odvětví označované jako přímé bankovnictví, které zprostředkovává vybrané peněžní služby a další komunikaci s bankou, popřípadě jinou bankovní institucí bez nutnosti fyzické návštěvy pobočky nebo kanceláře.[1] Toho je docíleno za pomoci technických prostředků, které mohou být užity téměř odkudkoliv a kdykoliv. Může se jednat například o mobilní telefon nebo přístroj komunikující za pomoci připojení k internetu.

Přímé bankovnictví je nejčastěji používáno pro služby, které zahrnují mimo jiné zjištění stavu na účtu klienta, získání informací o provedených a přijatých platbách na účtu, nebo možnosti zřízení jednorázového či trvalého příkazu k úhradě. Přímé, nebo někdy nazývané též elektronické bankovnictví, vzniklo hlavně z důvodu jednoduššího a pohodlnějšího využívání těchto služeb.

[1] PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy*. 1. Praha: Computer Press, 2000, 166 s. ISBN 80-7226-328-5, s.1

3.2. Formy přímého bankovnictví

Využívání služeb přímého bankovnictví je možno za pomoci některé z existujících možností. Klient může komunikovat s bankou s využitím následujících možností. Jednou z těchto možností je osobní návštěva pobočky banky. Tato možnost vyžaduje čas klienta a je výrazně ovlivněna provozní dobou, po kterou je možno ji navštívit. Jedna z možností, kdy klient již není omezován úředními hodinami, a která z technologického hlediska vznikla jako první je možnost využívat nástroj známý jako platební karta. Platební karta je nástroj, který umožňuje jejímu držiteli provádět platby či čerpat prostředky z účtu, ke kterému karta náleží. Poslední dva okruhy, ze kterých si klient může vybrat, jsou telefonní bankovnictví nebo produkt využívající ke komunikaci s bankou počítač. Tuto možnost lze nazvat zjednodušeným způsobem počítačové bankovnictví. Jak u komunikace za pomoci telefonu, tak komunikace s využitím počítače si lze zvolit z několika variant.

3.2.1. Platební karty

Platební karta je nástroj, který poskytují finanční instituce svým klientům k účtu, který vlastní. Jedná se o nástroj, který umožňuje placení za zboží a služby a výběru hotovosti z bankomatů, popřípadě v rámci služby Cash Back, jenž umožňuje vyplácení hotovosti na pokladně při platbě platební kartou.[2] Transakce pomocí platební karty musí být potvrzena ověřovacím kódem, který se označuje zkratkou PIN. V originálním znění Personal Identification Number, v překladu osobní identifikační číslo. Hlavní výhodou platebních karet je možnost bezhotovostní platby, přičemž plátce ani příjemce při platbě nemusí mít v držení velké finanční obnosy. Nevýhodou je naopak riziko krádeže karty. Pokud dojde ke krádeži je nutno ji neprodleně po jejím zjištění nahlásit, aby došlo k zablokování karty. Z tohoto důvodu se nedoporučuje v blízkosti karty uchovávat PIN kód.

[2] KreditKarta.cz. *Cashback* [online]. [cit. 2016-10-06]. Dostupné z: http://www.kreditkarta.cz/Cashback/

U platebních karet se často zaměňují pojmy debetní a kreditní karta. Zatímco pomocí debetní karty klient čerpá finanční prostředky ze svého účtu, u kreditní karty se prostředky čerpají z úvěrového účtu, který musí držitel karty následné splácet.[3]

Mezi nejznámější vydavatele platebních karet patří karetní asociace VISA nebo MasterCard.

3.2.2. Telefonní bankovnictví

Telefonní bankovnictví, které je v anglickém jazyce označované jako phonebanking či telebanking, pro komunikaci s bankou vyžaduje telefonní přístroj. Při vzniku této formy komunikace mohl klient komunikovat s telefonním bankéřem, což je zaměstnanec banky, nebo s automatickým telefonním systémem.[4] Klient se v tomto případě identifikuje svým identifikačním číslem a heslem.

S příchodem mobilních telefonů se možnosti telefonního bankovnictví rozšířili a klient mohl využívat pro komunikaci s bankou SMS zprávy či službu SIM Toolkit. Souhrnně se tato forma označuje jako GSM banking. Při využívání SMS zpráv pro komunikaci s bankou je možno využívat všechny typy mobilních telefonů. Je však nutné dodržovat danou strukturu SMS zprávy, aby mohla být požadovaná operace správně vyhodnocena a provedena.[5] Pro využívání SIM Toolkit musí klientův mobilní telefon i SIM karta podporovat technologii SIM Toolkit. Tuto službu je nutné aktivovat osobní návštěvou na pobočce banky. Do klientova mobilního telefonu je nahrána příslušná aplikace, která se následně zobrazí v menu telefonu. Přístup k aplikaci je chráněn pomocí bankovního PINu označovaným jako BPIN.[6]

Další rozvoj telefonního bankovnictví, díky kterému se dřívější formy telefonního bankovnictví dostávají do pozadí, nastal s rozvojem tzv. chytrých telefonů. V souvislosti s nimi se začal objevovat pojem smartbanking. Smartbanking umožňuje klientovi banky

---

[3] MATYÁŠ, Vašek. *Autentizace uživatelů a autorizace elektronických transakcí: příručka manažera = User authentication and electronic transaction authorization : manager's handbook*. Praha: Tate International, 2007. 318 s. Příručka manažera; 8. ISBN 978-80-86813-14-1., s. 115

[4] PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy*. 1. Praha: Computer Press, 2000, 166 s. ISBN 80-7226-328-5, s. 41

[5] Tamtéž, s. 54

[6] Tamtéž, s. 57

přistupovat ke svému účtu prostřednictvím aplikace nahrané v chytrém telefonu, či tabletu komunikující za pomoci mobilního internetového připojení. Smartbanking je v dnešní době dostupný nejen pro mobilní zařízení s operačním systémem iOS nebo Android, ale i pro ty s operačním systémem Windows Phone nebo Windows 8 a vyšší.

3.2.3. Počítačové bankovnictví

Počítačové bankovnictví je odvětví přímého bankovnictví, kdy klient pro komunikaci s bankou a účtem využívá počítač. Počítačové bankovnictví se v tomto ohledu dělí na dva směry, tzv. homebanking a internetbanking.

Pokud klient využívá služeb homebankingu, obdrží speciální software, pomocí kterého může za pomoci internetu využívat služby jako zjištění zůstatku na účtu, zřizování příkazů k úhradě, zadávání trvalých příkazů nebo konverzi měn. Nevýhodou homebankingu je jeho omezení pouze na jeden konkrétní počítač. Pokud je tedy software instalován na jeden stroj, nemůže být využíván na dalších počítačích. Výhodou je ovšem skutečnost, že produkty na bázi homebankingu jsou kompatibilní s účetními programy.[7] Informace o platbách je tedy možno přímo načíst do účetního softwaru, který klient využívá. Rovněž příprava příkazu k úhradě je zjednodušena možností transformovat data z účetního softwaru do datového souboru zasílaného bance ke zpracování. Z tohoto hlediska je zřejmé, že homebanking je orientovaný spíše pro firemní klienty bank. To ovšem neznamená, že není dostupný i běžným klientům.

Druhým směrem počítačového bankovnictví je internetbanking. Tato služba umožňuje zákazníkům komunikaci s bankou odkudkoliv, kde je dostupné připojení na internet. Na rozdíl od homebankingu zde není uživatel nijak omezen konkrétním počítačem, na kterém by byl instalovaný speciální software. Lze tedy využít libovolný počítač. Pro využívání služeb stačí pouze internetový prohlížeč, pomocí kterého klient zadá webovou adresu své banky a pomocí identifikačních údajů se přihlásí do systému. Po přihlášení do systému pak může provádět již výše zmíněné operace. Například zadávání příkazů k úhradě či prohlédnutí historie obratů na účtu.

[7] Tamtéž, s. 61

S rozvojem chytrých telefonů a tabletů již není počítačové bankovnictví, hlavně internetbanking, limitován pouze na počítače a notebooky

3.3. Vlastnosti přímého bankovnictví

Mezi hlavní výhody využívání přímého bankovnictví patří možnost manipulace s peněžními prostředky na účtu klienta a provádění operací bez nutnosti osobní návštěvy banky. Tato výhoda je oceňována nejen jednotlivými klienty bank, ale i společnostmi, které díky využívání služeb přímého bankovnictví mohou provádět či ověřovat přijaté platby přímo na svém pracovišti popřípadě z domova, což jednoznačně šetří mnoho času oproti osobní návštěvě, která je navíc limitována úřední dobou, po kterou je pobočka banky otevřena. Tento fakt je zároveň jedním z důvodů vzniku přímého bankovnictví, který měl a stále má, velký vliv na jeho vývoj. V dnešní době, pokud banky nenabízejí služby přímého bankovnictví, nemají šanci se prosadit na trhu. Přímé bankovnictví je výhodné i pro banky samotné. Snižuje se zátěž pracovníků a rovněž není nutné vynakládat takové zdroje na provoz jednotlivých poboček, čímž se snižují náklady.

K využívání služeb přímého bankovnictví je nutné, aby byl klient informován, že takovéto služby má možnost využívat. Pokud si klient zvolí využívání některé z nabízených forem přímého bankovnictví, dojde k sepsání smlouvy mezi klientem a bankou. Rovněž je potřeba vlastnit určité technické prostředky. Tyto prostředky se liší dle toho, jakou formu přímého bankovnictví klient využívá. Obě strany také musí být seznámeny s bezpečnostními opatřeními, které musejí být dodržovány, aby se zabránilo zneužití a krádeži dat či peněz.

Stejně jako hrozí riziko při klasickém peněžním styku, kdy může být klient či pobočka přepadeny i přímé bankovnictví má svá rizika a nevýhody. Ať už se jedná o ztrátu platební karty, či získání přístupových údajů k nějaké z uvedených forem přímého bankovnictví, riziko zneužití těchto údajů a následné finanční ztráty je vysoké. Jsou zde ovšem i nevýhody související s technologickou stránkou. Kupříkladu internetové bankovnictví je vázané na dostupnosti internetového připojení. Pokud se tedy klient využívající jeho služby nachází v oblasti, kde není připojení dostupné, znamená to pro něho komplikace. Obdobně tak například pokud klient využívá službu smartbanking a jeho chytrému telefonu se vybije baterie. Klienty, kteří využívají přímého bankovnictví, také ohrožuje nebezpečí možnosti organizovaného a cíleného útoku v podobě získání jejich

přístupových údajů pod falešnou záminkou. Právě tyto útoky jsou další motivací pro stálé zlepšování a vyvíjení lepšího zabezpečení služeb přímého bankovnictví.

4. Internetové bankovnictví

4.1. Internetové bankovnictví v České republice

Internetové bankovnictví se v České republice začalo objevovat od druhé poloviny 90. let minulého století.[8] Mezi tehdy nejznámějšími bankami, které začaly tento produkt nabízet, byla například Expandia Banka, nebo Investiční a poštovní banka, známá rovněž jako IPB.

V počátcích přímého bankovnictví v České republice nabízela Expandia Banka, a.s. pro komunikaci mezi klientem a bankou téměř všechny, v té době dostupné formy. Klient mohl komunikovat s bankou prostřednictvím telefonu, technologie GSM nebo za pomoci internetového připojení. Zákazníkům byl nabízen i homebankingový systém pod názvem E-komunikátor. Expandia Banka, v té době již přejmenována na eBanka, a.s., byla v roce 2006 prodána skupině Raiffeisenbank International.

I přes úspěchy a známost Expandia Banky, první kdo spustil službu internetového bankovnictví v České republice, byla v roce 1998 Fio banka, která v té době působila jako družstevní záložna.[9] Ta vznikla rozšířením služeb družstevní záložny z existující společnosti Fio obchodující s cennými papíry. V roce 2010 získala společnost bankovní licenci a od té doby působí pod názvem Fio banka. Další prvenství si tato banka připsala zavedením produktu typu Smartbanking.[10]

K výše zmíněným lze uvést i další banky jako je například Živnostenská banka se systémem NetBank, která nyní působí pod názvem UniCredit Bank ČR. Od roku 2002 služby internetového bankovnictví nabízejí ČSOB a Česká spořitelna.[11] Produkt ČSOB se nazývá ČSOB InternetBanking 24 a Česká spořitelna svůj produkt nabízí pod názvem SERVIS 24 Internetbanking. ČSOB, spolu s Poštovní spořitelnou začaly od roku 2003 jako

---

[8] MEŠEC.CZ. *Počátky internetového bankovnictví.* [online]. [cit. 2016-08-15]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

[9] FIO BANKA. *Historie* [online]. [cit. 2016-08-16]. Dostupné z: https://www.fio.cz/o-nas/fio-banka/historie

[10] Tamtéž.

[11] TŮMOVÁ, Věra. PENÍZE.CZ. *Odkud kam míří český internetbanking* [online]. 2008 [cit. 2016-08-15]. Dostupné z: http://www.penize.cz/prime-bankovnictvi/42614-odkud-kam-miri-cesky-internetbanking

první ve větším množství využívat pro autorizaci platebních operací ověřovací klíče zasílané za pomoci SMS zpráv na mobilní telefony.[12]

V dnešní době nabízejí služby internetového bankovnictví všechny velké banky v České republice.

4.2. Proč využívat služeb internetového bankovnictví

Internetové bankovnictví je jednoduchý a levný způsob jakým mohou klienti banky nakládat s penězi na svých účtech. Nespornou a patrně největší výhodou tohoto produktu přímého bankovnictví je možnost přistupovat ke svému účtu z pohodlí domova, popřípadě z jiného místa, kde je možno připojit se k internetu, 24 hodin denně 7 dní v týdnu a nemuset tak osobně navštěvovat pobočku banky. Pro klienty to znamená velkou úsporu času. Bez ohledu na provozní dobu pobočky lze provádět operace typu zjištění stavu na účtu, zjednání jednorázového či trvalého příkazu k úhradě, nebo provést výpis pohybů na účtu. Díky možnosti výpisů účtu má jeho majitel přehled o všech provedených platbách kdykoliv potřebuje.

Internetové bankovnictví v dnešní době ovšem nepředstavuje pouze možnost ovládání majitelova účtu a zadávání platebních příkazů. Klienti mohou jeho prostřednictvím získat informace o půjčkách, investicích, penzijním spoření či stavu hypotéky. Také je možno pomocí něho nastavovat parametry platebních karet. U internetového bankovnictví Raiffeisenbank je možnost uložení vzorů opakovaných plateb nebo online možnost sjednání půjčky či kreditní karty.[13] Také existuje možnost dobití kreditu u mobilního telefonu. Tuto možnost nabízí InternetBanking 24 banky ČSOB.[14] Z výše uvedeného vyplívá, že možnosti služeb internetového bankovnictví se neustále vyvíjejí a banky tak mohou svým klientům nabízet více možností, ve snaze usnadnit jim v dnešní uspěchané době život, čímž se stává pro klienty přitažlivější.

---

[12] Tamtéž.

[13] RAIFFEISENBANK. *Internetové bankovnictví: Podrobnosti o produktu.*[online]. [cit. 2016-08-15]. Dostupné z: https://www.rb.cz/osobni/ucty-a-bankovnictvi/internetove-bankovnictvi

[14] ČSOB. *InternetBanking 24 Celá banka ve vašem počítači* [online]. [cit. 2016-08-16]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking-24

4.3. Příklady produktů jednotlivých bank

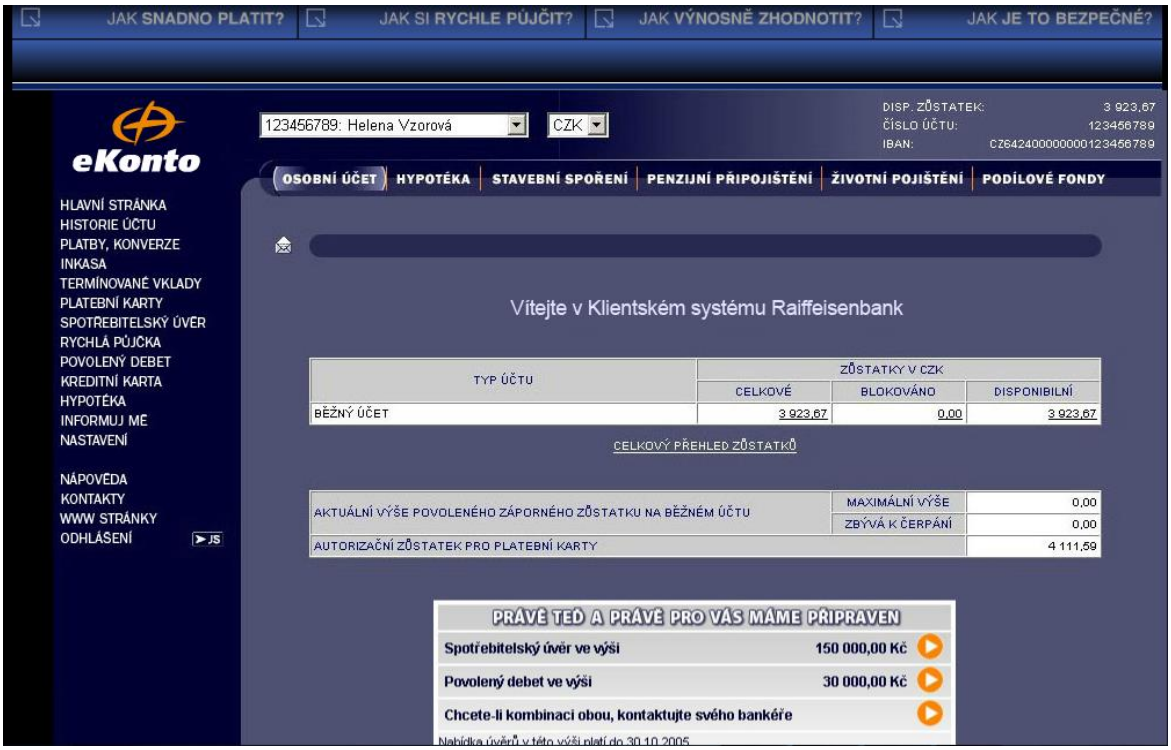
Pro ukázku internetového bankovnictví jsou vybrány produkty Raiffeisenbank a ČSOB, které v České republice patří mezi nejznámější.

4.3.1. Internetové bankovnictví Raiffeisenbank

Raiffeisenbank nabízí službu internetového bankovnictví pod názvem eKonto. Systém internetového bankovnictví Raiffeisenbank je ve skutečnosti převzatým systémem eBanky, která byla roku 2006 odkoupena. Přihlášení je možné z webových stránek banky.

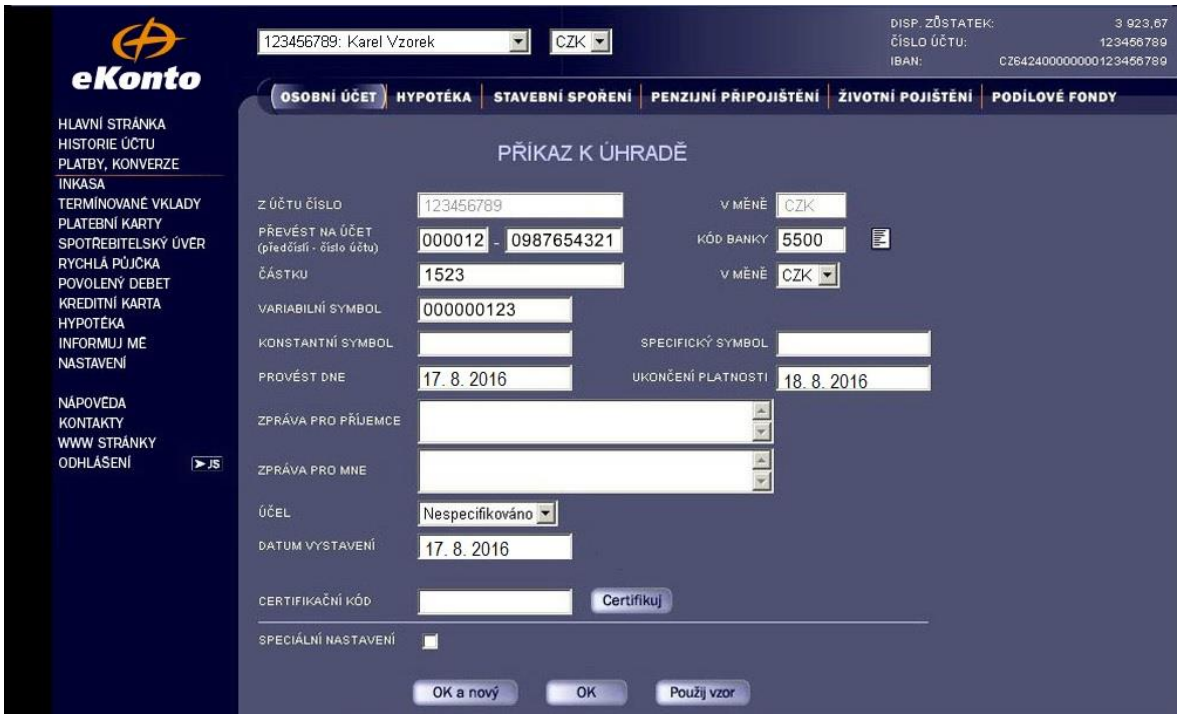
Internetové bankovnictví Raiffeisenbank umožňuje klientovi, kromě řízení svých financí získat historii plateb a výpisy z účtu ve formátu PDF, získat informace o půjčkách, či jejich sjednání online, možnost uložení vzoru opakovaných plateb, či zasílání informací, například o zůstatku pomocí SMS nebo emailové zprávy.

Po přihlášení je klient uvítán v klientském systému banky a ihned má k dispozici informace o svém účtu. Mezi informace o účtu patří, kromě typu klientského účtu, údaje o celkové částce na účtu a disponibilní částce, která informuje, kolik peněz má klient okamžitě k dispozici. Zobrazen je rovněž povolený limit případného přečerpání klientova účtu. Ukázku lze shlédnout na následujícím obrázku.



Obrázek 1: Služba eKonto po přihlášení uživatele. Zdroj: RAIFFEISENBANK. *Podívejte se, jak funguje internetové bankovnictví.* [online]. [cit. 2016-08-17]. Dostupné z: https://www.rb.cz/attachements/demo/

V levé části obrazovky se nachází menu, pomocí kterého si klient volí operace, které chce provést. Jako příklad bude ukázán příkaz k úhradě. V menu je zvolena položka Platby, Konverze a v podnabídce je zvolena Platba. Poté dojde přesunutí na formulář, kde jsou do vstupních polí zadány požadované údaje. Po zadání údajů klient klikne na tlačítko Certifikuj, načež na mobilní telefon přijde SMS zpráva s certifikačním kódem, který je získán po zadání PINu. Kód je opsán do příslušného políčka. Platba je potvrzena tlačítkem OK a na mobilní telefon opět přijde SMS zpráva. Tentokrát o provedené platbě.



Obrázek 2: Formulář pro zadání příkazu k úhradě v systému eKonto s ukázkovými údaji. Zdroj: RAIFFEISENBANK. *Podívejte se, jak funguje internetové bankovnictví.* [online]. [cit. 2016-08-17]. Dostupné z: https://www.rb.cz/attachements/demo/

4.3.2. Internetové bankovnictví ČSOB

ČSOB nabízí svým klientům služby internetového bankovnictví pod názvem ČSOB InternetBanking 24. Služba je nabízena zdarma ke všem účtům. Je dostupná přes odkaz na webových stránkách banky.

Pomocí internetového bankovnictví ČSOB lze upravovat parametry účtu, vystavených karet či úvěru. Klient má rovněž přehled o případných investicích a zřízených hypotékách. Může si i za jeho pomoci dobít kredit mobilního telefonu. Pomocí aplikace pro chytré telefony s názvem ČSOB Smart klíč se lze přihlašovat a potvrzovat jednotlivé platby. Službu InternetBanking 24 lze zřídit spolu se založením účtu, nebo dodatečně na některé z poboček banky.

Pomocí služby internetového bankovnictví ČSOB lze dále nastavit limity pro platební kartu, či zřítit službu 3D Secure pro bezpečné platby přes internet. Platební kartu je také možno pomocí této služby zablokovat, například v případě její ztráty. Klienti mohou využívat služby Info 24, která za pomoci SMS nebo emailu oznámí autorizaci

platby kartou nebo pohyb na účtu. Další služba pod názvem Komfortní vyúčtování umožňuje provádět platby s partnery, se kterými banka spolupracuje.

Pro přihlášení do aplikace může klient volit z několika možností. První možností je zadání identifikačního čísla, PINu a SMS klíče, druhá identifikačním číslem, PINem a Smart klíčem. SMS klíč, popřípadě Smart klíč se zadává po zadání identifikačního čísla a PINu.[15] Poslední možností je certifikát k elektronickému podpisu na čipové kartě.

Obrázek 3: Služba ČSOB InternetBanking 24 po přihlášení uživatele. Zdroj: ČSOB. *InternetBanking 24 Celá banka ve vašem počítači: ČSOB InternetBanking 24 – příručka.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/documents/10710/36574/csob-ib24-prirucka-zkrac.pdf

Po přihlášení je uživateli k dispozici prostředí, kde může provádět jím požadované operace. Nechybí zde samozřejmě informace o majiteli a aktuálním stavu účtu. Bankovní operace jsou pro větší přehlednost rozděleny do jednotlivých záložek. Každá záložka následně obsahuje menu v levé části obrazovky, kde lze vyhledat požadované funkce. Například pro zjištění výpisů účtu, na záložce Účty a transakce se zvolí v menu Informace o účtech a v zobrazené podnabídce položku výpisy. Následně dojde k zobrazení požadované informace.

[15] ČSOB. *InternetBanking 24 Celá banka ve vašem počítači: ČSOB InternetBanking 24 – příručka*. [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/documents/10710/36574/csob-ib24-prirucka-zkrac.pdf

4.4. Bezpečnost internetového bankovnictví

Vzhledem k faktu, že se klient nedostavuje při využívání služeb internetového bankovnictví do banky osobně, musí tyto instituce vynaložit značné úsilí na zajištění jednoznačné identifikace přistupujícího klienta a samozřejmě zabezpečení jeho identifikačních údajů a samotné komunikace, která probíhá šifrovaně. Internetové bankovnictví standardně využívá vícestupňovou ochranu. Banky také pro svou identifikaci využívají certifikáty, které jsou vydávány uznanou certifikační autoritou.

Existují dvě klíčové oblasti bezpečnosti internetového bankovnictví. Jedná se o autentizaci klienta a autorizaci neboli potvrzování transakcí.

4.4.1. Autentizace klienta

Autentizace je proces jednoznačného ověření identity uživatele, který přistupuje do služeb internetového bankovnictví. Autentizace se provádí z důvodu zabránění připuštění do systému neoprávněné osoby. Proces je zásadní pro bezpečnost internetového bankovnictví jako celku. Autentizace je prováděna za pomoci identifikačních údajů, které jsou klientovi předány při zřizování služby internetového bankovnictví. Tyto údaje se skládají z klientského čísla klienta a PINu, popřípadě klientského čísla a hesla.

Autentizace může být provedena i za pomoci podpisového certifikátu. Certifikát může být umístěn v samotném počítači, nebo na přenosném médiu. Možnost autentizace pomocí certifikátu umožňují například ČSOB[16] nebo Komerční banka[17].

4.4.2. Potvrzení transakce

K potvrzování transakcí může klient volit mezi několika alternativami. Nejrozšířenější formou potvrzováním plateb jsou jednorázové ověřovací kódy, které jsou zasílané za pomoci SMS zpráv na klientem určené telefonní číslo. Tyto kódy jsou následně po doručení přepsány do příslušného pole ve formuláři pro uskutečňování plateb.

[16] ČSOB. *InternetBanking 24 Celá banka ve vašem počítači.* [online]. [cit. 2016-08-16]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking-24#zabezpeceni

[17] KOMERČNÍ BANKA. *Certifikáty.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.kb.cz/cs/prime-bankovnictvi/certifikaty/vyzvednuti-a-prodlouzeni-certifikatu/

Za pomoci nastavení maximálního počtu chybných zadání potvrzovacího kódu lze přístup k internetovému bankovnictví zablokovat. Odblokování je možné na pobočce klientovi banky.

Další možností pro autorizaci plateb nabízenou bankami je elektronický podpis. Tato volba zahrnuje čipovou kartu, na které je umístěn certifikát. Nevýhodou tohoto řešení je nutnost disponovat čtečkou čipových karet. Ta může být nabízena za určitý poplatek samotnými bankami.

Mezi nejnovější možnost potvrzování transakcí patří tzv. Smart klíč. Technologie Smart klíče spočívá ve vygenerování klíče přímo v chytrém telefonu klienta za pomoci příslušné aplikace, která dokáže přečíst QR kód. QR kód je jakýsi nástupce běžně používaného čárového kódu. Zjištěná informace je následně přepsána do příslušného pole obdobně jako jednorázový SMS kód. Tato služba vyžaduje zadání PINu. Stejně jako u SMS kódů zde existuje možnost nastavení maximálního počtu chybných zadání, než bude přístup zablokován. Službu Smart klíč nabízí například ČSOB[18] nebo UniCredit Bank[19]. Příslušnou aplikaci je možno získat na Google Play, App Store či Windows Store pro příslušný operační systém chytrého telefonu. Smart klíč lze zařadit do kategorie potvrzovacích aplikací, což je nová forma potvrzování transakcí.

4.4.3. Komunikace

Zabezpečení internetové komunikace mezi klientem a bankou se rovněž musí věnovat náležitá pozornost. Spojení probíhá za pomoci protokolu HTTPs, který je nadstavbou původního protokolu HTTP. Zmíněný protokol pochází ze sady protokolů TCP/IP určených pro síťovou komunikaci. Data přenášená protokolem HTTPs jsou šifrována za pomoci protokolu SSL, popřípadě jeho nástupcem TLS. Tím je zabráněno odposlechnutí dat při jejich přenosu.

[18] ČSOB. *ČSOB Smart Klíč.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/csob-smart-klic

[19] FINPARÁDA. *Smart klíč - nový bezpečnostní prvek internetového bankovnictví UniCredit Bank.* [online]. [cit. 2016-08-18]. Dostupné z: http://finparada.cz/1887-Smart-klic-novy-bezpecnostni-prvek-Internetoveho-bankovnictvi-UniCredit-Bank.aspx

Při komunikaci se využívá asymetrické kryptografie s párem klíčů označovaných jako veřejný a privátní. Při zahájení komunikace dochází k vzájemné výměně veřejného klíče, který je ověřen. Pro ověření se používá digitální certifikát vydaný důvěryhodnou certifikační autoritou. Poté, co je identita obou komunikujících stran potvrzena, je po vzájemné domluvě vygenerován šifrovací klíč, jímž bude následná komunikace šifrována. Tento šifrovací klíč je posílán protistraně ve zprávě, která je zašifrována veřejným klíčem odesílatele a soukromým klíčem příjemce je následně rozšifrována.

5. Útoky proti internetovému bankovnictví

S příchodem možnosti využívat pro manipulaci s peněžními prostředky služeb internetového bankovnictví, se klientům bank sice naskytla příležitost vykonávat bankovní operace pohodlnou cestou, nicméně útočníkům se tak zároveň naskytlo nové pole působnosti, jak klienty o jejich peníze připravit. Klient, který využívá služeb internetového bankovnictví, je totiž považován za nejslabší článek v komunikačním řetězci s bankou. Je tomu tak z důvodu, že v mnohých případech nedokáže ihned rozeznat případné hrozící nebezpečí či nedodržuje bezpečnostní doporučení své banky a pro útočníky je pak v tom případě mnohem snazší zacílit se právě na klienty, než na banky samotné.

Při útocích cílených na internetové bankovnictví se kyberzločinci snaží docílit ovládnutí počítače a mobilního telefonu napadeného či získání přístupových údajů k internetovému bankovnictví, popřípadě jiné službě, například emailové schránce nebo profilu na sociální síti. K tomu je využíván takzvaný phishing, při kterém jsou rozesílány nevyžádané emailové zprávy adresátům. Tyto zprávy jsou označovány jako spam. Zprávy mají v příjemci vyvolat dojem, že jejich odesílatelem je právě jeho banka, popřípadě jiná instituce, jejíž jméno útočníci zneužijí. Klient zaslanou zprávu nepovažuje za nebezpečnou, popřípadě není na první pohled schopen případný podvod poznat a reaguje na ni.

Phishingové zprávy mířené na přímé bankovnictví lze, dle výše poznamenaných cílů útočníků rozdělit do dvou větví. První větví jsou emaily, které vybízejí příjemce k uhrazení jednorázové faktury, poplatku za využívání služby, či pohledávky pod hrozbou exekuce. Takováto zpráva obsahuje požadovanou částku a číslo účtu, na který mají být peníze poslány. Do této kategorie se řadí i snahy o získání údajů o platebních kartách, kdy je příjemce zprávy vyzván k vyplnění údajů o své platební kartě. Druhou větví phishingových zpráv se útočníci snaží do počítače příjemce propašovat škodlivý software. Tento software se označuje jako malware, nebo trojský kůň. Do styku lze přijít i se slovním spojením bankovní malware. Malware má následně za úkol stáhnout z internetu další škodlivý kód, který následně získá klientovi přístupové údaje. Tento způsob phishingového útoku se více prohloubil s rozvojem chytrých telefonů a jejich užíváním. Tvoří tak velmi nebezpečný a zároveň efektivní způsob jak zákazníka oklamat.

Kromě emailů se útočníci zaměřují rovněž na zneužití profilů na sociálních sítích. Typickým příkladem je populární Facebook. Zde útočníci zneužijí profil některého z přátel napadeného. Přístupové údaje získají pomocí odkazu na falešnou platební bránu a následně požádají o přeposlání potvrzovací SMS zprávy s ověřovacím kódem transakce s odůvodněním, že mají problém s mobilním telefonem. Dalším příkladem zneužití Facebooku byla snaha vylákat z klientů přístupové údaje pomocí falešné stránky České spořitelny, kde byla nabízena nové verze služby internetového bankovnictví SERVIS 24.[20] Klient byl navíc lákán finančním bonusem.

Prvotní útoky se vyznačovaly tím, že byly napsány velmi špatnou češtinou s velkým množstvím gramatických chyb. Zde tedy bylo snadné odhalit podvodnou činnost. Tato skutečnost se ovšem postupem času změnila. Phishingové zprávy začaly být sofistikovanější a poznat na první pohled podvodnou zprávu již není jednoduché.

5.1. Útok proti internetovému bankovnictví pomocí bankovního malware

Jak bylo uvedeno výše, využití bankovního malware je způsob jakým se útočníci snaží získat klientovy přístupové údaje a připravit ho tak o jeho peníze. Tento typ útoku má za cíl nakazit jak klientův počítač, tak i jeho chytrý telefon škodlivým kódem. Útok je velmi sofistikovaný, jelikož se snaží o prolomení obou bezpečnostních mechanismů chránící internetové bankovnictví. Necílí pouze na získání přístupových údajů, ale zároveň i na získání potvrzovacích SMS kódů, které slouží k ověření a následnému provedení platební transakce. Útok má následující průběh.

5.1.1. Průběh ovládnutí klientova počítače

Snaha o napadení klientova počítače je první fází. K tomuto účelu jsou rozesílány spamové emaily, které v příloze obsahují škodlivý software. Útočníci mohou získat emailové adresy klientů několika způsoby. Těmi nejčastějšími jsou nákupy těchto komodit na černém trhu

[20] ČESKÁ SPOŘITELNA. *Falešný profil na Facebooku nabízející „nový SERVIS 24“*. [online]. 2016 [cit. 2016-10-06]. Dostupné z: https://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality

a jejich náhodně generování. Příjemce tak může obdržet podvodný email určený zákazníkovi určité banky, i když jím ve skutečnosti není.

V takovémto spamovém emailu je kromě předem připraveného sdělení vysvětlující jeho účel přiložena příloha, v níž se škodlivý kód nachází. Obsah přílohy bývá označován za soubory s příponou typu *.pdf, *.zip apod. Ve skutečnosti se, ale nejedná o soubor žádného z těchto formátů, nýbrž o spustitelný *.exe soubor. Pokud je tento soubor otevřen, je počítač okamžitě infikován škodlivým kódem bez vědomí jeho vlastníka. Již proniknutý software pak následně stahuje z internetu další škodlivý kód, který má již za úkol získat přístupové údaje. Ty může získat odposloucháváním komunikace v internetovém prohlížeči, kterou odesílá na server útočníka nebo vložením kódu, který v prohlížeči zobrazí podvodnou webovou stránku, kam jsou údaje zadávány. Tyto podvržené webové stránky jsou věrnou kopií stránek originálních.

5.1.2. Průběh ovládnutí klientova chytrého telefonu

Kompromitování klientova chytrého telefonu je druhou fází útoku, která je podmíněna skutečností, že jeho počítač již byl útoku vystaven a úspěšně infikován. K ovládnutí telefonu je potřeba provedení několika kroků. Prvním krokem je již zmíněné nakažení klientova počítače škodlivým kódem. Tento kód po přihlášení do internetového bankovnictví v internetovém prohlížeči zobrazí pomocí metody označované jako injection falešné sdělení. Kromě podvržení kódu stránky, může být provedeno i takzvané přesměrování na stránku. Klient je tímto oznámením vyzván ke stažení bezpečnostní aplikace, jež má za úkol zvýšit zabezpečení chytrého telefonu. Dle typu chytrého telefonu, přesněji řečeno dle používaného operačního systému je zvolena příslušná verze dané aplikace. Ta je stažena a nainstalována. Aplikace ovšem nemá žádné bezpečnostní funkce. Právě naopak. Tyto aplikace jsou navrženy tak, že po instalaci zachytávají SMS zprávy přijímané na napadený telefon a následně je přepošlou útočníkovi. Tímto způsobem se útočníci dostanou i k ověřovacím SMS zprávám zasílaných bankami a získají ověřovací kód pro provedení transakce. Klient napadeného telefonu nemusí mít ani ponětí, že byla nějaká zpráva vůbec přijata. Podvodné aplikace totiž mohou oznámení o přijetí zamaskovat, či dokonce zajistit, že napadený telefon nebude možno použít.

5.1.3. Útok s využitím trojského koně Tinba

Tinba je zkratka pro název trojského koně Tinny Banker, který v roce 2014 mířil na několik bank v České republice. Konkrétně se jednalo o Českou spořitelnu, ČSOB, Eru a Fio banku.[21]

Tento trojský kůň byl rozesílán za pomoci phishingového emailu, který se vydával za exekuční příkaz. V příloze emailu je přiložen soubor zahrnující podrobnosti o exekučním příkazu. Po otevření přiloženého souboru se zobrazí dokument s podrobnostmi o příkazu. Tím je upoutána příjemcova pozornost, a zatímco dokument prohlíží, stáhne se do počítače další škodlivý kód. Tato procedura dodává zprávě na její autentičnosti. U předchozích útoků se po otevření přílohy žádný soubor nezobrazoval.

Přístupové údaje do internetového bankovnictví jsou zcizeny prostřednictvím podvrženého kódu v legitimních webových stránkách banky. Zcizené údaje jsou následně odeslány na server útočníka. Kód stránky, která má být podvržena se volí dle navštívených stránek konkrétní banky. Dalším krokem je vyzvání napadeného klienta ke stažení aplikace do jeho chytrého telefonu, která má zvýšit zabezpečení jeho účtu. V případě tohoto bankovního malware se jedná o aplikaci s názvem OTPdirect[22], jenž slouží ke generování jednorázových hesel při vstupu do internetového bankovnictví. Aplikace je dostupná ve více verzích a klient si konkrétní verzi volí dle operačního systému jeho telefonu. V nabídce se nachází Android, iOS, BlackBerry a Windows. Aplikace však funguje pouze na platformě Android, u ostatních nabízených operačních systémů se uživateli zobrazí oznámení, že má pokus opakovat později.

5.1.4. Útok s využitím trojského koně Hesperbot

Hesperbot je název trojského koně, který se rozšiřoval pomocí phishingové kampaně v České republice od srpna roku 2013. Útoku na služby internetového bankovnictví prostřednictvím viru Hesperbot čelilo v České republice několik bank. Jmenovitě

[21] HOŘEJŠÍ, Jaromír. AVAST. *Falešný exekuční příkaz ohrožuje uživatele českých bank* [online]. 2014 [cit. 2016-11-13]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

[22] Tamtéž.

se jednalo o Českou spořitelnu, ČSOB, Komerční banku, Raiffeisenbank a Unicredit Bank.[23]

Hesperbot se šířil jako příloha phishingového emailu, který se tentokrát vydával za zprávu, jejímž odesilatelem údajně byla Česká pošta. Zpráva obsahovala sdělení o neúspěšném pokusu o doručení zásilky včetně informace o případných sankcích vůči klientovi, pokud si zásilku nevyzvedne. Pro útok si útočníci registrovali doménu www.ceskaposta.net, která je téměř identická s tou skutečnou. Ta se ovšem nazývá www.ceskaposta.cz.[24]

Samotný trojský kůň se ukrývá v příloze pod označením zasilka.pdf.exe, která se vydává za soubor typu *.pdf, ovšem ve skutečnosti se jedná o spustitelný *.exe soubor po jehož otevření se do počítače příjemce začne stahovat další škodlivý kód.

Při podvržení kódu do webového prohlížeče je klientovi nabídnuta bezpečnostní aplikace do jeho chytrého telefonu. Lze si zvolit mezi platformami Android, Symbian a Blackberry.[25] Zda byla aplikace nainstalována, se útočník dozví po zadání aktivačního kódu v aplikaci, načež vrátí kód pro odpověď, který je zadán do podvržené webové stránky.

Kromě podvrhování kódu do webového prohlížeče má Hesperbot i jiné funkce. Tento trojský kůň může využívat funkce keylogger, která zaznamenává klávesy stisknuté uživatelem. Dále má schopnost pořizovat screenshoty obrazovky nebo zachycovat videa. Získané údaje jsou následně přeposílány na server útočníka. Velmi nebezpečnou vlastností Hesperbotu je vytváření VNC serveru, který umožňuje útočníkovi převzít kontrolu nad infikovaným počítačem zcela nepozorovaně. Kromě výše uvedených schopností je schopen i podvrhnout certifikáty ve webovém prohlížeči. K této proceduře využívá tzv. proxy, který představuje prostředníka v komunikaci mezi klientem a cílovým serverem

---

[23] POLESNÝ, David. ŽIVĚ.CZ. *Falešné e-maily České pošty nesly nový a velmi nebezpečný malware* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.zive.cz/bleskovky/falesne-e-maily-ceske-posty-nesly-novy-a-velmi-nebezpecny-malware/sc-4-a-170448

[24] LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – A New, Advanced Banking Trojan in the Wild* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/

[25] LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – Technical analysis part 1/2* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/06/hesperbot-technical-analysis-part-12/

5.1.5. Příklady falešných aplikací pro chytré telefony

Aplikací, k jejichž instalaci jsou klienti bank během útoku nabádáni, aby tak útočníci získali přístup k ověřovacím SMS, existuje několik. Příkladem může být výše zmíněná OTPdirect k jejíž instalaci nabádá bankovní malware Tinba. Další je výrobek firmy TrustPort a.s. s názvem TrustPort Mobile Security.[26] Autentičnost nabídky podporuje fakt, že takováto aplikace skutečně existuje a opravdu slouží k ochraně mobilních zařízení.[27]

Poté, co byl zveřejněn tento typ útoku proti službám internetového bankovnictví, začali být jeho uživatelé obezřetní, ohledně nabídek různých bezpečnostních aplikací. Podvodníci se tak snaží využívat jiné způsoby přístupu k autorizačním zprávám, které zahrnují běžně používané služby. Příkladem je aplikace SeznamOTP.apk objevující se od června 2014, jenž je cílena na uživatele aplikace Seznam.cz Email.[28] Tato podvodná aplikace se maskuje jako prostředek pro generování jednorázových hesel umožňujících bezpečnější přístup k účtu elektronické pošty, kterou provozuje Seznam.cz.

Další podvodná aplikace, která rovněž zneužívá jména oficiální společnosti, se tentokráte zaměřuje na uživatele sociální sítě Facebook. Varování před podvodnou aplikací vydala v březnu roku 2016 banka Air Bank.[29] Útočníci tentokráte nabízejí novou mobilní aplikaci pro přístup na facebookový účet jako náhradu za zablokování té původní. Po provedení instalace tak útočníci opět získají přístup k SMS zprávám.

5.1.6. Vzhled podvodné stránky

Na následujícím obrázku lze vidět podobu jedné z podvržených stránek, které vyzývají majitele infikovaného počítače k instalaci bezpečnostní aplikace do chytrého telefonu.

---

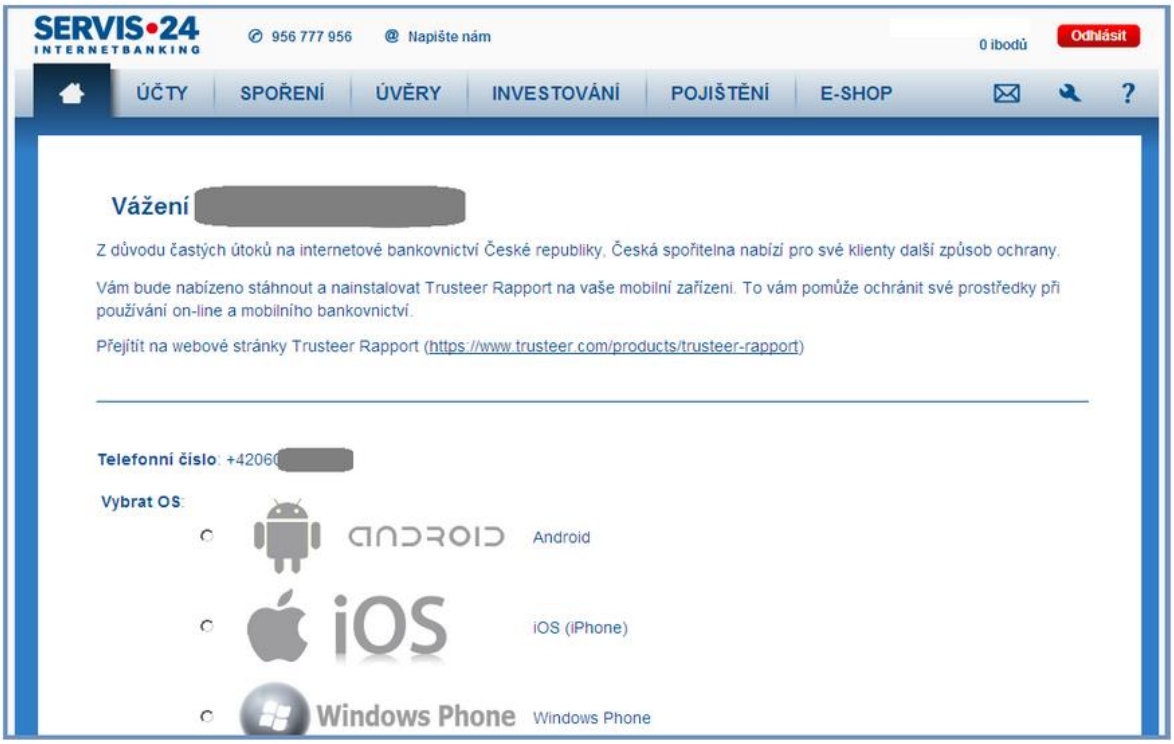
[26] ČERMÁK, Miroslav. CEVERANDSMART. *Českem se prohnala další vlna spamu, kdy se útočník vydává za slušného spoluobčana* [online]. 2015, 2015-02-25 [cit. 2015-10-20]. Dostupné z: http://www.cleverandsmart.cz/ceskem-se-prohnala-dalsi-vlna-spamu-kdy-se-utocnik-vydava-za-slusneho-spoluobcana/

[27] TRUSTPORT. *Home Users and Small Companies* [online]. [cit. 2017-03-01]. Dostupné z: http://www.trustport.com/en/home-users

[28] NOVINKY.CZ. *Podvodníci mění taktiku. Našli novou cestu, jak vybílit lidem účty* [online]. 2015 [cit. 2016-10-10]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

[29] AIR BANK. *Dejte si pozor na falešnou výzvu k instalaci nové mobilní aplikace pro Facebook* [online]. 2016 [cit. 2016-04-01]. Dostupné z: https://www.airbank.cz/novinky/dejte-si-pozor-na-falesnou-vyzvu-k-instalaci-nove-mobilni-aplikace-pro-facebook/

Varování před touto verzí podvodné stránky, jež vybízí k instalaci bezpečnostní aplikace Trusteer Rapport vydala Česká spořitelna v lednu 2014.



Obrázek 4: Podoba podvržené stránky, vybízející k instalaci bezpečnostní aplikace v internetovém bankovnictví České spořitelny. Zdroj: ČESKÁ SPOŘITELNA. *O nás: Archiv aktualit* [online]. 2014 [cit. 2016-10-06]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_2066.xml

Stránka podvržená za pomoci škodlivého kódu je na první pohled nerozeznatelná od originálu. Stránka obsahuje ve své hlavičce logo SERVIS 24 INTERNETBANKING, kontaktní číslo, jméno majitele účtu (v ukázce není viditelné) a tlačítko pro odhlášení. Pod hlavičkou je umístěno menu, pomocí kterého se uživatel může přepínat dle úkonu, který chce provést. Ve znění stránky se nachází oslovení uživatele a sdělení proč je mu daná aplikace nabízena. V případě tohoto sdělení se konkrétně jedná o nabídku rozšíření bezpečnosti s ohledem na již proběhnuté útoky. Součástí je i odkaz na webové stránky daného produktu. Se sdělením je zobrazena i nabídka ohledně verze nabízené aplikace pro konkrétní operační systém chytrého telefonu klienta. Zde konkrétně pro Android, iOS a Windows Phone.

5.1.7. Reakce na útoky

Před nebezpečím útoku banky pravidelně informují veřejnost a hlavně své klienty prostřednictvím svých webových stránek. Informace jsou uveřejňovány i na zpravodajských portálech a za pomoci médií. V případě útoků s využitím trojského koně Hesperbot, kromě uvedených způsobů poskytnutí informací, do kterých byly zapojeny i televizní stanice Nova[30] a Česká televize[31], vydala varování před jeho šířením spolu s popisem falešného emailu také Česká pošta, jejíž jméno bylo během útoku zneužito.[32] V případě vlny phishingových emailů, které obsahovaly falešné exekuční příkazy, varovala i Exekutorská komora České republiky[33], jejíž jméno bylo při této vlně útoku zneužito podobně jako tomu bylo v předchozím případě u České pošty.

5.1.8. Obdobné útoky v zahraničí

Phishingové útoky jsou hojně rozšířeny nejen v České republice, ale i v zahraničí. Pomocí výše popsaného viru Heperbot byli napadeni klienti bank ve Velké Británii, Turecku nebo v Portugalsku.[34] Cíli trojského koně Asacub, který se objevuje v různých podobách od června 2015, byly klienti využívající internetové bankovnictví v Rusku, Spojených státech Amerických a na Ukrajině.[35] V říjnu 2016 se pod útokem ocitla britská banka

[30] TN.CZ. *Maily pod hlavičkou České pošty obsahovaly vir! Byl to hackerský útok ze 4 zemí* [online]. 2013, 2013-09-05 [cit. 2016-12-18]. Dostupné z: http://tn.nova.cz/clanek/zpravy/zahranici/maily-pod-hlavickou-ceske-posty-obsahovaly-vir-byl-to-hackersky-utok-ze-4-zemi.html

[31] CT24. *Falešné e-maily s logem České pošty jako součást obří kriminální akce* [online]. 2013 [cit. 2016-12-18]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/1076886-falesne-e-maily-s-logem-ceske-posty-jako-soucast-obri-kriminalni-akce

[32] ČESKÁ SPOŠTA. *Phishingové útoky na Českou poštu neustávají* [online]. 2013 [cit. 2016-10-24]. Dostupné z: https://www.ceskaposta.cz/-/phishingove-utoky-na-ceskou-postu-neustavaji

[33] EXEKUTORSKÁ KOMORA ČESKÉ REPUBLIKY. *Exekutorská komora varuje před podvodnými e-maily vyzývajícími k úhradě dluhu* [online]. 2015 [cit. 2017-03-01]. Dostupné z: http://www.ekcr.cz/1/aktuality-pro-media/2060-exekutorska-komora-varuje-pred-podvodnymi-e-maily-vyzyvajicimi-k-uhrade-dluhu-19-10-2015?w=

[34] LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – A New, Advanced Banking Trojan in the Wild* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/

[35] FEEDIT.CZ. *Trojan Asacub cílí skrze Android na finance obětí* [online]. 2016 [cit. 2016-10-20]. Dostupné z: http://www.feedit.cz/wordpress/2016/01/26/trojan-asacub-cili-skrze-android-na-finance-obeti/

Tesco Bank. Dle společnosti ESET, jež působí v oblasti IT bezpečnosti, byl útok proveden s největší pravděpodobností za pomoci trojského koně Retefe.[36]

5.2. Jak se bránit útokům proti internetovému bankovnictví?

S rostoucí mírou výskytu snah podvodníků a kyberzločinců získat přístup ke klientským účtům prostřednictvím internetového bankovnictví, se právě klienti sami musí mít co nejvíce na pozoru. Měli by důrazně dodržovat nejen bezpečnostní doporučení své banky, ale i obecné zásady bezpečnosti na internetu. Jinými slovy, klienti by se měli řídit tzv. selským rozumem a ne bezmezně věřit, že vybraný odkaz, na který kliknou, je přesměruje na webovou stránku, o níž se domnívají, že je bezpečná. Klienti by si měli všímat, zda se v prostředí služby internetového bankovnictví nevyskytují nové grafické či textové prvky. Především ty, o kterých nebyli předem informováni a vyzývají k pořízení nějakého doplňku, či zadání důvěrných údajů. Pokud se klient s podobnou situací setká, měl by aplikaci přestat používat, odhlásit se a kontaktovat zákaznickou linku, kde případně může požádat o zablokování účtu. Rovněž by tak měl učinit i v případě, kdy pojal pouze podezření.

Při otevírání a čtení emailů je důležité se nejdříve podívat, kdo daný email odeslal a následně na předmět emailu. Pokud je předmětem emailu například exekuční příkaz příjemce by ho měl ignorovat. Takovýto příkaz může být zaslán pouze v papírové podobě poštou. V elektronické podobě může být zaslán pouze do datové schránky, což je úložiště pro příjem úředních dokumentů v elektronické podobě. Emailem může být zaslán pouze na žádost příjemce. Navíc je opatřen elektronickým podpisem.[37]

---

[36] HÁJKOVÁ, Gabriela. MEŠEC.CZ. *ESET: Za vybrané účty klientů Tesco Bank může asi příloha v podvodném e-mailu* [online]. 2016 [cit. 2016-11-17]. Dostupné z: http://www.mesec.cz/aktuality/eset-za-vybrane-ucty-klientu-tesco-bank-muze-asi-priloha-v-podvodnem-e-mailu/

[37] EXEKUTORSKÁ KOMORA ČESKÉ REPUBLIKY. *Exekutorská komora varuje před podvodnými e-maily vyzývajícími k úhradě dluhu* [online]. 2015 [cit. 2017-03-01]. Dostupné z: http://www.ekcr.cz/1/aktuality-pro-media/2060-exekutorska-komora-varuje-pred-podvodnymi-e-maily-vyzyvajicimi-k-uhrade-dluhu-19-10-2015?w=

Samozřejmostí je mít na počítači i na chytrém telefonu nainstalovaný antivirový software, který zařízení chrání před škodlivým softwarem a pravidelně jej aktualizovat. Klienti Komerční banky mohou navíc využít doplněk pro webový vyhledávač jménem Trusteer Rapport vyvinutý společností IBM cíleně proti phishingovým útokům.[38]

5.2.1. Bankovní desatero

Bankovní desatero je označení, které používají banky pro definici základních bezpečnostních doporučení při využívání služeb internetového bankovnictví. Znění desatera se může odlišovat dle konkrétní banky, nicméně v zásadě se jedná o následující bezpečnostní body.

Pro využívání služeb internetového bankovnictví využívat pouze bezpečný počítač. Pod pojmem bezpečný počítač se rozumí osobní, popřípadě pracovní počítač, který je využíván k běžné činnosti. Není tedy vhodné využívat počítače například v internetových kavárnách či jakýkoliv jiný neznámý stroj.

Do služby internetového bankovnictví se přihlašovat pouze ze známé internetové adresy, která je zadána přímo do adresního řádku internetového prohlížeče. Vstup je také možný kliknutím na odkaz přímo na webových stránkách banky. Není doporučeno přihlašovat se do internetového bankovnictví ze stránek, které byly nalezeny pomocí vyhledávačů jako například Google nebo Seznam. Pokud je tak učiněno, může dojít k přesměrování na podvodné stránky. Než dojde k samotnému přihlášení, ujistit se, že komunikace probíhá prostřednictvím bezpečného spojení. To je indikováno ikonou zeleného zámku u adresního řádku. Doporučována je také kontrola certifikátu, jehož podrobnosti se zobrazí po kliknutí na onen zámek.

Přístupové údaje k internetovému bankovnictví, jenž jsou představovány přihlašovacím jménem, heslem, PINem, popřípadě elektronickým certifikátem, musí být náležitě chráněny. Neměli by být nikde poznamenané a sdělené jiné osobě. Při volbě PINu a hesla by neměly být voleny snadno odvoditelné kombinace. Datum narození nebo jméno

[38] KOMERČNÍ BANKA. *Trusteer rapport - účinná ochrana vašeho prohlížeče* [online]. [cit. 2017-03-01]. Dostupné z: https://www.kb.cz/bezpecnost/klient/index.shtml

se vůbec nedoporučuje používat. Co se týče hesla, mělo by být zvoleno takové, které obsahuje minimálně osm znaků a zahrnuje malá velká písmena, číslice a speciální znaky.

Na počítači i chytrém telefonu by měl být nainstalován antivirový program chránící zařízení před škodlivým kódem. Dále je nutné provádět aktualizace operačního systému, antivirového softwaru, webového prohlížeče i dalšího programového vybavení. Aktualizacemi jsou získány bezpečnostní záplaty, které odstraňují případné chyby, které by mohli být útočníkem zneužity.

Nové programy a aplikace by měli být pořizovány pouze z oficiálních a ověřených zdrojů a to jak pro počítač, tak i pro chytrý telefon.

Nereagovat na emailové zprávy přijaté od neznámých odesilatelů. Emaily obsahující požadavek na vyplnění přístupových údajů, či odkaz na stránku, kde mají být vyplněny, by měly být ignorovány a smazány. Banky tímto způsobem důvěrné informace po svých klientech nepožadují.

Při potvrzování plateb pomocí kódu přijatého v SMS zprávě, zkontrolovat údaje zaslané spolu s potvrzovacím kódem s údaji platby zadaných v systému internetového bankovnictví. Vyvarovat se automatickému přepsání kódu bez předchozí kontroly údajů.

Ke svému účtu si zřídit službu zajišťující zasílání informačních SMS zpráv nebo emailů, které klienta informují o pohybech na jeho účtu.

U chytrých telefonů nastavit zákaz instalace aplikací z neznámých zdrojů a nastavení upozornění na potencionálně nebezpečné aplikace. Při instalaci nové aplikace se doporučuje sledovat, jaká oprávnění jsou požadována. Například zda aplikace vyžaduje přístup k SMS zprávám.

Pravidelně sledovat informace týkající se bezpečnosti, které banka sděluje. Tyto informace jsou zveřejňovány na webových stránkách banky klienta.

5.2.2. Kde získat informace?

Informace ohledně případných hrozeb a dalších aktualit týkajících se banky je možno získat prostřednictvím jejích webových stránek. Pro snadnější hledání požadovaných informací lze využít vyhledávací pole, do kterého je napsán hledaný řetězec, například aktuality nebo bezpečnost a zvolit vyhledat.

Kromě webových stránek bank, je informace možno získat i na jiných portálech. Jedná se převážně o portály s ekonomickým zaměřením, či zpravodajské portály. Příkladem mohou být webové stránky České bankovní asociace či portály Měšec nebo Finparáda. Varování jsou uveřejňována i v televizních zpravodajstvích.

Navzdory uveřejňovaným varováním stále dochází k případům, kdy se útočníkům podaří klienta banky oklamat. Na vině však nejsou pouze aktivity útočníků, ale hlavně neopatrnost a důvěřivost klientů. To dokazují zaznamenané případy krádeže peněz za pomoci zneužití profilů na sociální síti Facebook, kdy si napadený předem neověřil, že opravdu komunikuje s danou osobou.

Neopatrnost klientů také dokazuje průzkum, který provedla ČSOB. V průzkumu sice bylo zjištěno, že 65% dotazovaných by na zprávu požadující vyplnění přístupových údajů nereagovalo.[39] Další zjištění, jsou ovšem z hlediska bezpečnosti znepokojivá. Například heslo k internetovému bankovnictví si mění pouze 16% dotazovaných, sdílení hesla i s jinými aplikacemi přiznalo 15,5% nebo skutečnost, že 13% přistupuje do internetového bankovnictví přes webový prohlížeč.[40] Stejně tak existují i výrazné mezery v zabezpečení chytrých telefonů. Vše i přes doporučení uvedená v bankovním desateru.

[39] ČSOB. *ČSOB si posvítila na naše zlozvyky: Heslo do online bankovnictví si aktivně nemění většina z nás* [online]. 2016 [cit. 2016-12-18]. Dostupné z: https://www.csob.cz/portal/o-csob/o-csob-a-kbc/servis-pro-media/tiskove-zpravy/-/asset_publisher/5FasXY5AUiLR/content/id/1698538

[40] Tamtéž.

6. Autorizace transakcí pomocí OTP zasílaných SMS zprávou

6.1. Co je potvrzovací OTP?

OTP, nebo-li One-Time-Password (v překladu jednorázové heslo) je speciální kód, který se užívá pro ověření identity. V internetovém bankovnictví se užívá pro potvrzování transakcí zadaných klientem. Pokud chce klient provést transakci přes internet, musí pro její dokončení zadat kód, který mu byl doručen SMS zprávou.

OTP je nástrojem dvoufaktorové autentizace a je považován za autentizaci typu něco vím, popřípadě něco mám. To znamená, že existuje znalost, která se předává, v tomto případě OTP kód a zařízení, pomocí kterého lze tuto znalost předat. Předat ji lze pomocí počítače, kdy je kód zadán do požadovaného vstupního pole v prostředí internetového bankovnictví. Kromě potvrzování transakcí lze OTP kódy využít i při přihlašování. Vlastností dvou a vícefaktorová autentizace je fakt, že zvyšuje bezpečnost za cenu snížení uživatelského komfortu, ale vhodnou kombinací prostředků to lze akceptovat.

OTP kódy nelze samo o sobě považovat za dostatečný prostředek identifikace a autentizace dané osoby. Jsou proto kombinovány s jinými autentizačními prostředky. Z toho důvodu jsou označovány jako prostředek dvoufaktorové autentizace. V případě internetového bankovnictví se kombinují s přihlašovacími údaji. Identifikační číslo a heslo, popřípadě identifikační číslo a PIN, či jiný prostředek pro přihlášení, jsou považovány za autentizaci prvního stupně, které umožní vstup do prostřední internetového bankovnictví. OTP kód pro potvrzení zadané transakce, či pro přihlášení je prostředkem druhého stupně autentizace. Přístupové údaje jsou zadávány prostřednictvím webové stránky, pomocí které je také vyžadována autorizace transakce pomocí zvoleného prostředku. OTP, kterým je transakce v příkladu potvrzována, klient neobdrží přes internet, ale SMS zprávou na mobilní telefon. Z příkladu lze tedy vyčíst využití druhého komunikačního kanálu. Za ten jsou považovány také hardwarové kalkulátory. V souvislosti s dvoufaktorovou autentizací tedy klient něco ví, v uvedeném příkladu přihlašovací údaje a OTP kód a něco má, tedy prostředek pro jejich předání, konkrétně počítač.

OTP kódy užívané pro potvrzování transakcí v internetovém bankovnictví jsou generovány v systému banky, jíž je uživatel internetového bankovnictví klientem a následně mu jsou přeposlány na jím uvedené telefonní číslo za pomoci SMS zprávy. Tyto kódy mají podobu číslic a písmen o požadované délce. V praxi se užívají osmi až desetimístné kódy.

OTP je v bankovnictví také často označováno pojmem TAN, což je zkratka anglického názvu Transaction Authentication Number. V překladu Ověřovací číslo transakce.

6.2. Varianty OTP pro potvrzení transakce přes internetové bankovnictví

OTP mohou být v bankovnictví využity v několika variantách. Toto jsou odpovídající podoby.

6.2.1. TAN

Označovaný také jako klasický TAN. Klientovi banky je vygenerován seznam určitého počtu jednorázových kódů. Pro potvrzení transakce je vždy zvolen jeden konkrétní kód, který je uživatelem zadán. Tento již pak nelze znovu použít.

Lze se také setkat s variantou iTAN. Při využití iTAN je po klientovi vyžadován kód na konkrétní pozici v jím obdrženém seznamu.

6.2.2. TAN plus CAPTCHA

TAN v kombinaci se systémem CAPTCHA, je varianta užití TAN kódu, kdy je potřeba zadat mimo jednorázového kódu také kód zobrazený na stránce. Tento proces se snaží zabránit automatizovaným útokům. Tato varianta je využívána například v bankách v Německu. Příkladem je Raiffeisen-Volksbank eG.[41]

[41] RAIFFEISEN - VOLKSBANK TÜßLING UNTERNEUKIRCHEN EG. *Sicherheitshinweise* [online]. [cit. 2017-02-18]. Dostupné z: https://www.rv-banken.de/online-banking/sicherheitshinweis.html

6.2.3. mTAN

mTAN je označení pro Mobile Transaction Authentication Number. Někdy označované jako autentizační nebo potvrzovací SMS. Jedná se o nejrozšířenější variantu potvrzování transakcí prostřednictvím internetu. V této variantě TANu je potvrzovací kód zaslán klientovi formou SMS zprávy na mobilní telefon. Kromě samotného kódu jsou ve zprávě zahrnuty i informace o samotné transakci. Mezi tyto údaje patří čísla účtů, výše převáděné částky či variabilní symbol platebního styku. Tyto údaje banky doporučují před potvrzením transakce zkontrolovat s údaji zadanými ve formuláři internetového bankovnictví.

mTAN má platnost pouze určitou dobu. Jeho charakteristikou je také skutečnost, že pokud dojde k určitému počtu nesprávných zadání, či žádostí o nové autentizační kódy, je přístup zablokován. Počet chybných zadání může být defaultně nastaven bezpečnostní politikou banky popřípadě samotným klientem.

6.2.4. Autentizační kalkulátor

Autentizační kalkulátor je prostředek pro generování jednorázových kódů, který je odloučený od systému banky. To znamená, že mezi ním a bankou není přímé spojení. Kalkulátor pracuje na principu generování jednorázového kódu na základě údajů zadaných klientem. Tyto údaje jsou představovány například číslem účtu, převáděnou částkou a dalšími údaji. Vygenerovaný kód je následně zadán do systému pro potvrzení transakce. Pokud se kód zadaný uživatelem a kód vypočtený v systému banky neshodují, transakce není provedena. Užívání kalkulátoru pro generování kódů je podmíněno zadáním PIN kódu. Mezi jeho nezpochybnitelnou výhodu patří to, že jej lze použít nezávisle na mobilním signálu, oproti OTP zasílaným SMS.

Přestože se jedná o nejbezpečnější prostředek pro potvrzování transakcí, přináší s sebou své nevýhody. Při zadávání údajů pro generování kódu může dojít k chybě v podobě nesprávně zadané hodnoty, což má za následek neplatnost vygenerovaného kódu. Pro vygenerování nového je pak nutné provést celý proces zadávání znovu, což snižuje uživatelský komfort. Může dojít i k situaci, kdy se kalkulátor po určitém počtu pokusů zadání špatného PIN kódu zablokuje a je nutný servisní zásah. Další nevýhody představují pořizovací náklady, případné mechanické poškození a vybití baterie. U hardwarových

kalkulátorů se také vyskytuje problém tzv. rozsynchronizace. Tedy stavu, kdy kód vypočtený zařízením neodpovídá kódu vypočtenému interním systémem.

Autentizační kalkulátor je v současné době stále nabízen klientům Raiffeisenbank[42] či UniCredit bank[43].

6.3. Výhody potvrzovacích OTP zasílaných SMS zprávou

Největší výhodou tohoto řešení pro potvrzování transakcí spočívá v předávání potvrzovacího kódu. SMS zprávu obsahující potvrzovací kód lze doručit na jakýkoliv mobilní telefon, nejenom na chytré telefony. S tím souvisí další výhoda a to skutečnost, že pro přijetí kódu není potřeba žádného dalšího zařízení, jako je tomu u autentizačního kalkulátoru. Z pohledu finančních nákladů se tedy jedná o levné řešení, protože si klient nemusí pořizovat další zařízení. SMS zprávy jsou navíc poměrně levnou záležitostí.

Další výhoda předávání OTP SMS zprávou je v dostupnosti. Přesněji ve skutečnosti, že mobilní telefon má v dnešní době téměř každý.

Souhrnně tato varianta předávání představuje pro klienta komfortní řešení, na nějž se metoda také zaměřuje. Není zde potřeba zdlouhavě zadávat žádné údaje, jako u autentizačního kalkulátoru. Jediné přepisování v souvislosti s touto variantou předání potvrzovacího kódu spočívá v jeho zadání do formuláře v internetovém bankovnictví.

6.4. Nedostatky potvrzovacích OTP zasílaných SMS zprávou

I přes své značné výhody má přeposílání kódů SMS zprávami i svá úskalí. Tím nejvíce limitujícím je závislost na dostupnosti signálu. Aby byla zpráva přijata, musí se klient nacházet v místě kde je pokrytí signálem poskytováno. Z pohledu plateb prováděných v prostředí domova lze tuto skutečnost považovat za bezpředmětnou, ovšem pokud je potřeba provést neočekávanou platbu například na dovolené, může nedostatečný signál

[42] RAIFFEISENBANK. *Bezpečnost internetového bankovnictví* [online]. [cit. 2017-03-04]. Dostupné z: https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/bezpecnost-internetoveho-bankovnictvi

[43] UNICREDIT BANK. *O bezpečnosti: Typy bezpečnostních klíčů* [online]. [cit. 2017-03-04]. Dostupné z: https://www.unicreditbank.cz/cs/obcane/ucty/online-sluzby.html#obezpecnosti

představovat problém. Stejně tak při výpadku signálu. Při posílání SMS zprávy se také může vyskytnout problém v podobě zdržení doručení zprávy, například z důvodu čekání ve frontě či technické závady v síti operátora. Operátoři garantují platnost zprávy do 72 hodin, což je vzhledem ke krátké době platnosti OTP kódu neakceptovatelné.

Při přepisování přijatého kódu se klient může splést a zadat špatný znak. Následné potvrzení transakce je pak neplatné a je nutno požádat o nový potvrzovací kód.

V počátcích zavádění SMS jako nástroje pro potvrzování transakcí se vyskytly argumenty ohledně tvrzení, že ne každý klient nutně disponuje mobilním telefonem.[44] Proto byla tato metoda autorizace nabízena zpočátku jako dobrovolná, kdežto v dnešní době je bankami vyžadována.

Bezesporu největším nedostatkem, či spíše bezpečnostní hrozbou předávání potvrzovacích kódů pomocí SMS zpráv je riziko, že zpráva bude odposlechnuta útočníkem. Metod, kterými může útočník SMS zprávu s kódem získat existuje několik.

6.5. Hrozby proti OTP zasílaným pomocí SMS zprávy

Zde je potřeba uvést na pravou míru, že problém nespočívá v zasílaném OTP kódu, jako takovém, nýbrž v prostředku jeho přenosu. Tedy v podobě SMS zprávy, kterou je možno útočníkem získat několika metodami. Již zaznamenané útoky, kdy se útočníkům podařilo získat nejen přístupové údaje do internetového bankovnictví, ale i potvrzovací SMS dokazuje, že tato metoda autorizace transakce není tak bezpečná, za jakou byla považována. Z tohoto důvodu společnost National Institute of Standards and Technology, zkráceně NIST, sídlící ve Spojených státech, označila tuto metodu z bezpečnostního hlediska jako nedostačující a doporučila její nepoužívání jako prostředku dvoufaktorové autentizace.[45]

[44] PIŠTORA, Martin. MĚŠEC.CZ. *Bankovní bezpečnost: Rizika SMS* [online]. 2006 [cit. 2017-02-14]. Dostupné z: http://www.mesec.cz/clanky/bankovni-bezpecnost-rizika-sms/

[45] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *DRAFT NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management* [online]. 2016 [cit. 2017-02-14]. Dostupné z: https://pages.nist.gov/800-63-3/sp800-63b.html

6.5.1. Mobilní malware

V současnosti nejrozšířenější způsob jak se útočníci snaží získat přístup nejen k SMS zprávám v chytrém telefonu klienta, ale i k samotnému zařízení. Při útoku se útočník snaží propašovat do klientova mobilu škodlivý kód. K tomuto účelu se nejčastěji používá phishing, kdy je po cílové osobě požadováno provedení činnosti, jenž umožní nakažení telefonu. Nejčastěji se tak děje pomocí podvržených stránek ve webovém prohlížeči, které přesvědčují k instalaci dodatečné aplikace do chytrého telefonu klienta. Další možností jak škodlivý kód do telefonu nahrát je pomocí falešných SMS zpráv. Tyto zprávy obsahují odkaz na internetové stránky, kde je možno příslušnou aplikaci stáhnout. Nemusí se přitom nutně jednat o aplikaci související s internetovým bankovnictvím, jak dokazuje například zneužití jmen společností Seznam, Facebook, Alza[46] a DHL[47]. Kromě dodatečných bezpečnostních aplikací se tedy objevují aplikace pro sledování zásilky nebo falešné antivirové aplikace.

Tato metoda útoku se též nazývá MITP, což je zkrátka anglického názvu Man-In-The-Phone. Podrobnější popis průběhu a jeho následků je popsán v předcházející kapitole.

6.5.2. SIM SWAP FRAUD útok

Další útok, který ohrožuje tento způsob přenosu OTP je označován jako SIM SWAP FRAUD. Princip útoku SIM SWAP FRAUD je ve své podstatě velmi jednoduchý. Útočník, vydávající se za napadeného klienta požádá u telefonního operátora o zablokování SIM karty, s odůvodněním, že došlo ke ztrátě telefonu nebo poškození originální karty. Poté, co je originální karta zablokována, je vydána nová, kterou ovšem obdrží útočník, který následné může provést libovolnou transakci, jelikož telefonní číslo, na které mají být SMS zprávy obsahující autorizační kód posílány, je stejné. Údaje pro přístup do internetového bankovnictví mohou být útočníkem získány buď pomocí falešné internetové stránky, nebo s využitím phishingu. Aby se mohl útočník za klienta

[46] ALZA.CZ. *Alza.cz varuje před podvodnými SMS* [online]. 2017 [cit. 2017-03-04]. Dostupné z: https://www.alza.cz/alzacz-varuje-pred-podvodnymi-sms-

[47] ČSOB. *Na klienty ČSOB cílí podvodná mobilní aplikace pod hlavičkou společnosti DHL* [online]. 2017 [cit. 2017-03-04]. Dostupné z: https://www.csob.cz/portal/-/n171402b

úspěšně vydávat, je nutné zjistit o něm co nejvíce informací. Tomu se opět využívá phishing.

Tento útok na klienty internetového bankovnictví byl úspěšně proveden například ve Velké Británii.[48]

6.5.3. Další příklady ohrožení

Velmi rozšířené jsou také útoky zneužívající sociální sítě, například Facebook. Útočník se vydává za přítele klienta, na něhož zaměřil své aktivity. Přesvědčí ho k zapůjčení menší částky a odkáže ho na podvodnou webovou stránku, pomocí níž získá přístupové údaje do internetového bankovnictví. Následně je klient přemluven i k přeposlání potvrzovacího kódu. Tento potvrzovací kód však autorizuje vyšší částku, než jaká byla avizována.

Jako další hrozby je možné uvést také krádež telefonu klienta či přístup bez jeho vědomí, pomocí nichž může útočník přístup k SMS zprávám získat také. Vzhledem k faktu, že útoky mířící na klienty internetového bankovnictví cílí na stovky či tisíce klientů není tento způsob z pohledu útočníků praktický. Navíc při ztrátě telefonu klient danou skutečnost ohlásí bance a ta následně znemožní dané telefonní číslo užívat.

[48] BRIGNALL, Miles. THE GUARDIAN. *Sim-swap fraud claims another mobile banking victim* [online]. 2016 [cit. 2017-02-15]. Dostupné z: https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraudsters

7. Alternativy za OTP zasílaný SMS zprávou

Vzhledem ke skutečnostem, že potvrzování transakcí prováděných přes internet formou jednorázových kódů zasílaných SMS zprávami přestává být dostatečně bezpečné, jsou vyvíjeny snahy o nahrazení této formy autorizace bezpečnější metodou. V současné době se nejvíce hovoří o zabezpečení s využitím biometrie, která identifikuje člověka na základě jeho fyzických rysů. Kromě biometrie ovšem existují i jiné možnosti zabezpečení, jimiž jsou QR kódy nebo tzv. potvrzovací aplikace.

7.1. QR kód

7.1.1. Popis QR kódu

Označení QR je zkratkou anglického Quick Response, což v překladu znamená rychlá reakce či rychlá odezva. QR kód je jakýmsi následovníkem známého čárového kódu, ačkoliv se používají oba kódy. Oproti čárovému kódu dokáže QR kód uchovávat mnohem větší množství informací. Struktura QR kódu se skládá ze čtvercové mřížky. Jednotlivá pole mřížky mají buď černou, nebo bílou barvu. Černá symbolizuje logickou jedničku a bílá logickou nulu. Kódy jsou definovány ve čtyřiceti verzích, což udává stejný počet možných velikostí čtvercové mřížky. Mřížka je pak určena verzí vynásobenou čtyřmi a přičtením čísla sedmnáct.

QR kód se rozděluje na geometrickou a informační vrstvu. Geometrická vrstva slouží k definici pozic, z nichž jsou čteny bity obsahující informaci. Geometrická vrstva se skládá z tzv. tiché zóny šířky čtyři a obklopuje celý kód. Dále jsou jeho součástí tři Finders umístěné v rozích kódu. Finders určují velikosti bodů (čtverečků) kódu. Finders mají velikost 7x7. Dále obsahují vnitřní obvod velikosti 5x5 bílé barvy a vnitřní čtverec velikosti 3x3 černé barvy. Od zbytku kódu jsou odděleny tzv. proužkem šířky jedna. Celkově má tedy Finders velikosti 8x8 bodů. Obsaženy jsou také dvě linie, které se nacházejí mezi Finders. V těchto liniích se pravidelně střídá pozice s bílou a černou barvou. Informační vrstva QR kódu obsahuje již samotnou přenášenou informaci.

QR kód je možno nasnímat pomocí čtečky či fotoaparátu v chytrém telefonu nebo tabletu, k přečtení QR kódu a získání přenášené informace musí být ovšem dané zařízení vybaveno příslušnou aplikací.

QR kódy jsou využívány například k platbám, označení a evidenci zboží či pro přenos odkazů na webové stránky. QR kódy je standardizovány předpisem ISO 18004.[49] Pro účely plateb jsou QR kódy, přesněji jejich formát, standardizovány Českou bankovní asociací.[50] Zmíněný standard, obsahující i varianty QR kódu použitelného pro daný účel, je přiložen na datovém CD v souboru ve formátu *.pdf.

Obrázek 5: Ukázka QR kódu s velikostí mřížky 33x33. Zdroj: WIKIPEDIA, THE FREE ENCYCLOPEDIA. *QR code* [online]. [cit. 2017-02-18]. Dostupné z: https://en.wikipedia.org/wiki/QR_code

7.1.2. Využití v bankovnictví

QR kódy nejsou v bankovnictví úplnou novinkou. Jsou využívány jako prostředek pro placení ať už faktur či obyčejných plateb. Tento způsob placení se označuje jako QR platba. Po nasnímání a přečtení kódu jsou údaje o platbě automaticky vyplněny do formuláře.

[49] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 18004:2015: Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification* [online]. [cit. 2017-03-04]. Dostupné z: https://www.iso.org/standard/62021.html

[50] ČESKÁ BANKOVNÍ ASOCIACE. *Standard - Formát pro sdílení platebních údajů v rámci tuzemského platebního styku v CZK prostřednictvím QR kódů* [online]. 2015 [cit. 2017-03-04]. Dostupné z: https://www.czech-ba.cz/cs/standard-format-pro-sdileni-platebnich-udaju-v-ramci-tuzemskeho-platebniho-styku-v-czk-prostrednictvim-qr-kodu

Jako prostředek pro potvrzování transakcí na internetu je QR v současnosti již používán. Jedná se o součást mobilní aplikace Smart klíč, který je nabízen bankou ČSOB. QR kód se v této aplikaci používá v případě tzv. offline režimu, kdy není dostupné mobilní připojení k internetu. QR kód vygenerovaný v internetovém prohlížeči postačí nasnímat chytrým telefonem a aplikace Smart klíč následně zobrazí autorizační kód transakce, který je zadán do příslušného pole ve formuláři. QR kód je také možno využít pro přihlašování do internetového bankovnictví. Po potvrzení přihlašovacích údajů je zadán zjištěný řetězec do příslušného pole a potvrzen. QR kódy podporuje řada Smartbankingových aplikací.

7.2. Potvrzovací aplikace

Potvrzovací aplikace, známá také pod označení PUSH notifikace, je metoda autorizace, která umožňuje potvrzování operací, zadaných v internetovém bankovnictví přes chytrý telefon nebo tablet. Klient si do příslušného zařízení instaluje aplikaci, která danou funkcionalitu umožňuje. Aplikace pro svou funkčnost potřebuje kromě telefonu či tabletu další dvě základní věci. Tou první je dostupné mobilní připojení k internetu. Za druhé je potřeba povolit aplikaci v prostředí internetového bankovnictví.

Pokud chce klient v internetovém bankovnictví provést nějakou transakci, v mobilní aplikaci se objeví upozornění s příslušným zněním. K dokončení transakce zcela postačuje pouze její potvrzení. Velmi zjednodušeně řečeno lze říci, že tyto aplikace pracují na principu dialogu s volbou odpovědi Ano/Ne. Tímto způsobem lze také kontrolovat přihlašování do internetového bankovnictví. Potvrzovací aplikace mají výhodu v tom, že umožňují klientovi autorizovat transakce pohodlným a jednoduchým způsobem. Klient banky nemusí zdlouhavě přepisovat žádný potvrzovací kód.

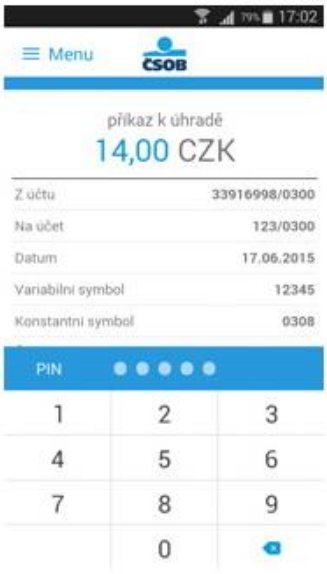
Důvod užívání této metody autorizace v bankovní sféře iniciovaly útoky na služby internetového bankovnictví s cílem získat SMS zprávy s autorizačními OTP kódy v chytrých telefonech klientů.

7.2.1. Potvrzovací aplikace ČSOB Smart klíč

ČSOB Smart klíč je potvrzovací aplikace nabízená klientům banky ČSOB od září roku 2015. Užívání aplikace záleží čistě na volbě klienta. Pokud se rozhodne pro jeho používání, je po jeho aktivaci automaticky znemožněna autorizace pomocí SMS zpráv.

Pro využívání je nutno si aplikaci pro příslušný operační systém chytrého telefonu stáhnout z oficiálního obchodu. Aktivace se provede v internetovém bankovnictví v sekci Nastavení. Po přijmutí SMS kódu, který je zadán do příslušného pole v prohlížeči dojde k vygenerování aktivačního kódu. Ten je zadán do aplikace Smart klíč. Posledním krokem je volba pětimístného PIN kódu, pomocí kterého budou transakce autorizovány.

ČSOB Smart klíč je dostupný pro chytré telefony s operačním systémem Android, iOS a Windows Phone.

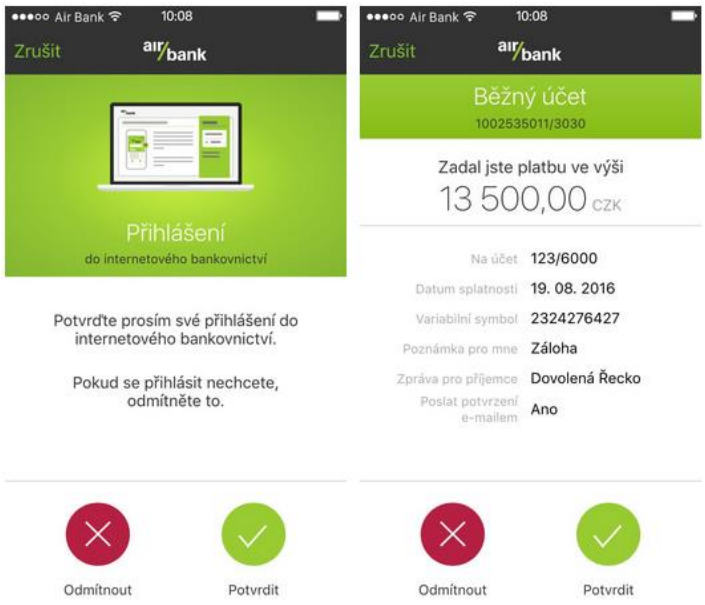


Obrázek 6: Potvrzení příkazu k úhradě v aplikaci ČSOB Smart klíč. Zdroj: DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx

7.2.2. Potvrzovací aplikace Air bank

Aplikaci pro potvrzování transakcí mohou klienti Air bank využívat od srpna 2016. Kromě potvrzování příkazů k úhradě je možno aplikaci využívat i pro potvrzení přihlašování do internetového bankovnictví. Dále umožňuje potvrzovat nastavení inkas či trvalých

plateb. Pro využívání je nutno aplikaci zaregistrovat v internetovém bankovnictví Air bank a následně ji vybrat jako volbu autorizace. Pokud nemá telefon přístup k internetovému připojení, je aplikací pro potvrzení vygenerován kód. Aplikace je pro klienty nabízena zdarma a její zřízení je čistě volbou klienta.



Obrázek 7: Potvrzení přihlášení a transakce v potvrzovací aplikaci Air bank. Zdroj: AIR BANK. *Neradi přepisujete kódy z SMS? Potvrzování bude brzy pohodlnější* [online]. 2016 [cit. 2017-02-25]. Dostupné z: https://www.airbank.cz/novinky/neradi-prepisujete-kody-z-sms-potvrzovani-bude-brzy-pohodlnejsi

7.3. Biometrie

7.3.1. Co je Biometrie?

Biometrie, či biometrické údaje, nebo biometrická data, představují fyzické charakteristiky, pomocí nichž lze jednoznačně identifikovat osobu. Biometrie spadá do kategorie autentizace typu něco jsem. Jedná se o autentizaci založenou na vlastnostech subjektu.

Subjekt lze dle biometrie identifikovat několika způsoby. Patří mezi ně otisky prstů, obraz duhovky a sítnice, obraz krevního řečiště, hlasová analýza, dynamika podpisu či psaní na klávesnici a dále. Pro úspěšné ověření identity za pomoci biometrie je nutno porovnat uložený vzorek se vzorkem získaném v reálném čase.

Biometrické údaje jsou dle §4 odstavce b zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, známějším pod názvem Zákon na ochranu osobních údajů, definovány jako citlivé údaje.[51]

Úspěšné zavedení a používání biometrie jako prostředku zabezpečení souvisí hlavně s jejím zohledněním v rámci systému jako celku a její následné implementaci. Mezi zohledňovanými parametry je například prostředí, kde se bude biometrie využívat, respektive kdo. Je také nutné zvolit adekvátní formu biometrického otisku, na jehož základě se volí odpovídající technika snímání.

7.3.2. Vlastnosti biometrie

Základní vlastnost biometrie spočívá v tom, že ji má daný subjekt vždy u sebe. To je zároveň její největší výhoda. Není potřeba si pamatovat žádné přihlašovací údaje. Biometrie je nepřenositelná na jinou osobu a hrozí tudíž jen malé riziko jejího nezjištěného zcizení, následného okopírování a zneužití. To ovšem neznamená, že to není zcela nemožné.

Při provádění identifikace pomocí biometrie se rozlišuje mezi dvěma pojmy. Identifikací a verifikací. Identifikace představuje porovnání v poměru 1:N, kde se hledá shoda se vzorkem v N šablonách. Verifikace je naopak porovnání v poměru 1:1, kdy se hledá shoda nasnímaného vzorku s konkrétní šablonou. Jinak řečeno je identita, která je předpokládanou identitou. Nalezením shody dojde k potvrzení, že se skutečně jedná o daný subjekt. Identifikace vyžaduje vyšší nároky na výpočet než verifikace.

Přestože identifikace za pomoci biometrie má mnoho předností, nezaručuje stoprocentní spolehlivost. Je proto kombinována s jinými metodami autentizace. Například s čipovou kartou, přístupovými údaji nebo strážným.

[51] ZÁKONY PRO LIDI.CZ. *Zákon č. 101/2000 Sb.: Zákon o ochraně osobních údajů a o změně některých zákonů* [online]. 2016 [cit. 2017-02-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

7.3.3. Vytvoření biometrického otisku

Předpokladem pro vytvoření biometrického vzorku je splnění několika podmínek. Snímaný vzorek musí být měřitelný, jedinečný a v čase neměnný. Požadavky na jeho zpracování spočívají v technické realizovatelnosti a automatizaci jeho snímání a vyhodnocení.

Vytvoření biometrického vzorku je provázeno několika fázemi. Nejprve je pořízen biometrický vzorek. Následuje biometrická charakteristika, představována určujícími informacemi po zpracování. Charakteristiky rozhodující pro identifikaci jsou označované jako biometrické markanty. Jako poslední je vytvořena biometrická šablona, jež představuje výsledek zpracování vzorku. Šablona je uložena pro budoucí porovnání s jiným vzorkem, popřípadě vzorky. Při ukládání biometrické šablony není ukládán celý pořízený vzorek jako takový, ale pouze jeho reprezentace vyjádřená pomocí matematických vzorců. Z výsledné šablony tedy nelze zpětně vytvořit originální otisk.

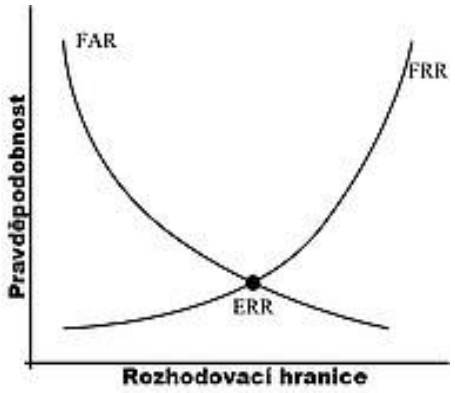
7.3.4. Vyhodnocení biometrické identifikace

Při vyhodnocování biometrické identifikace mohou nastat dva krajní případy. Prvním je chybné přijetí (FAR - False Accept Rate), kdy je neoprávněnému subjektu umožněn přístup.[52] Druhým je chybné odmítnutí (FRR - False Reject Rate), kdy je oprávněné osobě přístup zamítnut.[53] ERR, popřípadě EER (Equal Error Rate) představuje bod, kdy jsou si oba předchozí případy rovny.[54] U FAR a FRR se hledají takové hodnoty, kdy se k sobě přibližují nejvíce.

[52] BIMETRIC LINE. *Biometriky* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/

[53] Tamtéž.

[54] Tamtéž.

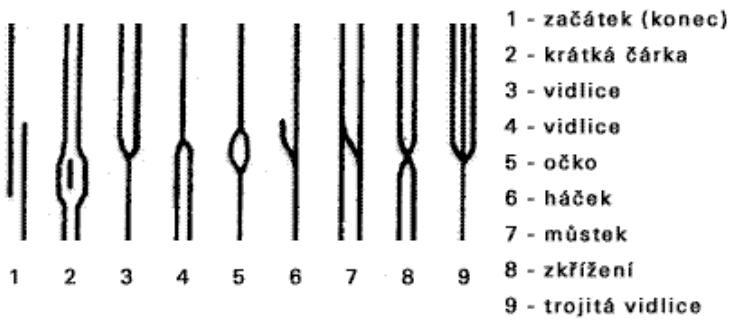


Obrázek 8: Vztah mezi FAR a FRR. Zdroj: BIMETRIC LINE. *Biometriky* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/

7.3.5. Biometrie otisku prstu

Identifikace podle otisků prstů patří mezi nejrozšířenější a nejznámější metody identifikace osoby pomocí biometrických rysů. Zároveň je tato metoda také nejstarší, není-li bráno v úvahu rozpoznávání podle obličeje. Identifikace dle otisků prstů je rozšířena především díky kriminalistice, kde slouží například k identifikaci pachatelů. Kromě policejně soudní oblasti pronikla i do oblasti komerční. Dnes ji lze nalézt například v místech, kam mají přístup jen privilegované osoby nebo v chytrých telefonech.

U otisku prstu se zkoumají podoby uspořádání papilárních linií. Díky vzájemnému křížení, rozvětvování a spojování vytváří tyto linie charakteristický vzor, který je pro každého člověka jedinečný. Otisky prstů jsou po celý život člověka neměnné, což představuje jejich velkou výhodu. Při hledání shody otisků se hledá podobnost v tzv. markantech, což jsou znaky vyznačující se charakteristickou podobou.



Obrázek 9: Příklady papilárních linií otisku prstu. Zdroj: *Obrazce a znaky kůže* [online]. [cit. 2017-02-26]. Dostupné z: http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

Snímače otisků prstů se rozdělují na kontaktní a bezkontaktní. Mezi kontaktní řadíme například optické, elektronické, optoelektronické nebo kapacitní. Druhou třídu snímačů zastupují například ultrazvukové. V chytrých telefonech se vyskytují snímače kapacitní a optické. Nově se objevují i snímače ultrazvukové, které využívají ultrazvukové vlny, porovnávající rozdíl příjmu odraženého signálu.

Optické snímače pracují s obrazem otisku prstu. Při analýze se vyhledávají světlá a tmavá místa. Tato místa jsou představována tzv. hřebeny a prohlubněmi, kterými jsou tvořeny papilární linie. Čím kvalitnější je pořízený snímek otisku, tím je vyšší i přesnost zpracování. Optické snímače jsou ze zmíněných tří typů snímačů nejzranitelnější, jelikož je lze oklamat kvalitně vytištěnou kopií otisku. Další riziko také představuje zanechání otisku na snímači. Z hlediska bezpečnosti užití v bankovnictví, tedy není ideální tento typ snímače využívat.

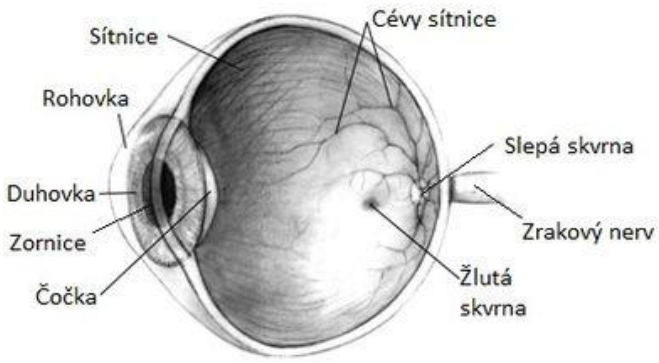
Kapacitní snímače využívají ke své činnosti soustavu kondenzátorů, které měří rozdíl odporu plochy snímače a samotného prstu. Hřebeny na rozdíl od prohlubní přiléhají k ploše snímače a vyznačují se tedy vyšší hodnotou odporu. Přesnost vyhodnocení závisí na počtu použitých kondenzátorů. Platí, že čím více, tím je otisk přesnější. Kapacitní snímače jsou oproti těm optickým mnohem bezpečnější, jelikož reagují na různé materiály různými hodnotami odporu.

7.3.6. Biometrie oka

Lidské oko představuje další část lidského těla, kterou lze použít k jednoznačné identifikaci. U lidského oka lze pro biometrické porovnání použít duhovku nebo sítnici. Jak duhovka, tak sítnice je pro každého člověka jedinečná a je nemožné ji fyzicky změnit.

Při identifikaci pomocí duhovky se po scanu oka zaměřuje pouze na duhovku. Ta je následně mapována do mřížky. Poté je nalezen střed a následně se vypočítá poloměr zornice a duhovky. Čím přesnější je určení souřadnic, tím účinnější je zpracování. Identifikace pomocí sítnice pro určení identity využívá vzory cév. Ke scanu se využívá infračervené záření a kamera, jež nasnímá oko pro zpracování.

Identifikace pomocí biometrie oka se kromě přístupu do zajištěných oblastí využívá i v elektronice. Identifikaci pomocí oční duhovky využívají některé modely chytrých telefonů a tabletů.

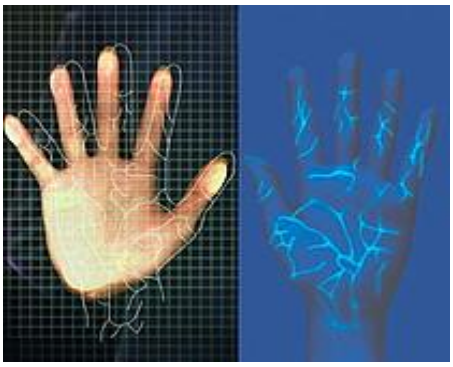


Obrázek 10: Řez lidským okem. Zdroj: WIKISOFIA. *Soustava a funkce smyslových orgánů* [online]. [cit. 2017-02-26]. Dostupné z: https://wikisofia.cz/wiki/Soustava_a_funkce_smyslov%C3%BDch_org%C3%A1n%C5%AF

7.3.7. Biometrie krevního řečiště

Pokud je hovořeno o biometrii krevního řečiště, jedná se o zkoumání podoby cévního systému. Stejně jako otisk prstu nebo lidského oka, je krevní řečiště jedinečné pro každého člověka a lze ho tedy pomocí něho jednoznačně identifikovat.

Otisk krevního řečiště se snímá na dlani nebo prstu. Samotná podoba krevního řečiště je následně získána pomocí infračerveného záření, jež reaguje s krevním barvivem. Výsledkem je jakási mapa, z níž se extrahují informace pro následnou identifikaci. Mezi tyto informace se řadí úhel svíraný žilami, délky jednotlivých úseků, apod. Výsledná informace je jako u všech biometrických metod ukládána v číselné podobě.



Obrázek 11: Mapa krevního řečiště lidské ruky. Zdroj: BIOMETRIC LINE. *Biometriky: Biometrie krevního řečiště* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/

Pro tento způsob autentizace je již nutný speciální hardware, který snímání vzorku pro porovnání umožňuje. Tato možnost se tedy pro běžného uživatele internetového bankovnictví jeví jako méně výhodná z pohledu nákladů, ovšem řadí se mezi ty nejbezpečnější varianty biometrické identifikace. Je zde ovšem velký potenciál využití této biometrické metody u bankomatů.

7.3.8. Současný stav biometrie v bankovnictví

Využití biometrie v bankovnictví za účelem identifikace osoby není úplnou novinkou. Biometrický podpis je užíván v řadě bank při uzavírání smluv. Takto podepsané dokumenty jsou uchovávány v elektronické podobě, což usnadňuje jejich uskladnění namísto papírové evidence. K podepisování slouží zařízení označované jako signpad, kam se klient podepíše speciálním perem. Biometrický podpis užívají například v Moneta Money Bank (dříve GE Money Bank), České spořitelně, ČSOB či Air bank.

Autorizace plateb v rámci internetového bankovnictví pomocí otisku prstu je možná v mobilní aplikaci ČSOB Smart klíč. Prozatím ovšem pouze pro operační systém iOS. Další banky, které umožňují autorizaci plateb otiskem prstu, jsou UniCredit Bank a Fio banka. Obě tak umožňují ve svých smartbankingových aplikacích. Přihlašování do mobilního bankovnictví otiskem prstu umožňují dále Komerční banka, Moneta Money Bank či mBank. Komerční banka umožňuje přihlašování do mobilního bankovnictví jak pro chytré telefony s operačním systémem iOS, tak i pro ty se systémem Android.[55] Česká spořitelna umožňuje otisky prstů využít při přihlašování do aplikace Můj stav, jenž umožňuje sledovat pohyby na účtu klienta.[56] Opět zatím pouze pro operační systém iOS. Z výše uvedeného je patrné, že otisky prstů jako způsob identifikace pronikly nejvíce do oblasti smartbankingu a z větší části je podporují jen zařízení firmy Apple.

[55] KOMERČNÍ BANKA. *Mobilní banka* [online]. [cit. 2017-02-28]. Dostupné z: https://www.kb.cz/cs/prime-bankovnictvi/mobilni-banka/

[56] ČESKÁ SPOŘITELNA. *Můj stav* [online]. [cit. 2017-02-25]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/open_product_200.xml

Obraz krevního řečiště jako metoda identifikace klienta v bankovnictví se využívá hlavně v zahraničí. Mezi země, kde ji bankovní instituce využívají, patří například Polsko (Bank BPH)[57], Turecko (Is Bankasi A.S.)[58], Velká Británie (Barclays)[59] nebo Japonsko (Bank of Kyoto)[60], kde je tato metoda nejrozšířenější. V České republice tato metoda biometrické identifikace prozatím není zavedena.

7.4. Srovnání alternativ za OTP zasílaný SMS zprávou

Následná tabulka obsahuje stručný souhrn klíčových vlastností uvedených alternativ, kterými lze nahradit stávající prostředek autorizace transakcí prováděných pomocí internetového bankovnictví. Pro porovnání jsou uvedeny i vlastnosti samotného OTP zasílaného SMS zprávami. Analýza je brána z pohledu nasazení v chytrém telefonu či tabletu klienta.

[57] ATM MARKETPLACE. *Poland's Bank BPH to roll out finger vein ID solution* [online]. 2012 [cit. 2017-02-26]. Dostupné z: https://www.atmmarketplace.com/news/polands-bank-bph-to-roll-out-finger-vein-id-solution/

[58] Tamtéž.

[59] GOMPERTZ, Simon. BBC. *Bank customers to sign in with 'finger vein' technology* [online]. 2014 [cit. 2017-02-26]. Dostupné z: http://www.bbc.com/news/business-29062901

[60] ATM MARKETPLACE. *Japanese bank to use finger-vein authentication on ATMs* [online]. 2005 [cit. 2017-02-26]. Dostupné z: https://www.atmmarketplace.com/news/japanese-bank-to-use-finger-vein-authentication-on-atms/

Metoda	Silné stránky	Slabé stránky	Příležitosti	Hrozby
OTP	Dostupnost Levné řešení Léty používaná metoda Využit druhý kanál	Závislost na signálu Chyba při opisu		Zcizení SMS Nedostupnost signálu Mobilní malware
QR kód	Generování informace přímo v telefonu Levné řešení Rozšiřitelnost Nezávislé na signálu Udržení druhého kanálu	Jiný způsob předání OTP Závislost na rozlišení při snímání Chyba při opisu	Vhodná alternativa při udržení principu TAN Rozšířenost QR kódů	Podvržení obrazce
Potvrzovací aplikace	Bezpečnost Levné řešení Use friendly Udržení druhého kanálu	Závislost na internetovém připojení Náklady na vývoj aplikace Rozšiřitelnost	Rozšířenost chytrých telefonů a tabletů Kombinace s biometrií	Ztráta, či krádež mobilního zařízení Nedostatečné zabezpečení mobilního zařízení
Biometrie	Bezpečnost Use friendly Malá šance na nezjištěné zcizení Udržení druhého kanálu	Nutný příslušný snímač Pořizovací cena zařízení Důvěra klientů Rozšiřitelnost	Užívaná jak v zahraničí, tak v ČR Nové typy snímačů Vývoj do budoucna	V závislosti na použité metodě

Tabulka 1: Analýza alternativ za OTP zasílaným SMS zprávou v závislosti na nasazení na mobilním zařízení.

Z analýzy je patrné, že každá z uvedených alternativa má své typické rysy a rovněž své výhody a nevýhody. Co se týče cenových nákladů QR kódy i potvrzovací aplikace jsou stejně jako SMS levnou záležitostí. Bráno z pohledu klienta. Fotoaparátem pro snímání QR kódů jsou dnes vybaveny všechny chytré telefony. Klient potřebuje pouze

příslušnou aplikaci na jejich přečtení. Potvrzovací aplikace jsou vytvářeny pro různé operační systémy chytrých telefonů, takže klient nemusí mít nutně nejvýkonnější model na trhu. Musí ovšem disponovat telefonem s operačním systémem, který umožňuje příslušnou aplikaci provozovat. U biometrie ovšem může nastat problém. Různé druhy snímačů užitých v chytrých telefonech pracují na různých principech a ten se odráží na jejich konstrukci a tím i na ceně.

Pokud má být biometrie používána jako nástroj pro autorizaci plateb, je možno ji využít ještě jedním způsobem, ne pouze v chytrých telefonech či tabletech. Lze využít externí snímač připojený k počítači. Jedná se v podstatě o obdobu čtečky pro čipovou kartu s elektronickým certifikátem, který tvoří jednu z nabízených alternativ pro potvrzování transakcí.

Obrázek 12: Externí biometrická čtečka krevního řečiště využívaná britskou bankou Barclays. Zdroj: GOMPERTZ, Simon. BBC. *Bank customers to sign in with 'finger vein' technology* [online]. 2014 [cit. 2017-02-26]. Dostupné z: http://www.bbc.com/news/business-29062901

8.Závěr

OTP kódy zasílané uživatelům internetového bankovnictví jako prostředek autorizace transakcí již neodpovídají dnešním bezpečnostním předpokladům. Přestože se vyskytuje názor, že se stále jedná o bezpečnou metodu autorizace, styl útoku popsaný v této práci dokazuje opak. Vzhledem ke stále větší sofistikovanosti snah útočníků je pro uživatele chytrých telefonů a jiné podobné elektroniky stále těžší a těžší případný útok odhalit. Ještě větší kámen úrazu spočívá v tom, že se vždy nejedná pouze o útoky cílené přímo na oblast online bankovnictví. Je tedy nasnadě, aby jejich majitelé byli více obezřetní v tom, jaké aplikace a z jakých zdrojů si do svého zařízení vkládají. Dále je třeba dbát na dodržování bezpečnostních pravidel, jež jsou uváděna v práci také. Bankovní desatero sice může svým názvem zavádět, ale některé jeho body jsou vztažené k bezpečnosti obecně.

Pokud jsou zhodnoceny všechny alternativy možné náhrady za autorizační SMS uvedené v této práci, lze usoudit následující. QR kódy jsou vhodnou alternativou, pokud se mají OTP stále využívat jako prostředek k autorizaci transakcí. Spíše se ale bude jednat pouze o doplňkovou funkci. Co se týče potvrzovacích aplikací pro chytré telefony jako druhé metody autorizace, je více než pravděpodobné, že do jejich funkcionality bude stále více pronikat biometrická identifikace klienta. Aplikace Smart klíč banky ČSOB uvedená jako příklad je vhodným kompromisem, který stále udržuje dva komunikační kanály pro potvrzování.

Biometrická identifikace bezesporu přináší nejjednoznačnější metodu identifikace klienta. Obzvlášť v případech, kdy je osoba identifikována podle biometrie oka či krevního řečiště. Biometrie oka sice poskytuje oproti otisku prstu jednoznačnou a bezpečnější identifikaci, ovšem je méně komfortní. Otisk prstu se dá pořídit jednoduchým přiložením prstu ke snímači. Biometrie krevního řečiště dozajista najde široké uplatnění v oblasti bankomatů a pravděpodobně i na pobočkách bank, jak je tomu v zahraničí. To ovšem nezáleží pouze na bankách samotných. Klienti musí dané metodě jednoznačně důvěřovat.

S výše uvedenými poznatky je také důležité pozastavit se nad myšlenkou bezpečnost versus použitelnost. Tato skutečnost říká, že čím větší je snaha o maximalizaci bezpečnosti, tím více se může snižovat uživatelský komfort. Příkladem je uváděný autentizační kalkulátor, který sice poskytuje maximální míru bezpečnosti ovšem jeho

používání je poněkud nekomfortní. Je tedy snaha hledat vhodné formy kompromisu mezi bezpečností a použitelností. Tím byly například potvrzovací SMS. S použitelností souvisí i míra schopnosti nasazení v dostatečném rozsahu a za ekonomicky akceptovatelných nákladů. Toto kritérium SMS zprávy stále poskytují.

Jak jde vývoj nových technologií neustále kupředu, je nutné na ně reagovat v dostatečném časovém předstihu. Pokud je uvažováno o biometrické identifikaci, je nutné brát v úvahu jeden klíčový aspekt její rozšiřitelnosti. Tím jsou problémy, které brání jejímu širokému využívání na poli mobilních zařízení. Hlavním je ten, že ne všechna mobilní zařízení disponují biometrickými čtečkami a pokud ano, nemusí se jednat o odpovídající variantu. Klienti také musí bezpodmínečně věřit v ochranu jimi poskytnutých biometrických údajů. Z pohledu uživatelského komfortu se otisk prstu jeví jako správná volba. Naopak biometrická identifikace pomocí oka může představovat problém, například pro osobu nosící brýle.

I přes sebedokonalejší formu autentizace a autorizace se klienti musí mít stále na pozoru a dodržovat zásady bezpečného chování na internetu. Rovněž je nutno dodržovat bezpečnostní zásady dané banky. Ať již bude alternativa jakákoliv, dvě skutečnosti jsou evidentní. Biometrická identifikace má před sebou velkou budoucnost nejen v oblasti bankovnictví a jednorázové OTP kódy představují dozajista uzavřenou kapitolou. Alespoň v oblasti bankovnictví.

.

9. Seznam obrázků a tabulek

9.1. Seznam obrázků

9.2. Seznam tabulek

10. Seznam použitých zdrojů

10.1. Literatura

1. PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy*. 1. Praha: Computer Press, 2000, 166 s. ISBN 80-7226-328-5.
2. MATYÁŠ, Vašek. *Autentizace uživatelů a autorizace elektronických transakcí: příručka manažera = User authentication and electronic transaction authorization: manager's handbook*. Praha: Tate International, 2007. 318 s. Příručka manažera; 8. ISBN 978-80-86813-14-1.
3. DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.
4. BAŠTAN, Petr. Biometrické metody autentizace jsou výhodné. *Computerworld*. 2012, **23**(7), 8-10. ISSN 1210-9924.
5. KARÁSEK, Tomáš. Máme se bát biometrie? *Security magazín*. 2009, **16**(6), 10-11. ISSN 1210-8723.
6. PUŽMANOVÁ, Rita. Biometrické systémy v praxi. *IT Systems*. 2004, **6**(3), 56-58. ISSN 1212-4567.

10.2. Internetové zdroje

7. ADAPTIC. *HTTPS* [online]. [cit. 2016-02-10]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/https/
8. AIR BANK. *Dejte si pozor na falešnou výzvu k instalaci nové mobilní aplikace pro Facebook* [online]. 2016 [cit. 2016-04-01]. Dostupné z: https://www.airbank.cz/novinky/dejte-si-pozor-na-falesnou-vyzvu-k-instalaci-nove-mobilni-aplikace-pro-facebook/
9. AIR BANK. *Air Bank spustila bezpečnější potvrzování plateb bez použití SMS kódů* [online]. 2016 [cit. 2017-02-25]. Dostupné z: https://www.airbank.cz/novinky/air-bank-spustila-bezpecnejsi-potvrzovani-plateb-bez-pouziti-sms-kodu/

10. AIR BANK. *Neradi přepisujete kódy z SMS? Potvrzování bude brzy pohodlnější* [online]. 2016 [cit. 2017-02-25]. Dostupné z: https://www.airbank.cz/novinky/neradi-prepisujete-kody-z-sms-potvrzovani-bude-brzy-pohodlnejsi

11. AIR BANK. *Pohodlnější způsob potvrzování je tady! Takhle si ho nastavíte…* [online]. 2016 [cit. 2016-11-17]. Dostupné z: https://www.airbank.cz/novinky/pohodlnejsi-zpusob-potvrzovani-je-tady-takhle-si-ho-nastavite

12. ALZA.CZ. *Alza.cz varuje před podvodnými SMS* [online]. 2017 [cit. 2017-03-04]. Dostupné z: https://www.alza.cz/alzacz-varuje-pred-podvodnymi-sms-

13. ALPIRO. *Protokol HTTPS* [online]. [cit. 2016-10-02]. Dostupné z: https://www.alpiro.cz/https.html

14. HOŘEJŠÍ, Jaromír. AVAST. *Falešný exekuční příkaz ohrožuje uživatele českých bank* [online]. 2014 [cit. 2016-11-13]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

15. ATM MARKETPLACE. *Poland's Bank BPH to roll out finger vein ID solution* [online]. 2012 [cit. 2017-02-26]. Dostupné z: https://www.atmmarketplace.com/news/polands-bank-bph-to-roll-out-finger-vein-id-solution/

16. ATM MARKETPLACE. *Japanese bank to use finger-vein authentication on ATMs* [online]. 2005 [cit. 2017-02-26]. Dostupné z: https://www.atmmarketplace.com/news/japanese-bank-to-use-finger-vein-authentication-on-atms/

17. JERMÁŘ, Petr. BANKY.CZ. *Raiffeisenbank se stala obětí phishingu* [online]. 2013 [cit. 2016-10-13]. Dostupné z: http://www.banky.cz/raiffeisenbank-se-stala-obeti-phishingu

18. TONAGATTI, Basavaraj. BASU NIVESH. *What is Mobile Phone SIM Swap fraud and how to protect your Bank Account?* [online]. 2015 [cit. 2017-02-14]. Dostupné

z: https://www.basunivesh.com/2015/07/13/what-is-mobile-phone-sim-swap-fraud-and-how-to-protect-your-bank-account/

19. GOMPERTZ, Simon. BBC. *Bank customers to sign in with 'finger vein' technology* [online]. 2014 [cit. 2017-02-26]. Dostupné z: http://www.bbc.com/news/business-29062901

20. BIMETRIC LINE. *Biometriky* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/

21. BIOMETRIC LINE. *Biometriky: Biometrie krevního řečiště* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/

22. BIOMETRIC LINE. *Biometriky: Biometrie otisku prstu* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

23. BIOMETRIC LINE. *Biometriky: Biometrie oka* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

24. BIOMETRIC SOLUTIONS. *Fingerprint Recognition* [online]. [cit. 2017-02-22]. Dostupné z: http://www.biometric-solutions.com/fingerprint-recognition.html

25. ČERMÁK, Miroslav. CLEVER AND SMART. *Autentizace* [online]. 2009, 2012-09-02 [cit. 2016-10-20]. Dostupné z: Autentizace

26. ČERMÁK, Miroslav. CLEVER AND SMART. *Autentizace: biometrické metody* [online]. 2009, 2013-11-15 [cit. 2017-02-22]. Dostupné z: http://www.cleverandsmart.cz/autentizace-biometricke-metody/

27. ČERMÁK, Miroslav. CLEVER AND SMART. *Autorizace transakce v internetovém bankovnictví jednorázovým heslem* [online]. 2011 [cit. 2017-02-09]. Dostupné z: http://www.cleverandsmart.cz/autorizace-transakce-v-internetovem-bankovnictvi-jednorazovym-heslem/

28. ČERMÁK, Miroslav. CEVER AND SMART. *Českem se prohnala další vlna spamu, kdy se útočník vydává za slušného spoluobčana* [online]. 2015, 2015-02-25 [cit. 2015-10-20]. Dostupné z: http://www.cleverandsmart.cz/ceskem-se-prohnala-dalsi-vlna-spamu-kdy-se-utocnik-vydava-za-slusneho-spoluobcana/

29. ČERMÁK, Miroslav. CLEVER AND SMART. *Man in the mobile aneb útok na uživatele internetového bankovnictví* [online]. 2011, 2014-03-26 [cit. 2017-02-14]. Dostupné z: http://www.cleverandsmart.cz/man-in-the-mobile-aneb-utok-na-uzivatele-internetoveho-bankovnictvi/

30. ČERMÁK, Miroslav. CLEVER AND SMART. *Probíhá phishing na klienty internetového bankovnictví ČS* [online]. 2014, 2014-12-13 [cit. 2016-11-03]. Dostupné z: http://www.cleverandsmart.cz/probiha-phishing-na-klienty-internetoveho-bankovnictvi-cs/

31. ČERMÁK, Miroslav. CLEVER AND SMART. *Zrádné smartphony aneb chytré telefony, které vás mohou i zničit* [online]. 2011, 2012-11-18 [cit. 2017-02-14]. Dostupné z: http://www.cleverandsmart.cz/zradne-smartphony-aneb-chytre-telefony-ktere-vas-mohou-i-znicit/

32. ČERMÁK, Miroslav. CLEVER AND SMART. *Zrádné smartphony: spyware* [online]. 2011 [cit. 2017-02-14]. Dostupné z: http://www.cleverandsmart.cz/zradne-smartphony-spyware/

33. WEBSTER, George. CNN. *Biometric ATM gives cash via 'finger vein' scan* [online]. 2010 [cit. 2017-03-04]. Dostupné z: http://edition.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/

34. CO JE TO? *Bankovnictví - Co je to, význam slov, co znamená, termíny, pojmy* [online]. [cit. 2016-07-29]. Dostupné z: http://cojeto.superia.cz/bankovnictvi/

35. CSIRT.CZ. *Podvodné SMS obsahující malware se vydávají za SMS od přepravce* [online]. 2017 [cit. 2017-02-28]. Dostupné z: https://www.csirt.cz/page/3491/podvodne-sms-obsahujici-malware-se-vydavaji-za-sms-od-prepravce/

36. ČESKÁ BANKOVNÍ ASOCIACE. *Standard - Formát pro sdílení platebních údajů v rámci tuzemského platebního styku v CZK prostřednictvím QR kódů* [online]. 2015 [cit. 2017-03-04]. Dostupné z: https://www.czech-ba.cz/cs/standard-format-pro-sdileni-platebnich-udaju-v-ramci-tuzemskeho-platebniho-styku-v-czk-prostrednictvim-qr-kodu

37. ČESKÁ NÁRODNÍ BANKA. *Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví* [online]. [cit. 2016-06-23]. Dostupné z: https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html

38. ČESKÁ SPOŘITELNA. *Autorizace transakce pomocí autorizačních SMS* [online]. [cit. 2017-02-22]. Dostupné z: https://www.servis24.cz/stat/ebanking/s24/help/cs/ib_trn_sms_aut.html

39. ČESKÁ SPOŘITELNA. *Falešný profil na Facebooku nabízející „nový SERVIS 24“.* [online]. 2016 [cit. 2016-10-06]. Dostupné z: https://www.csas.cz/banka/content/inet/internet/cs/sc_17573.xml?archivePage=phishing&navid=nav00156_phishing_aktuality

40. ČESKÁ SPOŘITELNA. *SERVIS 24 - Internetbanking: Pohodlná obsluha a kontrola Vašich financí* [online]. [cit. 2016-08-15]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/open_product_118.xml

41. ČESKÁ SPOŘITELNA. *O nás* [online]. [cit. 2016-08-15]. Dostupné z: https://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=bezpecnost&from=banner_sm_onas

42. ČESKÁ SPOŘITELNA. *O nás: Archiv aktualit* [online]. 2014 [cit. 2016-10-06]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_2066.xml

43. ČESKÁ SPOŘITELNA. *Můj stav* [online]. [cit. 2017-02-25]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/open_product_200.xml

44. ČESKÁ SPOŘITELNA. *Phishing - tiskové zprávy a aktuality* [online]. [cit. 2016-08-15]. Dostupné z: https://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=phishing

45. ČESKÁ SPOŘITELNA. *Stručně o phishingu* [online]. [cit. 2016-10-06]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/strucne-o-phishingu-d00014563

46. ČESKÁ SPOŘITELNA. *Vaše dotazy - Phishing* [online]. [cit. 2016-10-06]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/vase-dotazy---phishing-d00014587

47. ČESKÁ SPOŘITELNA. *SERVIS 24 - Internetbanking: Vaše dotazy - SERVIS 24 Internetbanking* [online]. [cit. 2017-02-14]. Dostupné z: https://www.csas.cz/banka/nav/osobni-finance/servis-24---internetbanking/vase-dotazy---servis-24-internetbanking-d00020073

48. ČESKÁ SPOŘITELNA. *Zásady bezpečného používání Internetbankingu* [online]. [cit. 2016-10-06]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/sc_2634.xml

49. ČESKÁ SPOŘITELNA. *Zabezpečení služby SERVIS 24 Internetbanking* [online]. [cit. 2016-10-06]. Dostupné z: https://www.servis24.cz/stat/ebanking/s24/help/cs/ib_hlp_gen_tech_security.html

50. ČESKÁ POŠTA. *Česká pošta upozorňuje klienty na podvodný email* [online]. 2013 [cit. 2016-10-24]. Dostupné z: https://www.ceskaposta.cz/-/ceska-posta-upozornuje-klienty-na-podvodny-email

51. ČESKÁ POŠTA. *Phishingové útoky na Českou poštu neustávají* [online]. 2013 [cit. 2016-10-24]. Dostupné z: https://www.ceskaposta.cz/-/phishingove-utoky-na-ceskou-postu-neustavaji

52. ČSOB. *Obsluha klientů na pobočkách ČSOB se mění. Nově lze vše vyřídit bezpapírově* [online]. 2016 [cit. 2017-02-26]. Dostupné z: https://www.csob.cz/portal/o-csob/o-csob-a-kbc/servis-pro-media/tiskove-zpravy/-/asset_publisher/5FasXY5AUiLR/content/id/2484023

53. ČSOB. *Nástrahy při obnově hesla do bankovnictví* [online]. 2016 [cit. 2016-10-10]. Dostupné z: https://www.csob.cz/portal/-/n160418?redirect=%2Fportal%2Fbezpecnost%3Fic1%3DHP-CSOB~Pojisteni-internetovych-rizik~D-Banner

54. ČSOB. *Demo služby ČSOB InternetBanking 24* [online]. [cit. 2016-08-16]. Dostupné z: https://maintenance.csob.cz/swf/ib24-demo-2011-11.swf

55. ČSOB. *ČSOB Smart Klíč* [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/csob-smart-klic

56. ČSOB. *InternetBanking 24 Celá banka ve vašem počítači* [online]. [cit. 2016-08-16]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking-24

57. ČSOB. *InternetBanking 24 Celá banka ve vašem počítači* [online]. [cit. 2016-08-16]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking-24#vse-o-sluzbe

58. ČSOB. *InternetBanking 24 Celá banka ve vašem počítači.* [online]. [cit. 2016-08-16]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/internetbanking-24#zabezpeceni

59. ČSOB. *InternetBanking 24 Celá banka ve vašem počítači: ČSOB InternetBanking 24 – příručka.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/documents/10710/36574/csob-ib24-prirucka-zkrac.pdf

60. ČSOB. *ČSOB Smart Klíč.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.csob.cz/portal/lide/produkty/internetove-a-mobilni-bankovnictvi/csob-smart-klic

61. ČSOB. *ČSOB si posvítila na naše zlozvyky: Heslo do online bankovnictví si aktivně nemění většina z nás* [online]. 2016 [cit. 2016-12-18]. Dostupné z: https://www.csob.cz/portal/o-csob/o-csob-a-kbc/servis-pro-media/tiskove-zpravy/-/asset_publisher/5FasXY5AUiLR/content/id/1698538

62. ČSOB. *Na klienty ČSOB cílí podvodná mobilní aplikace pod hlavičkou společnosti DHL* [online]. 2017 [cit. 2017-03-04]. Dostupné z: https://www.csob.cz/portal/-/n171402b

63. ČSOB. *Téměř miliarda zařízení s Androidem je v ohrožení* [online]. 2016 [cit. 2016-10-10]. Dostupné z: https://www.csob.cz/portal/bezpecnost/-/asset_publisher/unK5J9Pd3Nap/content/n160812?inheritRedirect=false&redirect=%2Fportal%2Fbezpecnost%3Fic1%3DHP-CSOB~Pojisteni-internetovych-rizik~D-Banner

64. ČSOB. *Zásady bezpečného užívání elektronického bankovnictví* [online]. [cit. 2016-11-12]. Dostupné z: https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi

65. ČSOB. *Zabezpečení počítače a mobilních zařízení* [online]. [cit. 2016-11-12]. Dostupné z: https://www.csob.cz/portal/bezpecnost/zabezpeceni-pocitace-a-mobilnich-zarizeni

66. CT24. *Falešné e-maily s logem České pošty jako součást obří kriminální akce* [online]. 2013 [cit. 2016-12-18]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/1076886-falesne-e-maily-s-logem-ceske-posty-jako-soucast-obri-kriminalni-akce

67. ČESKÝ ROZHLAS. *Nový vir ohrožuje internetové bankovnictví. Hackeři cílí hlavně na chytré mobily* [online]. 2014 [cit. 2016-11-03]. Dostupné z: http://www.rozhlas.cz/zpravy/technika/_zprava/novy-vir-ohrozuje-internetove-bankovnictvi-hackeri-cili-hlavne-na-chytre-mobily--1337706

68. SEDLÁK, Jan. E15.CZ. *Virus zneužívající Českou poštu napadal velké tuzemské banky* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://e-svet.e15.cz/internet/virus-zneuzivajici-ceskou-postu-napadal-velke-tuzemske-banky-1019128

69. JAVŮREK, Karel. E15.CZ. *10 biometrických technologií, které vás identifikují* [online]. [cit. 2017-02-22]. Dostupné z: http://vtm.e15.cz/aktuality/10-biometrickych-technologii-ktere-vas-identifikuji

70. ERASVĚT. *Era testuje biometrické podpisy* [online]. 2015 [cit. 2017-02-26]. Dostupné z: https://www.erasvet.cz/informace-z-ps/pro-media/stranky/tz150219.aspx

71. ERASVĚT. *Obětí phishingu a škodlivých virů přibývá* [online]. 2015 [cit. 2016-10-20]. Dostupné z: https://www.erasvet.cz/informace-z-ps/pro-media/stranky/tz150115.aspx

72. ESET. *ESET odhalil trojana, který ohrožoval klienty českých bank* [online]. 2013 [cit. 2016-12-18]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-odhalil-trojana-ktery-ohrozoval-klienty-ceskych-bank/

73. EXEKUTORSKÁ KOMORA ČESKÉ REPUBLIKY. *Exekutorská komora varuje před podvodnými e-maily vyzývajícími k úhradě dluhu* [online]. 2015 [cit. 2017-03-01]. Dostupné z: http://www.ekcr.cz/1/aktuality-pro-media/2060-exekutorska-

komora-varuje-pred-podvodnymi-e-maily-vyzyvajicimi-k-uhrade-dluhu-19-10-2015?w=

74. FEEDIT.CZ. *Trojan Asacub cílí skrze Android na finance obětí* [online]. 2016 [cit. 2016-10-20]. Dostupné z: http://www.feedit.cz/wordpress/2016/01/26/trojan-asacub-cili-skrze-android-na-finance-obeti/

75. FINEXPERT.CZ. *Hackeři zneužili aplikaci TrustPort Mobile Security při útoku na ČS* [online]. 2014 [cit. 2016-11-13]. Dostupné z: http://finexpert.e15.cz/hackeri-zneuzili-aplikaci-trustport-mobile-security-pri-utoku-na-cs

76. ŠEDÝ, Pavel. FINEXPERT.CZ. *Do banky přes internet* [online]. 2008 [cit. 2017-02-18]. Dostupné z: http://finexpert.e15.cz/do-banky-pres-internet

77. ONDRÁČKOVÁ, Kamila. FINEXPERT.CZ. *ČSOB spouští novou službu ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://finexpert.e15.cz/csob-spousti-novou-sluzbu-csob-smart-klic

78. FINANCE.CZ. *Přímé bankovnictví* [online]. [cit. 2016-07-31]. Dostupné z: http://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

79. DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx

80. DUSOVÁ, Veronika. FINPARÁDA. *Fio banka nabízí nově svým klientům správu peněz pomocí otisku prstu* [online]. 2015 [cit. 2017-02-26]. Dostupné z: http://www.finparada.cz/2864-Fio-banka-nabizi-nove-svym-klientum-spravu-penez-pomoci-otisku-prstu.aspx

81. BUBÁK, Zdeněk. FINPARÁDA. *Air Bank zavedla potvrzování plateb bez opisování kódu ze SMS. Nově stačí mobilní aplikace* [online]. 2016 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3835-Air-Bank-zavedla-potvrzovani-plateb-bez-opisovani-kodu-ze-SMS.aspx

82. BUBÁK, Zdeněk. FINPARÁDA. *Mobilní banka od Komerční banky umí jako třetí v ČR číst otisky prstů majitele účtu* [online]. 2015 [cit. 2017-02-25]. Dostupné z:

http://www.finparada.cz/2966-Mobilni-banka-od-Komercni-banky-umi-jako-treti-v-CR-cist-otisky-prstu-majitele-uctu.aspx

83. BUBÁK, Zdeněk. FINPARÁDA. *Otiskem prstu zaplatíte u další banky. UniCredit Bank vylepšila svůj Smart Banking* [online]. 2016 [cit. 2017-02-26]. Dostupné z: http://www.finparada.cz/4097-Otiskem-prstu-zaplatite-u-dalsi-banky.aspx

84. BUBÁK, Zdeněk. FINPARÁDA. *Velké srovnání smartbankingu. Jak můžete ovládat svůj účet z mobilu?* [online]. 2013 [cit. 2016-07-31]. Dostupné z: http://www.finparada.cz/1111-Velke-srovnani-smartbankingu.aspx

85. BUBÁK, Zdeněk. FINPARÁDA. *QR kód - nový pomocník při placení. U které banky jej můžete použít?* [online]. 2014 [cit. 2017-02-22]. Dostupné z: http://finparada.cz/1819-QR-kody-novy-pomocnik-pri-placeni.aspx

86. BUBÁK, Zdeněk. FINPARÁDA. *Smart klíč - nový bezpečnostní prvek internetového bankovnictví UniCredit Bank* [online]. 2014 [cit. 2017-02-28]. Dostupné z: http://www.finparada.cz/1887-Smart-klic-novy-bezpecnostni-prvek-Internetoveho-bankovnictvi-UniCredit-Bank.aspx

87. FIO BANKA. *Historie společnosti.* [online]. [cit. 2016-08-16]. Dostupné z: https://www.fio.cz/o-nas/fio-banka/historie

88. FIO BANKA. *Internetbanking: Zabezpečení* [online]. [cit. 2016-08-16]. Dostupné z: https://www.fio.cz/bankovni-sluzby/internetbanking/zabezpeceni

89. FIO BANKA. *Internetbanking: Funkce internetbankingu* [online]. [cit. 2016-08-16]. Dostupné z: https://www.fio.cz/bankovni-sluzby/internetbanking/funkce

90. FIO BANKA. *Funkce Smartbankingu* [online]. [cit. 2017-02-28]. Dostupné z: https://www.fio.cz/bankovni-sluzby/smartbanking/funkce

91. VALÁŠEK, Michal. HOSPODÁŘSKÉ NOVINY. *Hesla na jedno použití: Nejsnadnější způsob, jak lépe chránit svoje data* [online]. 2014 [cit. 2017-02-14]. Dostupné z: http://tech.ihned.cz/pocitace/c1-63119170-bezpecnejsi-internet-dvoufazova-autentizace

92. MONIOVÁ, Eva. IDNES.CZ. *Platnost vašeho hesla brzy vyprší, navždy. Banky sázejí na biometrii* [online]. 2016 [cit. 2017-02-26]. Dostupné z:

http://ekonomika.idnes.cz/banky-zacinaji-k-zabezpeceni-uctu-pouzivat-biometricke-prvky-p6k-/test.aspx? c=A160622_090837_test_nio

93. MONIOVÁ, Eva. IDNES.CZ. *Proudění krve v ruce jako identifikátor k účtu. Zkoušejí ho i české banky* [online]. 2014 [cit. 2017-02-22]. Dostupné z: http://ekonomika.idnes.cz/banka-pin-otisk-ruky-krevniho-reciste-bezpecnost-f7k-/ekonomika.aspx?c=A140916_2099818_ekonomika_skr

94. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 18004:2015: Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification* [online]. [cit. 2017-03-04]. Dostupné z: https://www.iso.org/standard/62021.html

95. KOMERČNÍ BANKA. *Bezpečnost* [online]. [cit. 2016-11-03]. Dostupné z: https://www.kb.cz/bezpecnost/index.shtml

96. KOMERČNÍ BANKA. *Bezpečnost: Desatero bezpečnosti* [online]. [cit. 2016-11-03]. Dostupné z: https://www.kb.cz/bezpecnost/desatero-bezpecnosti/index.shtml

97. KOMERČNÍ BANKA. *Bezpečnost: Počítač* [online]. [cit. 2016-11-03]. Dostupné z: https://www.kb.cz/bezpecnost/pocitac/index.shtml

98. KOMERČNÍ BANKA. *Bezpečnost: Váš mobil* [online]. [cit. 2016-11-03]. Dostupné z: https://www.kb.cz/bezpecnost/mobil/index.shtml

99. KOMERČNÍ BANKA. *Certifikáty.* [online]. [cit. 2017-03-01]. Dostupné z: https://www.kb.cz/cs/prime-bankovnictvi/certifikaty/vyzvednuti-a-prodlouzeni-certifikatu/

100. KOMERČNÍ BANKA. *Komerční banka zdarma zpřístupnila klientům nejmodernější řešení IBM na ochranu klientů internetového bankovnictví* [online]. 2015 [cit. 2016-11-03]. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/komercni-banka-zdarma-zpristupnila-klientum-nejmodernejsi-reseni-ibm-na-ochranu-klientu-internetoveho-bankovnictvi-1920/

101. KOMERČNÍ BANKA. *Mobilní banka* [online]. [cit. 2017-02-28]. Dostupné z: https://www.kb.cz/cs/prime-bankovnictvi/mobilni-banka/

102. KOMERČNÍ BANKA. *Aktuální hrozby* [online]. [cit. 2016-10-17]. Dostupné z: https://www.kb.cz/bezpecnost/aktualni-hrozby/index.shtml

103.KOMERČNÍ BANKA. *Podezřelá vyskakovací okna na přihlašovacích stránkách nebo po přihlášení do internetového bankovnictví MojeBanka nebo MojeBanka Business* [online]. 2015 [cit. 2016-10-17]. Dostupné z: https://www.kb.cz/bezpecnost/aktualni-hrozby/podezrela-vyskakovaci-okna-na-prihlasovacich-strankach-nebo-po-prihlaseni-do-internetoveho-bankovnictvi-mojebanka-nebo-mojebanka-business-4.shtml

104.KOMERČNÍ BANKA. *Podvodné e-maily – phishing: Podvodné e-maily s přílohami* [online]. 2015 [cit. 2016-10-17]. Dostupné z: https://www.kb.cz/bezpecnost/aktualni-hrozby/podvodne-e-maily-phishing-5.shtml

105.KOMERČNÍ BANKA. *Trusteer rapport - účinná ochrana vašeho prohlížeče* [online]. [cit. 2017-03-01]. Dostupné z: https://www.kb.cz/bezpecnost/klient/index.shtml

106.KREDITKARTA.cz. *Cashback* [online]. [cit. 2016-10-06]. Dostupné z: http://www.kreditkarta.cz/Cashback/

107.KREBS ON SECURITY. *The Limits of SMS for 2-Factor Authentication* [online]. 2016 [cit. 2017-02-15]. Dostupné z: https://krebsonsecurity.com/2016/09/the-limits-of-sms-for-2-factor-authentication/

108.MBANK. *MBank znovu vylepšuje mobilní aplikaci* [online]. 2016 [cit. 2017-02-28]. Dostupné z: https://www.mbank.cz/blog/post,667,mbank-znovu-vylepsuje-mobilni-aplikaci.html

109.MBANK. *Přihlaste se na svém iPhonu do mBank aplikace pomocí Touch ID* [online]. 2016 [cit. 2017-02-28]. Dostupné z: https://www.mbank.cz/blog/post,676,prihlaste-se-na-svem-iphonu-do-mbank-aplikace-pomoci-touch-id.html

110.HÁJKOVÁ, Gabriela. MEŠEC.CZ. *ESET: Za vybrané účty klientů Tesco Bank může asi příloha v podvodném e-mailu* [online]. 2016 [cit. 2016-11-17]. Dostupné z: http://www.mesec.cz/aktuality/eset-za-vybrane-ucty-klientu-tesco-bank-muze-asi-priloha-v-podvodnem-e-mailu/

111.HÁJKOVÁ, Gabriela. MĚŠEC.CZ. *Další phisingový útok, tentokrát na klienty Komerční banky* [online]. 2015 [cit. 2016-10-13]. Dostupné z:

http://www.mesec.cz/aktuality/dalsi-phisingovy-utok-tentokrat-na-klienty-komercni-banky/

112.HÁJKOVÁ, Gabriela. MĚŠEC.CZ. *Další podvodné maily: Věrohodnější a proto více nebezpečné* [online]. 2015 [cit. 2016-10-13]. Dostupné z: http://www.mesec.cz/aktuality/dalsi-podvodne-maily-verohodnejsi-a-proto-vice-nebezpecne/

113.MĚŠEC.CZ. *Internetové bankovnictví: Počátky internetového bankovnictví* [online]. [cit. 2016-08-15]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

114.PIŠTORA, Martin. MĚŠEC.CZ. *Bankovní bezpečnost: Rizika SMS* [online]. 2006 [cit. 2017-02-14]. Dostupné z: http://www.mesec.cz/clanky/bankovni-bezpecnost-rizika-sms/

115.ZÁMEČNÍK, Petr. MĚŠEC.CZ. *Raiffeisenbank: Podvodné lákání přístupu k účtu* [online]. 2007 [cit. 2016-10-13]. Dostupné z: http://www.mesec.cz/clanky/raiffeisenbank-podvodne-lakani-pristupu-k-uctu/

116.DOSKOČILOVÁ, Veronika. MĚŠEC.CZ. *Biometrie v bankovnictví: pro výběr hotovosti přiložíte jen prst* [online]. 2015 [cit. 2017-02-22]. Dostupné z: http://www.mesec.cz/clanky/biometrie-v-bankovnictvi-pro-vyber-hotovosti-prilozite-jen-prst/

117.DOSKOČILOVÁ, Veronika. MĚŠEC.CZ. *Napodobením biometrických údajů můžete přijít o identitu (ROZHOVOR)* [online]. 2016 [cit. 2017-02-22]. Dostupné z: http://www.mesec.cz/clanky/napodobenim-biometrickych-udaju-muzete-prijit-o-identitu-rozhovor/?ic=gallery-sidebar-articles&icc=podari-li-se-nekomu-napodobit-nasi-biometrii-v-podstate-jsme-prisli-o-identitu-rozhovor

118.KŮŽEL, Filip. MOBILMANIA.CZ. *Doporučují jej banky, Google i Facebook. Přesto není zabezpečení přes SMS bezpečné* [online]. 2016 [cit. 2017-02-14]. Dostupné z: http://www.mobilmania.cz/clanky/doporucuji-jej-banky-google-i-facebook-presto-neni-zabezpeceni-pres-sms-bezpecne/sc-3-a-1335137/default.aspx

119.MORAVEC, Petr. MOBILIZUJEME. *Čtečky otisku prstů pod drobnohledem – jak fungují?* [online]. 2016 [cit. 2017-02-22]. Dostupné z: https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji

120.MORAVEC, Petr. MOBILIZUJEME. *Věděli jste, že mobil už dnes můžete odemykat i pomocí ucha?* [online]. 2015 [cit. 2017-02-26]. Dostupné z: https://mobilizujeme.cz/clanky/zorientujte-se-v-biometrii-diky-smartphonum-uz-se-nejedna-o-sci-fi

121.FIŠER, Jakub. MOBILIZUJEME. *Moneta přichází s novou mobilní bankou, co nabídne?* [online]. 2016 [cit. 2017-02-22]. Dostupné z: https://mobilizujeme.cz/clanky/moneta-prichazi-s-novou-mobilni-bankou-co-nabidne

122.MONETA MONEY BANK. *Smart banka* [online]. [cit. 2017-02-28]. Dostupné z: https://www.moneta.cz/lide/prime-bankovnictvi/smart-banka

123.NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *DRAFT NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management* [online]. 2016 [cit. 2017-02-14]. Dostupné z: https://pages.nist.gov/800-63-3/sp800-63b.html

124.NOVINKY.CZ. *Nebezpečný virus se snaží napálit uživatele Seznam.cz Emailu* [online]. 2014 [cit. 2016-11-03]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/339053-nebezpecny-virus-se-snazi-napalit-uzivatele-seznam-cz-emailu.html

125.NOVINKY.CZ. *Podvodníci mění taktiku. Našli novou cestu, jak vybílit lidem účty* [online]. 2015 [cit. 2016-10-10]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

126.NOVINKY.CZ. *Podvodné SMS nepřestávají strašit. Příjemce připraví o peníze* [online]. 2017 [cit. 2017-02-19]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/429797-podvodne-sms-neprestavaji-strasit-prijemce-pripravi-o-penize.html

127.NOVINKY.CZ. *Česká spořitelna varovala před virem, který lidem vysává peníze z účtu* [online]. 2014 [cit. 2016-11-03]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/347018-ceska-sporitelna-varovala-pred-virem-ktery-lidem-vysava-penize-z-uctu.html

128.PENÍZE.CZ. *Cashback: jednoduchý výběr peněz zdarma konečně také v ČR* [online]. 2006 [cit. 2016-09-04]. Dostupné z: http://www.penize.cz/platebni-karty/18345-cashback-jednoduchy-vyber-penez-zdarma-konecne-take-v-cr

129.CHYTILOVÁ, Dana. PENÍZE.CZ. *Česká spořitelna: rušíme bezpečnější Servis 24* [online]. 2006 [cit. 2017-03-07]. Dostupné z: http://www.penize.cz/prime-bankovnictvi/17764-ceska-sporitelna-rusime-bezpecnejsi-servis-24

130.PENÍZE.CZ. *Platební karty* [online]. [cit. 2016-07-31]. Dostupné z: http://www.penize.cz/platebni-karty

131.TŮMOVÁ, Věra. PENÍZE.CZ. *Odkud kam míří český internetbanking* [online]. 2008 [cit. 2016-08-15]. Dostupné z: http://www.penize.cz/prime-bankovnictvi/42614-odkud-kam-miri-cesky-internetbanking

132.QR PLATBA. *Konec přepisování platebních údajů z faktur.* [online]. [cit. 2017-03-04]. Dostupné z: http://qr-platba.cz/

133.QR PLATBA. *Grafický manuál* [online]. [cit. 2017-03-04]. Dostupné z: http://qr-platba.cz/graficky-manual/

134.QIKNI.CZ. *Co je QR kód a jak na něj?* [online]. [cit. 2017-02-22]. Dostupné z: http://www.qikni.cz/qr-kod/

135.RAIFFEISENBANK. *Internetové bankovnictví: Podrobnosti o produktu.*[online]. [cit. 2016-08-15]. Dostupné z: https://www.rb.cz/osobni/ucty-a-bankovnictvi/internetove-bankovnictvi

136.RAIFFEISENBANK. *Podívejte se, jak funguje internetové bankovnictví.* [online]. [cit. 2016-08-17]. Dostupné z: https://www.rb.cz/attachements/demo/

137.RAIFFEISENBANK. *Postup pro ověření komunikace* [online]. [cit. 2016-10-13]. Dostupné z: https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/postup-pro-overeni-komunikace

138.RAIFFEISENBANK. *Bezpečnost internetového bankovnictví* [online]. [cit. 2017-03-04]. Dostupné z: https://www.rb.cz/informacni-servis/doplnkove-informace-k-produktum/bezpecne-bankovnictvi/bezpecnost-internetoveho-bankovnictvi

139.RAIFFEISENBANK. *Internetové bankovnictví* [online]. [cit. 2016-08-15]. Dostupné z: https://www.rb.cz/osobni/ucty-a-bankovnictvi/internetove-bankovnictvi

140.RAIFFEISENBANK. *Aktuality: Nová vlna podvodných emailů* [online]. 2015 [cit. 2016-10-13]. Dostupné z: https://www.rb.cz/o-nas/aktuality/29072015-phishing-2

141.RAIFFEISENBANK. *Aktuality: Upozorňujeme na novou vlnu podvodných emailů* [online]. 2013 [cit. 2016-10-13]. Dostupné z: https://www.rb.cz/o-nas/aktuality/upozornujeme-na-novou

142.RAIFFEISEN - VOLKSBANK TÜßLING UNTERNEUKIRCHEN EG. *Sicherheitshinweise* [online]. [cit. 2017-02-18]. Dostupné z: https://www.rv-banken.de/online-banking/sicherheitshinweis.html

143.ROOT.CZ. *Autorizace v internetovém bankovnictví* [online]. 2006 [cit. 2017-02-14]. Dostupné z: https://www.root.cz/clanky/autorizace-v-internetovem-bankovnictvi/

144.KARÁSEK, Jakub. SMARTMANIA.CZ. *Jak na Lumiiích 950 a 950 XL funguje přihlašování oční duhovkou?* [online]. 2015 [cit. 2017-03-04]. Dostupné z: http://edition.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/

145.SMÉKAL, Marek. SUPERAPPLE.CZ. *Touch ID, nebo kódový zámek?* [online]. 2016 [cit. 2017-02-22]. Dostupné z: https://superapple.cz/2016/05/touch-id-nebo-kodovy-zamek/

146.SVĚT SÍTÍ. *SSL protokol (1) - princip a přínosy* [online]. 2002 [cit. 2016-10-02]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=SSL-protokol-1-princip-a-prinosy-2542002

147.TN.CZ. *Maily pod hlavičkou České pošty obsahovaly vir! Byl to hackerský útok ze 4 zemí* [online]. 2013, 2013-09-05 [cit. 2016-12-18]. Dostupné z: http://tn.nova.cz/clanek/zpravy/zahranici/maily-pod-hlavickou-ceske-posty-obsahovaly-vir-byl-to-hackersky-utok-ze-4-zemi.html

148.TRUSTPORT. *Home Users and Small Companies* [online]. [cit. 2017-03-01]. Dostupné z: http://www.trustport.com/en/home-users

149.BRIGNALL, Miles. THE GUARDIAN. *Sim-swap fraud claims another mobile banking victim* [online]. 2016 [cit. 2017-02-15]. Dostupné z: https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraud

150.UNICREDIT BANK. *O bezpečnosti: Typy bezpečnostních kliče*ů [online]. [cit. 2017-03-04]. Dostupné z: https://www.unicreditbank.cz/cs/obcane/ucty/online-sluzby.html#obezpecnosti

151.UNICREDIT BANK. *Smart Banking* [online]. [cit. 2017-02-28]. Dostupné z: https://www.unicreditbank.cz/cs/obcane/ucty/online-sluzby.html#smartbanking

152.LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – A New, Advanced Banking Trojan in the Wild* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/

153.LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – Technical analysis part 1/2* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/06/hesperbot-technical-analysis-part-12/

154.LIPOVSKY, Robert. WELIVESECURITY. *Hesperbot – technical analysis: part 2/2* [online]. 2013 [cit. 2016-10-24]. Dostupné z: http://www.welivesecurity.com/2013/09/09/hesperbot-technical-analysis-part-22/

155.WIKISOFIA. *Soustava a funkce smyslových orgánů* [online]. [cit. 2017-02-26]. Dostupné z: https://wikisofia.cz/wiki/Soustava_a_funkce_smyslov%C3%BDch_org%C3%A1n%C5%AF

156.WIKIPEDIA, THE FREE ENCYCLOPEDIA. *Biometrics* [online]. [cit. 2017-02-22]. Dostupné z: https://en.wikipedia.org/wiki/Biometrics

157.WIKIPEDIA, THE FREE ENCYCLOPEDIA. *One-time password* [online]. [cit. 2017-02-14]. Dostupné z: https://en.wikipedia.org/wiki/One-time_password

158.WIKIPEDIA, THE FREE ENCYCLOPEDIA. *QR code* [online]. [cit. 2017-02-18]. Dostupné z: https://en.wikipedia.org/wiki/QR_code

159.WIKIPEDIA, THE FREE ENCYCLOPEDIA. *Transaction authentication number* [online]. [cit. 2017-02-14]. Dostupné z: https://en.wikipedia.org/wiki/Transaction_authentication_number

160.WIKIPEDIE OTEVŘENÁ ENCYKLOPEDIE. *Internetové bankovnictví* [online]. [cit. 2016-08-15]. Dostupné z: https://cs.wikipedia.org/wiki/Internetov%C3%A9_bankovnictv%C3%AD

161.WIKIBANKING.NET. *Online banking: pushTAN* [online]. [cit. 2017-02-16]. Dostupné z: http://www.wikibanking.net/onlinebanking/mobilebanking/pushtan/

162.ZÁKONY PRO LIDI.CZ. *Zákon č. 101/2000 Sb.: Zákon o ochraně osobních údajů a o změně některých zákonů* [online]. 2016 [cit. 2017-02-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

163.ZÁKONY PRO LIDI.CZ. *Zákon č. 120/2001 Sb.: Zákon o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů* [online]. 2016 [cit. 2016-11-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2001-120

164.JANŮ, Stanislav. ŽIVĚ.CZ. *Americký úřad varuje: dvouúrovňové ověřování pomocí SMS není bezpečné* [online]. 2016 [cit. 2017-02-14]. Dostupné z: http://www.zive.cz/clanky/americky-urad-varuje-dvouurovnove-overovani-pomoci-sms-neni-bezpecne/sc-3-a-184594/default.aspx

165.ŽIVĚ.CZ. *Internetové bankovnictví v Česku* [online]. 1999 [cit. 2016-08-15]. Dostupné z: http://www.zive.cz/clanky/internetove-bankovnictvi-v-cesku/sc-3-a-9572/default.aspx

166.POLESNÝ, David. ŽIVĚ.CZ. *Falešné e-maily České pošty nesly nový a velmi nebezpečný malware* [online]. 2014 [cit. 2016-10-24]. Dostupné z: http://www.zive.cz/bleskovky/falesne-e-maily-ceske-posty-nesly-novy-a-velmi-nebezpecny-malware/sc-4-a-170448

167.*Obrazce a znaky kůže* [online]. [cit. 2017-02-26]. Dostupné z: http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

11. Seznam použitých zkratek

Zkratka	Plné znění	Význam
PIN	Personal Identification Number	Osobní identifikační číslo
BPIN	Bankovní PIN	
OTP	One-Time-Password	Jednorázové heslo
QR	Quick Response	Rychlá odezva
TAN	Transaction Authentication Number	Ověřovací číslo transakce
mTAN	Mobile TAN	Mobilní TAN
SIM	Subscriber Identity Module	Modul Identity Předplatitele
SMS	Short message service	Služba krátkých textových zpráv
GSM	Groupe Spécial Mobile	Globální Systém pro Mobilní komunikaci
FAR	False Accept Rate	Míra chybného přijetí
FRR	False Reject Rate	Míra chybného odmítnutí
ERR/EER	Equal Error Rate	Míra chybného srovnání
SSL	Secure Sockets Layer	Šifrovací protokol
TLS	Transport Layer Security	Šifrovací protokol
HTTP	Hypertext Transfer Protokol	Protokol pro výměnu hypertextových dokumentů
HTTPs	Hypertext Transfer Protokol Secure	HTTP spolupracující s protokolem SSL/TLS
TCP/IP	Transmission Control Protocol/Internet Protocol	Sada protokolů pro komunikaci v počítačové síti
PDF	Portable Document Format	Přenosný formát dokumentů

Zkratka	Plné znění	Význam
EXE	Executable	Spustitelný
ZIP		Formát pro kompresi dat
Tzv.	Takzvaný	
Apod.	A podobně	

12. Seznam příloh

A. Příklady bankovního desatera

B. Popis QR kódu určeného k platbě

C. Příklad znění podvodného emailu s falešným exekučním příkazem

D. Útok cílený proti Raiffeisenbank malwarem Hesperbot

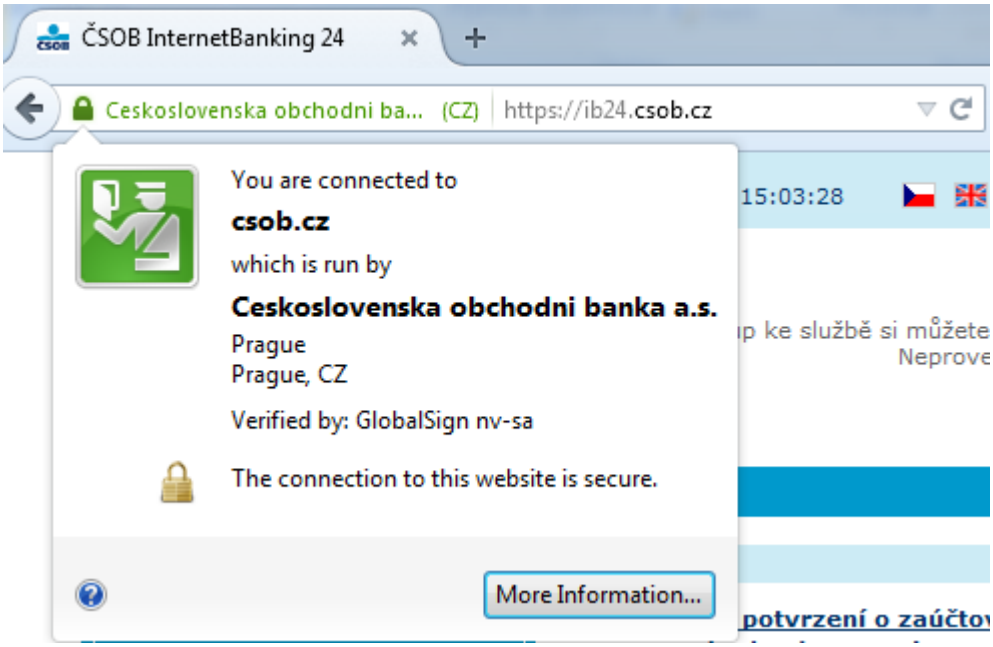
E. Proces potvrzení transakce v aplikaci ČSOB Smart klíč

F. Příklady biometrických snímačů

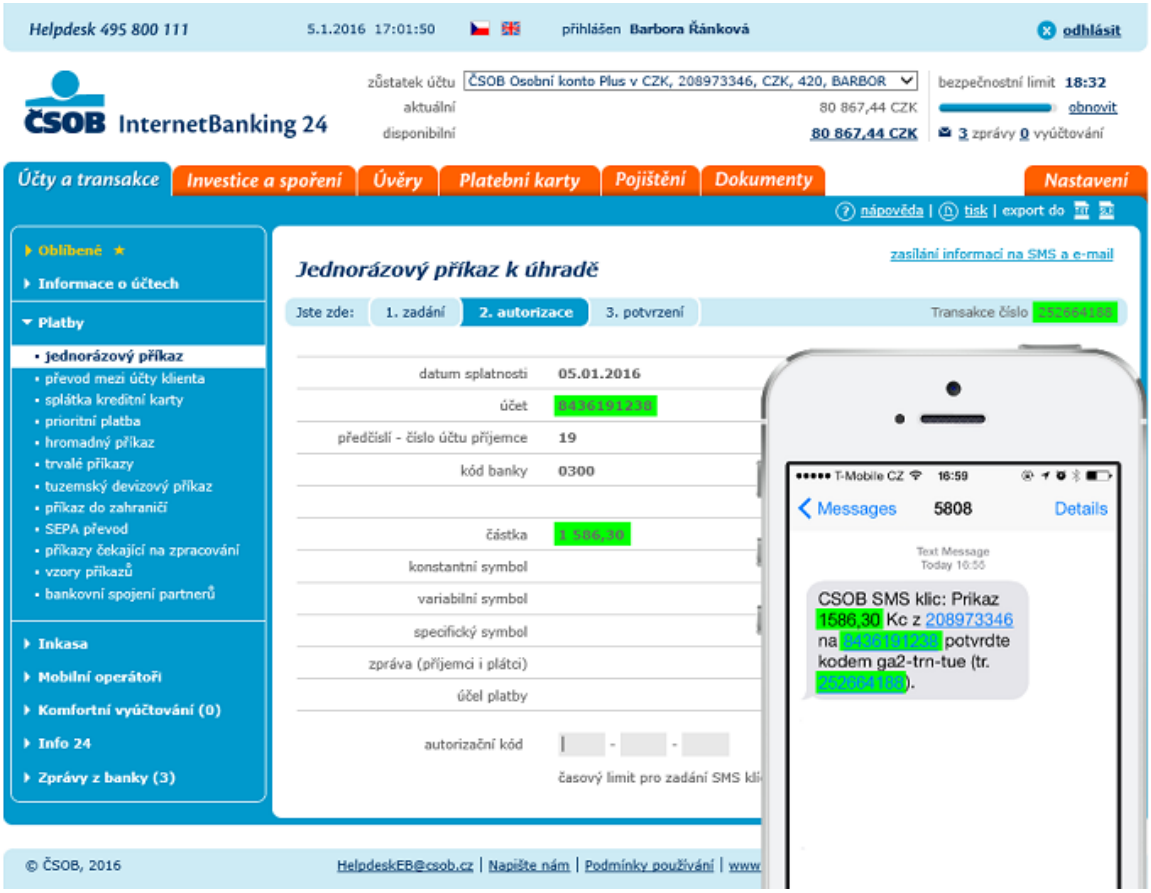
G. Datové CD obsahující:

- Podoba práce ve formátu PDF
- Podoba práce ve formátu XPS
- Standard - Formát pro sdílení platebních údajů v rámci tuzemského platebního styku v CZK prostřednictvím QR kódů, srpen 2015 ve formátu PDF

Příloha A: Příklady bankovního desatera



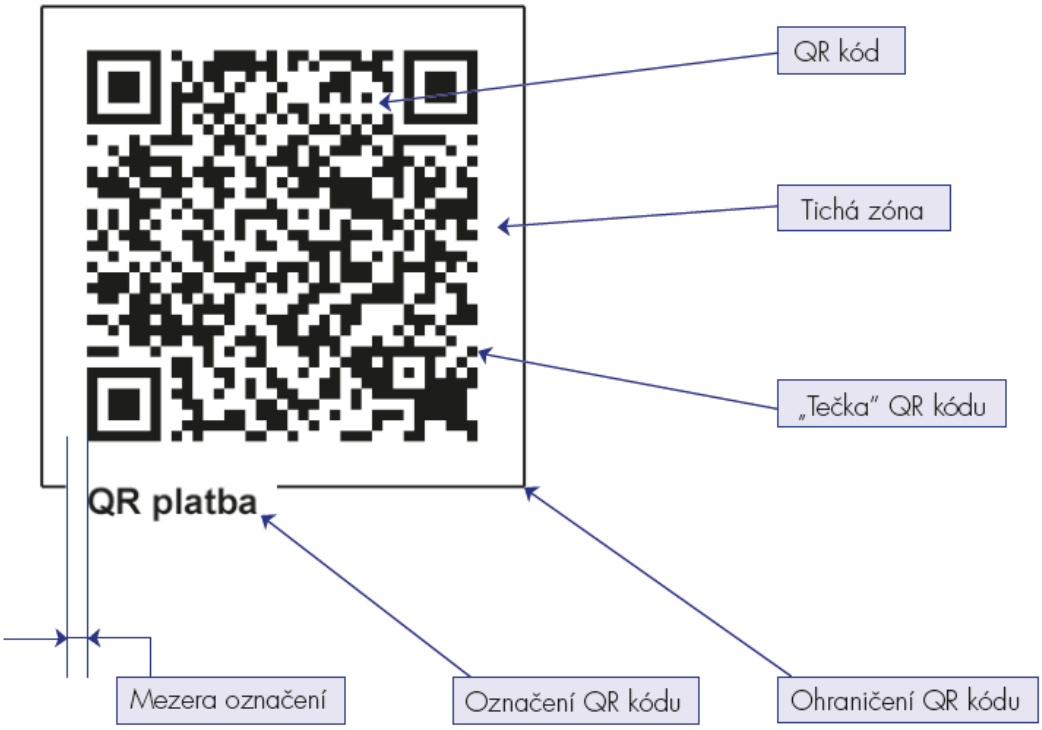
Obr. 1: Kontrola bezpečného spojení s bankou. Zdroj: ČSOB. *Zásady bezpečného užívání elektronického bankovnictví* [online]. [cit. 2016-11-12]. Dostupné z: https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi



Obr. 2: Kontrola údajů před potvrzením platby. Zdroj: ČSOB. *Zásady bezpečného užívání elektronického bankovnictví* [online]. [cit. 2016-11-12]. Dostupné z: https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi

.

Příloha B: Popis QR kódu určeného k platbě



Obr. 3: Popis QR kódu určeného k platbě. Zdroj: QR PLATBA. *Grafický manuál* [online]. [cit. 2017-03-04]. Dostupné z: http://qr-platba.cz/graficky-manual/

Příloha C: Příklad znění podvodného emailu s falešným exekučním příkazem

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

„Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 51736937, se sídlem Kateřinská 13, 184 00 Praha 2 pověřený provedením exekuce: č.j. 10 EXE 197/2014 -17, na základě exekučního titulu: Příkaz č.j. 077209/2014-567/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, jakož i povinnosti uhradit náklady na nařízení exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 9 027,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 167,00 Kč včetně DPH 21% Náklady exekuce paušálem: 4 616,00 Kč včetně DPH 21%

Pro splnění veškerých povinností je třeba uhradit na účet soudního exekutora (č.ú. 549410655/5000, variabilní symbol 82797754, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 14 810,00 Kč

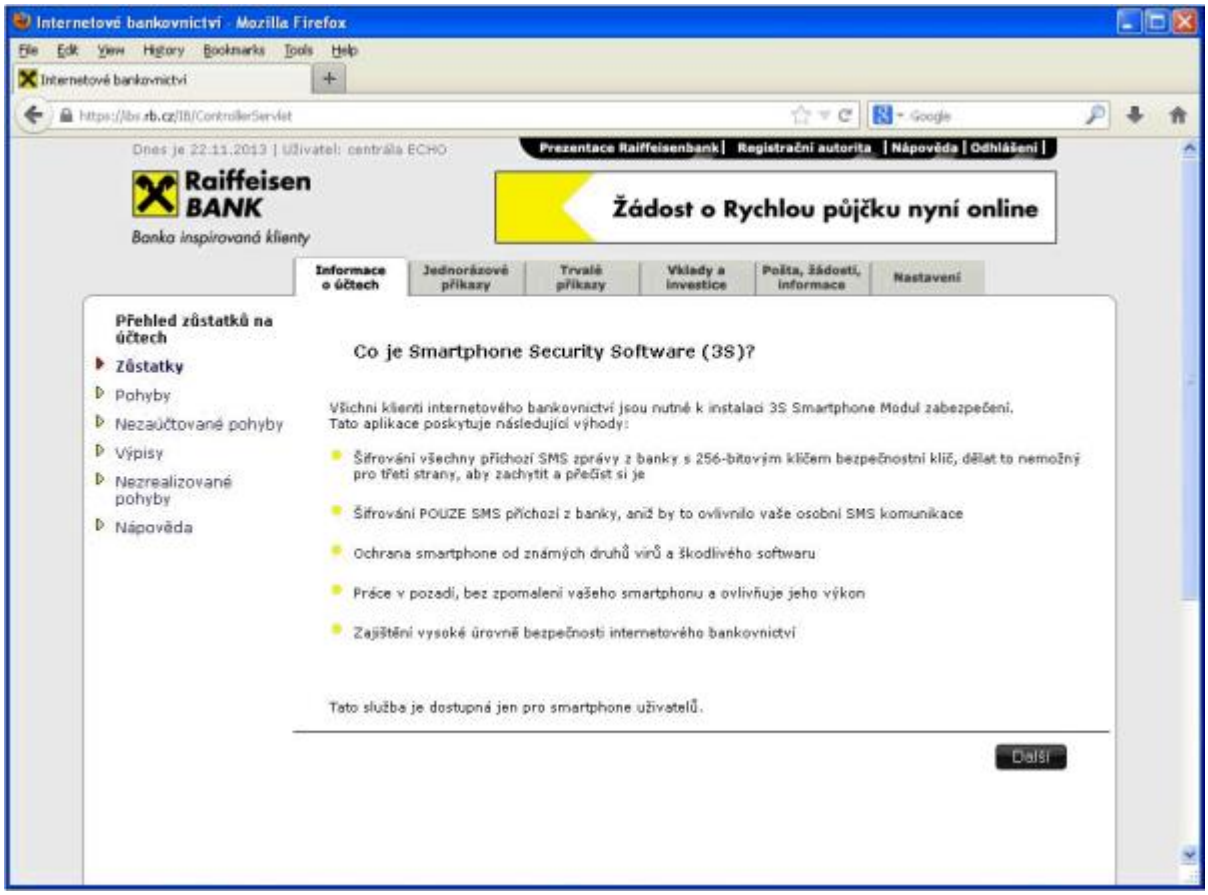
Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Alexey Mishkel“

Zdroj: HOŘEJŠÍ, Jaromír. AVAST. *Falešný exekuční příkaz ohrožuje uživatele českých bank* [online]. 2014 [cit. 2017-03-05]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

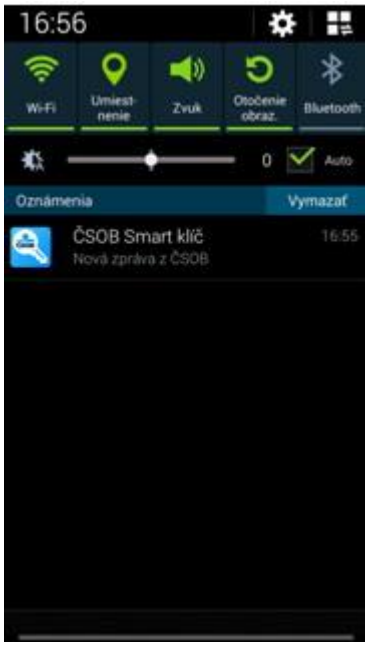
Příloha D: Útok cílený proti Raiffeisenbank malwarem Hesperbot



Obr. 4: Podoba podvržené stránky v internetovém bankovnictví Raiffeisenbank vyzývající k instalaci bezpečnostní aplikace do chytrého telefonu. Zdroj: RAIFFEISENBANK. *Aktuality: Upozorňujeme na novou vlnu podvodných emailů* [online]. 2013 [cit. 2017-03-05]. Dostupné z: https://www.rb.cz/o-nas/aktuality/upozornujeme-na-novou

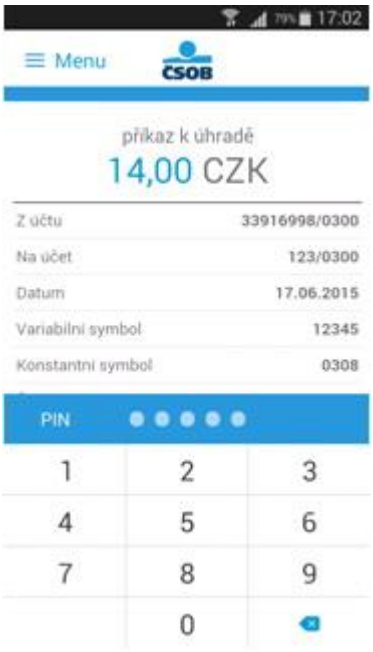
Obr. 5: Podoba emailu oznamující o nevyzvednutí zásilky. Zdroj: RAIFFEISENBANK. *Aktuality: Upozorňujeme na novou vlnu podvodných emailů* [online]. 2013 [cit. 2017-03-05]. Dostupné z: https://www.rb.cz/o-nas/aktuality/upozornujeme-na-novou

Příloha E: Proces potvrzení transakce v aplikaci ČSOB Smart klíč



Obr. 6: Krok 1 - přijetí upozornění o transakci. Zdroj: Zdroj: DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx

Obr. 7: Krok 2 - zobrazení údajů o transakci. Zdroj: DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx



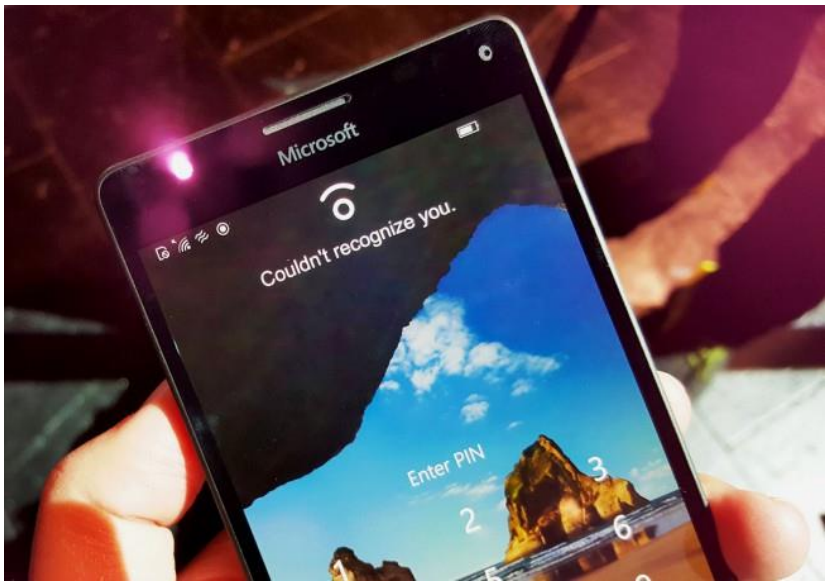
Obr. 8: Krok 3 - potvrzení transakce PIN kódem. Zdroj: DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx

Obr. 9: Krok 4 - dokončení transakce. Zdroj: DUSOVÁ, Veronika. FINPARÁDA. *ČSOB spouští novou autorizační metodu - ČSOB Smart klíč* [online]. 2015 [cit. 2017-02-25]. Dostupné z: http://www.finparada.cz/3025-CSOB-spousti-novou-aurizacni-metodu-CSOB-Smart-klic.aspx

Příloha F: Příklady biometrických snímačů

Obr. 10: Bankomat využívající pro identifikaci biometrické metody krevního řečiště. Zdroj: WEBSTER, George. CNN. *Biometric ATM gives cash via 'finger vein' scan* [online]. 2010 [cit. 2017-03-04]. Dostupné z: http://edition.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/

Obr. 11: Čtečka otisků prstů užívaná v iPhonech firmy Apple. Zdroj: SMÉKAL, Marek. SUPERAPPLE.CZ. *Touch ID, nebo kódový zámek?* [online]. 2016 [cit. 2017-03-04]. Dostupné z: https://superapple.cz/2016/05/touch-id-nebo-kodovy-zamek/



Obr. 12: Smartphone Lumia 950 se zabudovanou čtečkou oční duhovky. Zdroj: KARÁSEK, Jakub. SMARTMANIA.CZ. *Jak na Lumiiích 950 a 950 XL funguje přihlašování oční duhovkou?* [online]. 2015 [cit. 2017-03-04]. Dostupné z: https://smartmania.cz/lumia-950-xl-ctecka-duhovky-prihlasovani-windows-12197/