Masarykova univerzita v Brně

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informační studií a knihovnictví

MAGISTERSKÁ DIPLOMOVÁ PRÁCE

2013 **Anna Růžičková**

Masarykova univerzita v Brně

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informační studií a knihovnictví

Bc. Anna Růžičková

ZNEUŽÍVÁNÍ INTERNETOVÉHO BANKOVNICTVÍ: MEDIÁLNÍ ANALÝZA

Magisterská diplomová práce

Vedoucí práce: PhDr. Pavla Kovářová

2013

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracovala samostatně s využitím uvedených pramenů a literatury.

……...

Podpis autora práce

Poděkování

Na tomto místě bych ráda poděkovala vedoucí práce PhDr. Pavle Kovářové za podnětné rady, připomínky a hlavně trpělivost při vedení práce.

Přátelům, za jejich čas a námahu při konstruktivním kritizování nebo jenom za trpělivost.

A svým blízkým (hlavně Markovi), za výdrž a toleranci.

Bibliografický záznam

RŮŽIČKOVÁ, Anna. *Zneužívání internetového bankovnictví: mediální analýza*. Brno, 2013. 69 s., 15 s. příloh. Diplomová práce. Masarykova univerzita, Filozofická fakulta, Kabinet informačních studií a knihovnictví. Vedoucí práce PhDr. Pavla Kovářová.

Anotace

Diplomová práce *„Zneužívání internetového bankovnictví: mediální analýza“* se skládá ze dvou částí. První část je teoretická, což znamená, že definuje internetové bankovnictví a zabezpečení procesů internetového bankovnictví, např. autentizace. Dále se zabývá útoky na bankovnictví, jako je phishing, malware apod. Na závěr této části popisuje úlohu médií v zobrazování kyberkriminality. Druhá část je praktická, tzn. že popisuje metodologii obsahové analýzy médií, a poté analyzuje a interpretuje výsledná zjištění.

Klíčová slova

internetové bankovnictví, autentizace, autorizace, podvod, kyberkriminalita, phishing, obsahová analýza, internetové zpravodajství

Annotation

Diploma thesis *"Misuse of the Internet banking: the media analysis"* consists of two parts. The first part is theoretical, it means that it defines the internet banking and processes of internet banking security, e.g. authentication. It also deals with the internet banking attacks, like phishing, malware attacks and so one. At the end of theroetical part it describes the role of the media in the displaying of cybercrime. The second section is practical, so it describes the methodology of the content analysis of media and analyses and interprets the final findings.

Keywords

internet banking, authentication, authorization, fraud, cybercrime, phishing, content analysis, internet news

Obsah

Úvod **9**

1. Úvod do internetového bankovnictví **10**

1.1. Procesy internetového bankovnictví 13

1.2. Zabezpečení přístupu do internetového bankovnictví 13

1.2.1. Autentizace 13

1.2.2. Autorizace 16

1.3. Zabezpečení bankovních procesů 17

1.3.1. Zabezpečení autentizace klienta 18

1.3.2. Zabezpečení zpráv 18

1.3.3. Zabezpečení komunikačního kanálu 19

1.3.4. Zajištění bankovního systému proti průnikům do banky 20

1.3.5. Bezpečné chování uživatelů 21

1.4. Trendy v bankovnictví 22

2. Útoky na internetové bankovnictví **25**

2.1. Útok na uživatele 25

2.1.1. Útok na hesla 25

2.1.2. Phishing 26

2.1.3. Pharming 28

2.1.4. Malware 28

2.1.5. Operace High Roller 30

2.2. Útoky proti webovým aplikacím 31

2.2.1. XSS útok 32

2.2.2. Cross-site request forgery 33

2.2.3. Clickjacking 34

2.2.4. HTML Injection 34

2.3. Útok na komunikaci 35

2.3.1. Útok ze středu 35

2.4. Útok na bankovní server 36

2.4.1. Případ Citibank 36

2.4.2. DDoS 37

3. Úloha médií v zobrazování kyberkriminality **38**

3.1 Zpravodajství ... 39
3.1.1 On-line zpravodajství ... 39
3.1.2 Kvalita zpravodajství ... 41
4. Metodologická část ... 42
4.1 Cíl výzkumu ... 42
4.2 Metodologie ... 43
4.2.1 Výběrový soubor ... 43
4.2.2 Kódovací jednotka ... 45
4.2.3 Stanovení výzkumných otázek ... 45
5. Analytická část ... 47
5.1 Počet zpráv ... 47
5.2. Výzkumná otázka č. 1 ... 49
5.2.1. Analýza zpravodajství Novinky.cz ... 49
5.2.2. Analýza zpravodajství iDnes.cz ... 50
5.2.3. Analýza zpravodajství iHNed.cz ... 51
5.2.4. Analýza zpravodajství Aktuálně.cz ... 52
5.2.5. Odpověď na výzkumnou otázku č. 1 ... 52
5.2.6. Dílčí otázky ... 53
5.3. Výzkumná otázka č. 2 ... 54
5.3.1. Odpověď na výzkumnou otázku č. 2 ... 55
5.4. Výzkumná otázka č. 3 ... 55
5.4.1. Odpověď na výzkumnou otázku č. 3 ... 56
5.5. Výzkumná otázka č. 4 ... 57
5.5.1. Odpověď na výzkumnou otázku č. 4 ... 58
Závěr ... 60
Seznam zkratek, obrázků a tabulek ... 62
Použitá literatura ... 64
Přílohy ... 73

Úvod

Internetové bankovnictví je poměrně hodně rozšířenou finanční službou[1]. Její oblíbenost stále roste, ať už přímo internetového bankovnictví, nebo jeho poddruhů, jako např. smartbanking apod. S tím ale zároveň roste příležitost pro podvodníky, kteří se snaží získat finance kriminálním útokem na internetová bankovnictví uživatelů. Ve své práci jsem se zaměřila právě na tyto útoky, kterým mohou být uživatelé vystaveni. Cílem mojí práce je potom vypracování mediální obsahové analýzy. V ní prozkoumám obsahy internetových zpravodajství, popisující tyto útoky, a jejich kvalitu z několika vybraných hledisek. Tyto tato média jsou totiž nezanedbatelným zdrojem informací[2].

Diplomová práce se skládá ze dvou částí: teoretické a praktické. V první části diplomové práce vysvětluji internetové bankovnictví a zařazuji jej do širšího kontextu elektronického bankovnictví, potom popisuji prvky internetového bankovnictví. Jedna kapitola je věnována autentizaci a autorizaci uživatelů, tj. omezení přístupu do aplikace on-line bankingu. Dále jsou zde zobrazeny způsoby zabezpečení jednotlivých bankovních procesů, mj. také chování uživatelů. Zde charakterizuji pravidla bezpečného chování, která by měli uživatelé dodržovat při využívání bankovní aplikace.

V druhé části jsou již přímo vylíčeny útoky na aplikace internetového bankovnictví identifikované v odborné literatuře. Největší nebezpečí pravděpodobně představují phishingové útoky cílící přímo na uživatele. V rámci kapitol, líčících útoky podle napadeného prvku, jsou také zobrazeny útoky, které jsou nějakým způsobem významné. U útoků na webovou aplikaci, komunikaci a na bankovní server bylo zjištění uskutečněných útoků poněkud problematické, neboť banky se vyhýbají poskytování těchto informací. Proto se popis významného útoku nachází pouze u bankovního serveru.

Další částí práce je definování úlohy médií v zobrazování kyberkriminality a charakterizování žurnalistického útvaru zpravodajství. Dále popisuji přímo internetová zpravodajství, která se vyznačují dalšími specifiky, např. kombinováním znaků tištěných a audiovizuálních médií. Na závěr charakterizuji vybrané kvalitativní požadavky na zpravodajství. Z nich poté vychází metodologie obsahové analýzy.

V praktické části je nejprve rozvedena právě metodologie obsahové analýzy. Zdůvodňuji zde výběr výzkumného vzorku a dalších faktorů. V analytické části jsou uvedeny odpovědi na výzkumné otázky pomocí grafů a tabulek.

Ve své práci se nezabývám problémem zabezpečení a útoků na smartbanking, vzhledem k rozsáhlosti a specifikům tohoto tématu. Smartbanking je poddruhem internetového bankovnictví, kdy se operace na účtu provádějí pomocí speciální internetové aplikace pro operační systémy chytrého telefonu nebo tabletu (Budoucnost distribučních kanálů v České republice a na Slovensku: Trendy a nové vize, 2012).

Na konec bych chtěla ještě poznamenat, že anglické zdroje jsou přeloženy přímo mnou – jedná se zejména o monografii *Cybercrime* Davida Walla a o kapitolu *User Identification and Authentication Concepts* z monografie Dobromira Todorova. Na další poté v textu upozorním.

---

[1] Jak moc, lze vidět v grafu zobrazujícím počet uživatelů internetového bankovnictví na straně 11.

[2] Např. zpravodajství Novinky.cz mělo v březnu 2013 přes 3 mil. návštěvníků (Měsíční zpráva: Březen 2013, 2013).

1. Úvod do internetového bankovnictví

Internetové bankovnictví spadá do přímého elektronického bankovnictví. Přímé elektronické bankovnictví umožňuje správu osobních nebo firemních financí prostřednictvím elektronických kanálů, tedy pomocí pevné telefonní linky[3], mobilního telefonu[4] nebo pomocí počítače. Klienti tudíž nepotřebují pro provádění základních bankovních transakcí navštívit bankovní pobočku. Počítač umožňuje více způsobů bankovnictví - může na něm být např. nainstalovaná offline bankovní stanice. Tento způsob se nazývá homebanking a díky možnosti propojení s účetními systémy se využívá zejména pro správu firemních nebo podnikových financí. Další možností je přístup k osobním nebo firemním financím přes internet. Do elektronického bankovnictví se také řadí platební karta, která sice neumožňuje správu účtu, ale umožňuje výběr hotovosti, zjištění zůstatku na účtu nebo lze pomocí ní platit za zboží či služby.

Internetové bankovnictví můžeme definovat jako správu osobních nebo firemních financí pomocí internetu. Platební produkt internetového bankovnictví je vymezen jako „prostředek vzdáleného přístup k peněžní hodnotě" (Máče, 2006, str. 160). Z toho vyplývá, že internetové bankovnictví pracuje s elektronickou podobou fyzických peněžních prostředků.

Internetové bankovnictví může sloužit jako příklad snahy finančních institucí o poskytování lepších služeb, které jsou důležité pro vymezení bank v konkurenčním prostředí. Dochází totiž ke globalizaci bankovnictví, a tím k otvírání lokálních trhů pro další hráče. Banky se musí transformovat z tradičních institucí na moderní a flexibilní společnosti, aby udržely svou pozici a své zisky.

Přesouvání služeb na internet má také další výhody, zejména se jedná o úsporu času a financí, nebo zkvalitnění některých služeb. Úspora času a financí má dopad na banku i klienta. Na straně banky dojde ke snížení nákladů na transakci, a tím pádem ke zvýšení zisků. Toto snížení pocítí i klient. Na straně klienta je to zejména úspora času, ke které dojde odstraněním nutnosti navštívit fyzicky banku, díky možnosti přístupu 24 hodin denně 7 dní v týdnu a v neposlední řadě i díky zrychlení jednotlivých procesů. Zkvalitnění služeb, které tento způsob bankovnictví klientovi umožňuje, je právě časově neomezený přístup. Přístroj, pomocí něhož je přistupováno k elektronickému bankovnictví, je většinou přenosný, takže uživatel není vázán ani na konkrétní místo. Tyto přístroje jsou také široce rozšířené, ať už se jedná o telefony nebo počítače. Výhodu internetového bankovnictví oproti ostatním způsobům lze spatřovat také v přehlednosti správy účtu a uskutečněných transakcí.

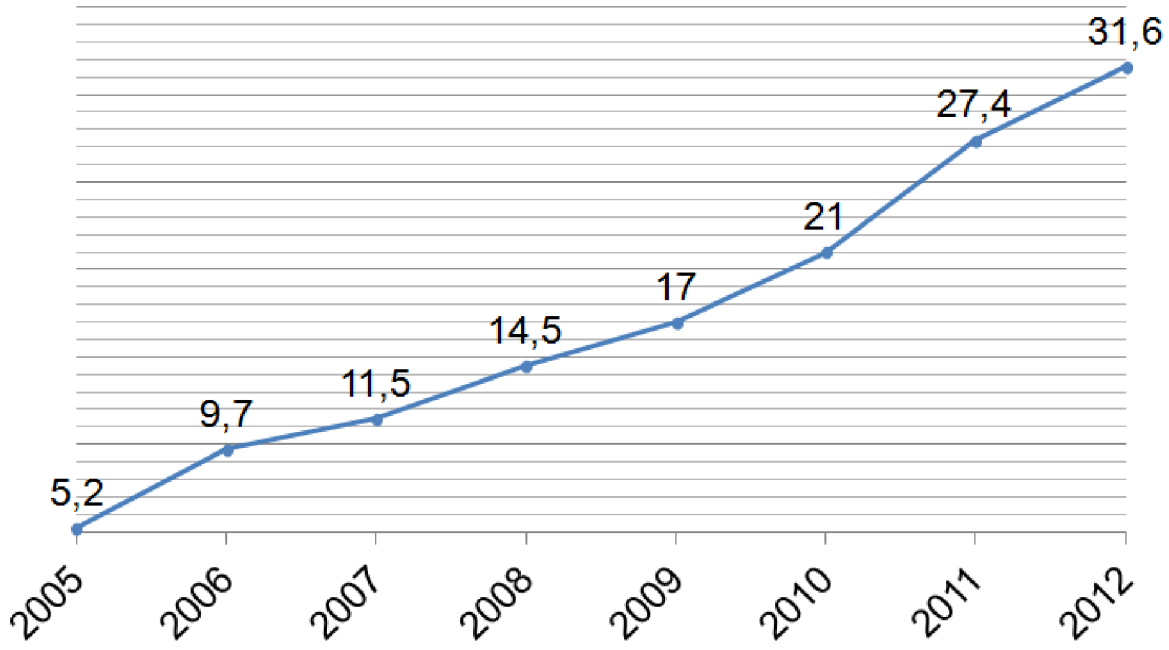
Nevýhodou jsou vyšší požadavky na bezpečnost, které jsou zapříčiněny komunikací banky s virtuální identitou klienta místo fyzické. Virtuální identita má více nároků na ověření totožnosti uživatele a oprávnění přístupu k účtu, jak si vysvětlíme v kapitole 1.3.1. Uživatel tak musí dodržovat více bezpečnostních zásad, než byl zvyklý u přímé fyzické komunikace s bankou. Další nevýhodou pro klienta může být přenesení

---

[3] V tomto případě se jedná o komunikaci s callcentrem banky, kde může být buď člověk, tedy bankéř, nebo automatizovaný systém.

[4] Zde můžeme samozřejmě využít stejné kanály jako v případě pevné telefonní linky. Dále můžeme realizovat platby nebo se podívat na výpisy z účtu pomocí standardizovaných SMS nebo využít přístup přes WAP, tzn. připojit se k internetu. Tímto termínem není míněn tzv. smartbanking, tedy ovládání účtu přes internet pomocí speciální aplikace pro chytrý telefon nebo tablet, ale pomocí standardních telefonních služeb, tzn. hovorů a SMS zpráv.

odpovědnosti za případné ztráty z banky na klienta (Matyáš a Krhovják, 2008, str. 13). Na tuto nevýhodu upozorňují jednotlivé banky, např. PPF banka a další, ve svých pokynech pro internetové bankovnictví. Dodržování bezpečnostních pokynů je tedy v zájmu uživatele.



Obrázek 1 Uživatelé internetového bankovnictví v ČR (v procentech), zdroj: Informační technologie v domácnostech a mezi jednotlivci, 2012

V České republice roste počet uživatelů internetového bankovnictví, který je ale v porovnání s ostatními zeměmi Evropské unie podprůměrný, jak ukazuje obrázek č. 1 (Informační technologie v domácnostech a mezi jednotlivci, 2012). Je důležité poznamenat, že data v grafu se týkají celkové populace nad 16 let. Počet uživatelů nicméně neustále roste, a s rozšířením chytrých telefonů a otevíráním bank směrem ke klientům se dá očekávat, že rostoucí trend bude pokračovat.

Seznam bank, které nabízejí systém internetového bankovnictví

1. Air Bank
2. AXA Bank (poskytuje pouze spořící a hypoteční účty)
3. BRE Bank - produkt se jmenuje mBank
4. Citibank
5. Česká spořitelna
6. Českomoravská stavební spořitelna (pouze stavební spoření), jinak Era účet
7. Československá záruční a rozvojová banka
8. ČSOB (Součástí této banky je Poštovní spořitelna, která poskytuje internetové bankovnictví pod názvem Era.)
9. Equa banka
10. Evropsko-ruská banka
11. Fio banka
12. GE Money Bank
13. ING Banka
14. JT banka
15. Komerční banka
16. LLBW Bank (Landes Bank Baden-Würtenberg)
17. Oberbank
18. Poštová banka
19. PPF banka
20. Raiffeisenbank
21. Raiffeisenbank im Stiftland - cílí především na Západní Čechy
22. Sberbank
23. UniCredit Bank
24. Volksbank Löbau-Zittau
25. VÚB (Všeobecná úvěrová banka)
26. Waldviertler Sparkasse - regionální (česko-rakouské pomezí)
27. Wüstenrot
28. Zuno

Seznam bank[5] naznačuje, že internetové bankovnictví poskytuje 28 z celkového počtu 44 bank, registrovaných u České národní banky (Seznamy regulovaných a registrovaných subjektů finančního trhu, 2013). Z toho můžeme vidět, že službu internetového bankovnictví nabízí svým klientům většina českých bank.

[5] Tento seznam byl vytvořen pomocí Seznamu regulovaných a registrovaných subjektů, který je publikován na stránkách České národní banky. Webové stránky jednotlivých bank byly poté prozkoumány za účelem nalezení aplikace on-line bankingu.

1.1. Procesy internetového bankovnictví

Internetové bankovnictví je proces vzdáleného přístupu k bankovním účtům přes síť internet, který se skládá z několika prvků. Nejprve si klient otevře webový prohlížeč a připojí se prostřednictvím poskytovatele internetových služeb (ISP) do sítě internet. Na internetu se připojí ke svému internetovému bankovnictví prostřednictvím bankovního ISP. Nakonec proběhne kontakt mezi bankovním ISP a bankovním systémem, kdy se klient připojí k bankovnímu systému.

1.2. Zabezpečení přístupu do internetového bankovnictví

Pro přístup do internetového bankovnictví, tedy do bankovního systému, se objevují dvě důležité operace, omezující přístup k bankovnímu systému a definující operace, které může uživatel v systému provádět. Jedná se o identifikaci a autentizaci klienta, tedy formulace identity uživatele a její ověření. S tímto krokem je spojena autorizace - určení činností, ke kterým má klient oprávnění. Uživatel se po úspěšné autentizaci dostane do svého bankovního účtu, zde ale může vykonávat pouze pasivní činnost jako prohlížení stavu účtu, provedených plateb atp. Pro provedení aktivních transakcí, např. zadávání plateb, je nutné operace ještě dodatečně autorizovat, tedy odsouhlasit provedení operace.

Zvýšení ochrany přístupu do bankovního systému přes internet je nutné z toho důvodu, že na rozdíl od tradičního bankovnictví se zde pracuje s virtuální identitou uživatele. Při klasickém přístupu probíhá ověření identity vizuálním srovnáním identifikačního dokladu a osoby klienta pracovníkem banky.

1.2.1. Autentizace

Autentizace, tj. ověření identifikace klienta, probíhá pomocí informací, které přísluší jedné virtuální identitě, tedy pouze jednomu uživateli. Základní metody, jak autentizovat uživatele, jsou tři: autentizace znalostí, autentizace vlastnictvím a autentizace vlastností (Matyáš a Krhovják, 2008, str. 10).

1.2.1.1. Autentizace znalostí

Nejjednodušším způsobem, jak uživatele autentizovat, je autentizace znalostí. Tento způsob předpokládá, že uživatel má nějakou specifickou znalost, typicky hesla nebo PINu. Uživatelské jméno a heslo (nebo PIN) jsou základní metodou ověření identity klienta. Kvůli jednoduchosti těchto údajů (např. bankovní PIN má čtyři číslice[6]), a tím pádem i jednoduchosti jejich prolomení, se ale doporučuje kombinovat autentizaci znalostí s dalšími autentizačními způsoby.

Výhodou tohoto způsobu je, že není vyžadován fyzický předmět nebo čtecí zařízení pro autentizaci. Autentizační systém nevyžaduje složitou údržbu. Na straně uživatele je výhodou snadná zapamatovatelnost autentizačního údaje. Spoléhání se pouze na intelekt uživatele může zároveň být nevýhodou - uživatel může přihlašovací údaje zapomenout. Některé banky umožňují zasílání zapomenutého hesla na mobilní

[6] Může mít ale více číslic, podle použité služby.

telefon[7]. Uživatel ale samozřejmě musí zodpovědět bezpečnostní otázky, zvolené při zakládání účtu. Klient si dále může vytvořit pomůcku, na kterou si autentizační údaj zaznamená. Autentizační údaj mu poté může být odcizen[8]. Heslo pro autentizaci může být také prolomeno hrubou silou[9]. Tomuto případu se snaží vyhnout základní požadavky na složitost hesel, např. použití více druhů znaků (velká a malá písmena, číslice, znaky), nebo délka hesla, která by se měla pohybovat mezi 8 a 12 znaky. Další metodou ochrany je omezení počtu pokusů při zadávání hesla nebo PINu. Po překročení limitu je přístup k účtu zablokován. K odblokování dojde buď po uplynutí určité časové lhůty nebo po fyzické návštěvě pobočky banky a ověření totožnosti klienta. Některé banky nabízejí možnost odblokování pomocí telefonu[10].

1.2.1.2. Autentizace vlastnictvím

Další metodou je autentizace vlastnictvím. V tomto případě se využívá fyzický předmět, který se zpravidla označuje jako token. „Tokeny mají buď specifické fyzikální vlastnosti (tvar, elektrický odpor, elektrickou kapacitu,…), obsahují tajné informace (např. kvalitní heslo nebo kryptografický klíč), nebo jsou dokonce schopné provádět některé výpočty (obvykle kryptografické).” (Matyáš a Krhovják, 2008, str. 19)

V internetovém bankovnictví se používají autentizační kalkulátory, klientské přístupové certifikáty[11] nebo čipové karty. Dále bych do této metody zařadila vlastnictví mobilního telefonu klienta, na který banka zasílá jednorázové autentizační SMS.
Autentizační kalkulátory jsou zařízení, většinou podobná kalkulačce. Pro přihlášení do autentizačního kalkulátoru se většinou používá PIN. Kalkulátor poté vygeneruje jednorázové heslo, které uživatel zadá do systému internetového bankovnictví. Pro komunikaci kalkulátoru s počítačem se používá optické rozhraní nebo infračervený port (Matyáš a Krhovják, 2007). Příklad optického autentizačního kalkulátoru generujícího jednorázová hesla na základě animované čárové grafiky, která se zobrazí na obrazovce počítače, můžeme vidět u Landesbank Löbau - Zittau (Sm@rt-TAN plus, 2013).

Klientské přístupové certifikáty jsou časově omezené kryptografické protokoly, vydávané bankou. Při autentizaci je navíc potřeba certifikát podepsat soukromým klíčem[12]. Kromě potvrzení autentizace se nevyužívají, do systému se tedy nahrávají jednorázově. Certifikát lze uložit buď v počítači klienta nebo na čipové kartě. Čipové karty jsou samy o sobě schopné provádět s klientským certifikátem kryptografické operace. Certifikát se do systému nenahrává, a tedy neopustí kartu (Matyáš a Krhovják, 2008, str. 80).

Výhodou těchto zařízení je schopnost zapamatovat si složitější údaje, než dokáže lidský intelekt. Další klady jsou zřejmé - obtížnější možnost zneužití fyzického předmětu nebo uložení výpočetně složitějších klíčů a hesel. Nevýhodou oproti tomu je nemožnost přihlášení do bankovního systému bez tohoto předmětu, což vyžaduje mít

---

[7] Konkrétně Air Bank a Wüstenrot. Wüstenrot zašle heslo po ověření bezpečnostních údajů a na základě telefonátu klienta do banky.

[8] Typický příklad je zaznamenávání PIN na papír a následné umísťování tohoto papíru v blízkosti platební karty.

[9] O prolomení hesel hrubou silou píšu v kapitole 2.1.1.

[10] Příkladem může být CitiBank a jejich zákaznická telefonní linka CitiPhone.

[11] Kromě klientských, tj. osobních certifikátů, existují ještě serverové, které jsou vydávány pro konkrétní instituci (Typy digitálních certifikátů, 2003).

[12] Pro certifikáty a pro soukromé klíče viz kapitolu 1.3.2.

předmět při přihlašování u sebe. Dalším nedostatkem je závislost na výrobci kalkulátoru, protože zařízení většinou vyžadují specifickou infrastrukturu. Od toho se odvíjí vyšší složitost kalkulátoru, která je také ovlivněna vyššími požadavky na bezpečnost. Výsledkem součtu těchto faktorů je vyšší cena požadovaná výrobci.

1.2.1.3. Autentizace vlastností

Poslední metoda vychází z využití biometrických údajů. Využívá se jedinečná vlastnost uživatele, tj. fyziologická vlastnost nebo chování uživatele. Mezi výhody patří složitější zneužití biometrických údajů nebo jedinečnost údajů, které jsou vlastní vždy pouze jedné osobě. Nevýhodou je, že kvůli lehkým změnám, způsobeným náladou (u hlasu nebo podpisu) nebo fyzickým stavem (u měření tepové frekvence), není tato metoda úplně přesná. Pracuje tedy s intervalem možností, místo s jednoznačnou odpovědí na otázku ano-ne. Další nevýhoda spočívá v potřebě nějakého čtecího zařízení, aby se údaje přenesly do výpočetního zařízení. V oboru internetového bankovnictví nepovažuji tuto metodu za efektivní, neboť kvůli výše zmíněné neúplné přesnosti se doplňuje vizuální kontrolou jiným pracovníkem. Kontrola pomocí biometrických údajů je proto vhodnější ve veřejných prostorách, např. na letišti (Doseděl, 2004, str. 69).

Kombinací vždy jednoho prostředku z dvou různých metod autentizace dosáhneme dvoufaktorové autentizace. V internetovém bankovnictví je to typicky autentizace vlastnictvím (mobilní telefon, klientský certifikát) zároveň s autentizací znalostí (uživatelské jméno a heslo, PIN). Nejvyšší prvkem zabezpečení v současnosti představuje třífaktorová autentizace. Biometrické informace jsou snímány a zpracovány tokenem, server po úspěšném ověření PINu a biometrických údajů z tokenu zahájí komunikaci pomocí protokolu výzva-odpověď, kdy si server a token vymění důvěrné údaje. Tyto údaje jsou uloženy nebo vygenerovány tokenem. K úspěšné autentizaci je tedy zapotřebí úspěšně ověřit všechny tyto prvky. V případě selhání jedné části autentizačního procesu je autentizace neúspěšná.

Tabulka 1 Používané autentizační metody

	uživatelské jméno a heslo	PIN	autentizační kalkulátor	SMS	certifikát	čipová karta
AXA bank	• (+ captcha, tj. test používaný k rozlišení lidí od strojů, a datum narození)					
Air Bank	•					
CitiBank	•		•	•		
Česká spořitelna	•			•	•	•
ČSOB	•	•				•
ČRRB	•			•		•
Equa bank	•				•	
E-R Banka	•			•	•	
GE Money Bank	•			•	•	
Fio banka	•				•	
ING Banka	•	•		•		
JT banka	•		•	•		
Komerční banka	•	•			•	•
mBank	•					
Oberbank	•	•		•		
Poštová banka	•					
PPF banka	•	•	•	•	•	
Raiffeisen bank	•	•	•	•		
Raiffeisenbank im Stiftland	•		•			
Sberbank	•	•	•			•
UniCredit Bank	•		•	•		
Volksbank Löbau-Zittau	•	•	•			•
VÚB	•	•	•			•
Waldviertler Sparkasse	•			•		•
Wüstenrot	•					
Zuno	•					

V tabulce č. 1 jsou popsány autentizační metody, používané jednotlivými aplikacemi pro internetové bankovnictví. Tabulka byla vytvořena průzkumem těchto aplikací. Vyplývá z ní, že nejnižší úroveň zabezpečení autentizace mají banky: Air Bank, mBank, Poštová banka, Wüstenrot a Zuno, protože pro přístup do internetového bankovnictví využívají pouze uživatelské jméno a heslo.

1.2.2. Autorizace

Autorizovat lze dva prvky bankovních operací - klienta a transakce.
Autorizací klienta se rozumí přidělení oprávnění pro práci v systému, případně definování akcí, které uživatel může nebo nemůže vykonávat (Matyáš a Krhovják, 2008). Vzhledem k úzkému propojení procesů autentizace a autorizace uživatele bývá

občas těžké je odlišit. Teoreticky znamená proces autentizace pouze ověření totožnosti, a autorizace povolení přístupu uživatele (Todorov, 2007). Většinou je autorizace součástí identifikace a autentizace uživatele. V internetovém bankovnictví se uživateli povoluje přístup jedině do jeho bankovního účtu. Nikam jinam v bankovním systému přístup nemá. V případě autorizace uživatele se tedy přiděluje oprávnění pouze pro pasivní operace jako prohlížení účtu atd.

V případě, že uživatel chce provést aktivní operace na účtu, jako např. platby, je potřeba autorizovat transakce. Ověřuje se tím, zda má klient oprávnění tyto operace provést.

V internetovém bankovnictví se pro autorizaci klienta i transakcí obvykle používají stejné metody jako pro autentizaci. Většinou se využívá dvoufaktorová autentizace. Klient může operace autorizovat opakovaným zadáním hesla nebo PIN, svým certifikátem a soukromým klíčem uloženým v počítači nebo na čipové kartě. Autorizace se také může uskutečnit pomocí zaslání jednorázového autorizačního kódu (např. autorizační SMS), který je potom do systému zadán. Další možnosti je autorizace pomocí souboru jednorázových kódů, obdržených klientem v papírové podobě od banky. Ty se označují jako TAN - Transaction Authentication Number (Matyáš a Krhovják, 2008). V České republice tuto metodu používá Oberbank.

Někdy je autorizace transakce vyžadována pouze v případě, že výše transakce přesáhne předem stanovenou částku nebo denní limit.

1.3. Zabezpečení bankovních procesů

Největší nároky na bezpečnost ze všech druhů elektronického bankovnictví má právě internetové bankovnictví a jeho poddruhy, např. smartbanking[13]. Příčina tkví ve vzdáleném přístupu k bankovním účtům prostřednictvím internetu. Tato síť není zabezpečená a jako taková je snadným terčem útoků. Proto je potřeba přidávat bezpečnostní opatření. Nutností je zajištění bezpečnosti aplikace internetového bankovnictví a fyzické bezpečnosti systému (Přádka a Kala, 2000, str. 75).

Při zajišťování bezpečnosti bankovní aplikace je potřeba mj. pamatovat na:

- jednoznačnou autentizaci obou aktérů komunikace (viz stranu 20),
- bezpečnost přenosového kanálu (za účelem zamezení odposlechnutí hesla) a
- důvěrnost a prokazatelnost původu zpráv, které si banka a klient vymění.

Zabezpečení systému uživatele dosáhneme pomocí používání firewallu a používání antivirových programů. Na straně banky se jedná mj. o zabezpečení systému pomocí firewallů proti útokům na bankovní systém zvenčí i ve vnitřní síti (proti útokům insiderů[14]). Zajištění fyzické bezpečnosti je popsáno v kapitole 1.3.4.

[13] Smartbanking má ještě větší nároky na bezpečnost, neboť při rozšířeném autentizování klienta nebo autorizace transakcí pomocí SMS zpráv probíhá přijímání zpráv a manipulace s účtem na jednom přístroji. Banky to řeší pomocí oddělení aplikace pro internetové bankovnictví, ke které se musí klient přihlásit zvlášť. Uživatelé si zatím příliš neuvědomují, že chytrý telefon slouží již jako malý počítač, a je třeba ho adekvátně k tomu chránit.

[14] Insider je termín, používaný pro uživatele, pohybující se ve vnitřní síti, nebo zaměstnance.

1.3.1. Zabezpečení autentizace klienta

Proces autentizace klienta do systému je třeba zabezpečit. Autentizační metody se dělí na slabé a silné podle toho, kolik času je potřeba k jejich prolomení. Slabé autentizační metody jsou hesla a PINy. Tyto metody nepoužívají kryptografické metody. Na hranici mezi silnými a slabými metodami leží jednorázová hesla s omezenou dobou platnosti. Silné autentizační metody potom jsou takové, které pro autentizaci využívají tokeny a pracují na kryptografickém principu výzva-odpověď, používají tedy pro ověření přístupu náhodně vygenerovaná čísla a obsah zpráv je na sobě závislý (Matyáš a Krhovják, 2008).

Další možnosti zabezpečení autentizace představuje personalizovaný login nebo grafická klávesnice. Personalizovaný login znamená, že na stránce se vyskytuje obrázek nebo oslovení, které si uživatel zvolil a je pro něj jedinečné. V případě, že se tento jedinečný prvek neobjeví, klient má jistotu, že se dostal na stránky napodobující pravé stránky internetového bankovnictví. Komunikaci tedy ukončí před předáním citlivých dat, která se snaží podvržená stránka získat. Grafická klávesnice je nástroj zobrazující se na stránce internetového bankovnictví. Uživatel tedy zadá heslo nebo PIN kliknutím myši a nikoliv fyzickou klávesnicí počítače. Snižuje se tak riziko útoku pomocí keyloggeru, tzn. malware zaznamenávající údery kláves. Z českých bank nabízí grafickou klávesnici Servis 24, tj. internetové bankovnictví České spořitelny, Fio banka nebo Wüstenrot.

1.3.2. Zabezpečení zpráv

Při autentizování zpráv je potřeba ověřit mj. jednoznačnou identitu odesílatele a důvěrnost a integritu, tedy nepozměněnost zprávy. Data chráníme před prozrazením a před neoprávněnou změnou. K tomu slouží metody šifrování zprávy a digitálního podpisu. Pro ochranu před kompromitací dat se používá také zabezpečený přenosový protokol, tedy SSL nebo TLS. Zprávy si vyměňují systém klienta nebo elektronické autentizační nástroje se systémem internetového bankovnictví.

Šifrování zpráv se používá při odesílání zpráv bance a následnému přijímání zpráv od banky. Zprávy jsou šifrovány pomocí kryptografické metody šifrovacích klíčů. Kryptografie zná dvě metody šifrování - symetrické a asymetrické. Symetrické šifrování spočívá v tom, že oba subjekty - odesílatel i příjemce, mají stejný klíč k šifrování i dekódování. Tato metoda se v internetovém bankovnictví používá pouze v protokolu RC4[15], který s dalšími nástroji tvoří přenosový protokol TLS. Asymetrická kryptografie využívá toho, že oba dva subjekty v komunikaci mají dva klíče, veřejný a soukromý. Veřejný klíč subjekty znají, ale soukromý ne. Soukromý klíč je potřeba chránit proti prozrazení. Při odesílání zprávy je zpráva zašifrována veřejným klíčem příjemce a odeslána. Příjemce zprávu rozšifruje pomocí svého soukromého klíče. Text zprávy nelze pomocí klíče, kterým byla zašifrována, zpětně rozšifrovat.

Digitální podpis pracuje na opačném principu než šifrování zpráv. Stejně jako šifrování zpráv využívá asymetrickou kryptografii, tedy princip veřejných a soukromých klíčů. Při šifrování je ale důležité, aby zprávu nepřečetl nikdo jiný než oprávněná

[15] RC4 je proudová šifra, tzn., že šifruje proud znaků bit po bitu. Výhodou proudových šifer je snadnější implementace a větší rychlost šifrování textu (Winlab, 2004, překlad autorky).

osoba. Ta použije soukromý klíč, který zná pouze ona. Při použití digitálního podpisu může kdokoli ověřit pomocí veřejného klíče platnost podpisu, vytvořeného oprávněnou osobou příslušným soukromým klíčem.

Z toho vyplývá, že digitální podpis slouží k jednoznačnému ověření identity odesílatele a integrity zprávy. Zaručuje, že zpráva nebyla při přenosu nijak modifikována (v opačném případě by došlo ke změně otisku). Při vytváření digitálně podepsané zprávy se nejprve jednosměrnou hashovací funkcí zhustí text zprávy na digitální otisk (hash), který má mnohem méně bitů než zpráva. Vytvořit zpětně zprávu z digitálního otisku je výpočetně velmi náročné, v konečném čase skoro nemožné. (Doseděl, 2004)

Platnost veřejného klíče je ale nutné ověřit a jednoznačně k němu přiřadit identitu konkrétní osoby nebo instituce. K tomu slouží certifikáty vydávané certifikačními autoritami. Certifikační autority, jakožto důvěryhodné třetí strany, svým digitálním podpisem potvrzují spojení veřejného klíče s konkrétním jedincem. Certifikáty obsahují osobní údaje osoby vlastnící veřejný klíč. Tyto údaje jsou certifikační autoritou ověřeny při osobní návštěvě. Certifikační autority dále vydávají seznamy kompromitovaných veřejných klíčů, ve kterých si příjemce může ověřit platnost klíče.

Certifikační autoritou může být státní instituce[16], obecně uznávaná autorita (VeriSign) nebo i samotná finanční instituce, tedy banka. Tyto instituce mohou být pro účely vydávání certifikátů spojeny do účelových sdružení. (Matyáš a Krhovják, 2008, str. 12) V případě finančních institucí jsou serverové certifikáty zpravidla potvrzené certifikační autoritou VeriSign. Uživatel si může platnost serverového certifikátu ověřit ve webové aplikaci pro internetové bankovnictví kliknutím na ikonu zámku v prohlížeči. Zde se zobrazí certifikační autorita a stránky, na které byla webové aplikace vydána.

1.3.3. Zabezpečení komunikačního kanálu

Komunikačním kanálem, který je v internetovém bankovnictví využit, jsou webové stránky banky nebo přímo webové stránky aplikace pro internetové bankovnictví. Jedná se o využití protokolu HTTP[17] pro přenos HTML souborů, tj. dat (Doseděl, 2004, str. 108). Protokol HTTP ale není nijak zabezpečený, přenášená data tedy mohou být prozrazena.

K zabezpečení protokolu HTTP dochází po úspěšné autentizaci klienta i serveru. Protokol je poté zabezpečen přenosovým protokolem SSL[18] vrstvy. V současnosti se ale používá standardizovaný protokol TLS 1.0, odvozený ze SSL. Tyto protokoly se liší pouze v detailech (z pohledu uživatele), které jsou ale natolik významné, že se změnil název. Protokol TLS se stejně jako SSL používá pro autentizaci serveru a zabezpečení komunikace v síti internet před kompromitací a modifikací. Výsledkem je protokol, označovaný jako HTTPS. Data jsou při použití TLS protokolu chráněna proti změně či útoku, a také jsou šifrována.

---

[16] V České republice jsou Ministerstvem vnitra akreditovány pro poskytování certifikačních služeb tři certifikační autority: První certifikační autorita, a. s., Česká pošta, s. p. a eIdentity a.s. (Ministerstvo vnitra, 2010).

[17] HyperText Transport Protocol

[18] Secure Socket Layer

TLS dále slouží jako autentizační prostředek, pomocí kterého se může ověřovat identita klienta a serverů. Tato možnost je volitelná. „V praxi se využívá většinou jen autentizace serveru, výjimkou jsou různé internetové bankovní služby." (Doseděl, 2004, str. 75) Na začátku komunikace se klient a server domluví na kryptografickém protokolu srozumitelném pro obě strany a vymění si náhodně vygenerovaná čísla. Tyto nástroje slouží jako základ pro šifrování probíhající komunikace. Klíče se generují nové pro každou začatou komunikaci. Dále si klient a server vymění certifikáty veřejných klíčů pomocí metody výzva-odpověď. Klient tedy serveru zašle náhodně vygenerované číslo, server ho zašifruje svým soukromým klíčem a odešle zpět. Klient jej pomocí veřejného klíče dešifruje. Když klient odešle náhodně vygenerované číslo zašifrované veřejným klíčem serveru, server ho naopak vrátí dešifrované.

Potvrzení zabezpečení komunikace mezi klientem a bankou pomocí protokolu TLS (přenosového protokolu https) se objeví v adresovém řádku webového prohlížeče klienta. Zabezpečení je také zdůrazněno pomocí vizuálních prvků, tedy pomocí ikony zámku a zeleného adresového řádku. Tyto způsoby označují důvěryhodnou a ověřenou webovou aplikaci. Uživatel si může kliknutím zobrazit podrobnosti o zabezpečení, tzn. šifrovací protokoly, certifikáty, ověřené certifikační autoritou apod. Bankovní (serverové) certifikáty, které se zobrazí, slouží k ověření identity vzdáleného počítače, v tomto případě bankovních stránek.

1.3.4. Zajištění bankovního systému proti průnikům do banky

Banky jsou proti útokům zvenčí zabezpečeny pomocí firewallu, tedy pomocí souboru HW a SW opatření, které jsou v komunikačním procesu umístěny před všechny další bankovní systémy. Tyto prostředky jsou vhodným způsobem kombinovány, aby zamezily předem definovaným rizikům spojení mezi dvěma sítěmi. Komunikace je přitom omezena pouze zvnějšku dovnitř sítě, opačným směrem není potřeba ji nějak chránit. Firewall může zakazovat provoz na portech pomocí IP filtru[19] nebo pomocí aplikačního proxy. Druhý případ omezuje provoz na jednotlivých portech pro jednotlivé aplikace, např. na jeden program pro stahování pošty. Dále je možné pomocí personálních firewallů ochránit jednotlivé počítače. To se hodí zejména při opuštění zabezpečené firemní sítě nebo jako obrana proti útokům uvnitř sítě.

Řízení přístupu k procesům internetového bankovnictví zajišťuje bezpečnost internetového bankovnictví před rizikem kumulace moci nad systémem do jedněch rukou. Je potřeba oddělit role správců systému tak, aby každý správce spravoval pouze jednu část procesu. Žádný pracovník tedy nemá přístup do celého systému. Druhy správců a jejich funkce se obecně stabilizovaly následovně – superuživatel (konfiguruje systém), bezpečnostní správce (nastavuje přístupová práva) a auditor (provádí kontrolu dodržování pravidel, analýzu logů apod.). V běžném provozu je to potom správce prostředků, který se stará o běžnou údržbu systému, a operátor, který provádí činnosti, jako např. zálohování nebo řešení problémů (Doseděl, 2004, str. 82). Toto ustálení není pevné, v jednotlivých systémech se může měnit. Tímto krokem se tedy zvyšuje bezpečnost systému. Rozdělení procesů dále slouží k tomu, aby se zamezilo vykonávání neoprávněných operací. V tomto případě by vyžadovaly

[19] Může používat buď jednoduchý IP filtr, sloužící jako blokovač internetového provozu, nebo stavový, který propustí do sítě data, vyprovokovaná nějakou akcí uvnitř sítě (Doseděl, 2004).

součinnost více lidí, zvyšuje se tak možnost odhalení nelegálních aktivit. Systém dále využívá technologii digitálních podpisů. Při zadávání příkazů k vnitřním operacím ověřuje, zda příkaz k operaci zadal oprávněný uživatel. Operátorské příkazy nelze bankovnímu systému podvrhnout. Pro určení práv uživatelů se používá základní pravidlo: nejprve jsou uživateli zakázány všechny činnosti, potom se mu povolují jen ty činnosti, které bezpodmínečně potřebuje k vykonávání své práce. Toto pravidlo také platí pro určování práv uživatelů nepatřících k vnitřní síti banky.

1.3.4.1. Zajištění fyzické bezpečnosti uvnitř banky

Na straně banky je potřeba zajistit fyzickou bezpečnost systému a procesů internetového bankovnictví, např. fyzickou bezpečnost bankovních serverů. Ty jsou bezpečně uloženy ve schránkách, které jsou zabezpečeny proti neoprávněnému vniknutí. V případě autentizačního (soukromého) klíče internetového bankovnictví slouží k ochraně speciální zařízení, tzv. šifrátor, umístěné ve velmi kvalitním nerozebíratelném obalu. Pokud je vnitřním systémem zaznamenáno porušení obalu, dojde ke zničení klíče. Klíč také nikdy zařízení neopouští. Jedinou operaci, kterou zařízení umožňuje vykonávat, je šifrování dat. (Doseděl, 2004, str. 53) Při zálohování klíče pro případ technologické ztráty se klíč rozdělí na dvě čipové karty, každou dostane jedna osoba. Třetí osoba pak zná heslo k soukromému klíči.

Dalším opatřením na straně bank může být pravidlo čtyř očí, označováno také jako metoda „Dual Control Policy" (Matyáš a Krhovják, 2008, str. 44). Toto pravidlo stanovuje, že pro každou operaci v bankovním systému je nutná přítomnost minimálně dvou na sobě nezávislých důvěryhodných správců. Oba dva správci musí provedení operace odsouhlasit. Banky se tedy snaží zvýšit kontrolu těchto procesů a zároveň omezit poměrně vysokou moc správců systému (Doseděl, 2004, str. 82).

1.3.5. Bezpečné chování uživatelů

Nejméně zabezpečený prvek procesu internetového bankovnictví představuje počítač klienta. Je to také jediný prvek, za jehož zabezpečení zodpovídá klient. Proto je nutné zabezpečit počítače uživatelů pomocí antivirových programů a firewallů. Personální firewally tvoří bariéru mezi počítačem uživatele a internetem. V případě, že narazí na nestandardní chování nebo požadavky z internetu, aplikace zablokují, popřípadě se uživatele zeptají, zda si je přeje spustit. Antivirové programy jsou nástroje, které detekují a odstraňují z počítače malware. Tyto nástroje je potřeba neustále aktualizovat, protože takto se do programu dostávají bezpečnostní záplaty na nově objevené hrozby. Počítače je dále třeba pomocí spamových filtrů chránit před nevyžádanou poštou a pomocí kryptografických protokolů před odposloucháváním.

Přesto útoky na internetové bankovnictví na straně uživatele poškozují i banku. Banky proto na svých stránkách uvádějí základní bezpečnostní pokyny, kterými by se měli uživatelé při používání této služby řídit. Těmito prostředky se snaží banky zabezpečit provoz internetového bankovnictví a vzdělávat svoje uživatele. Klienti bank by se měli naučit, že požadavky na větší zabezpečení internetového bankovnictví nejsou nadstandardem, ale nutností. Měli by si tedy osvojit bezpečné chování na síti, mj. ve vztahu k systému internetového bankovnictví.

Společnými znaky bezpečnostních pokynů na stránkách bank jsou:

1. Používejte důvěryhodný počítač v zabezpečené síti.
2. Vždy se ujistěte o správné adrese banky, a ujistěte se, že komunikace mezi bankou a Vámi je zabezpečená pomocí protokolu HTTPS. Z jiné adresy než oficiální bankovní k internetovému bankovnictví nepřistupujte.
3. Při přihlašování do internetového bankovnictví si kliknutím na zámek v prohlížeči zkontrolujte správnost serverového certifikátu, tj. vydavatele (většinou CA VeriSign) a webovou adresu, které byl certifikát vydán. Dále si zkontrolujte dobu platnosti certifikátu.
4. Hesla nikomu nesdělujte, nikam je nezasílejte, nikam si je nezapisujte. Zvolte bezpečné heslo, tj. vhodnou kombinaci číslic, písmen a znaků.
5. Při zasílání autentizačních a/nebo autorizačních SMS na telefon dodržujte zásady ochrany telefonu, nikomu jej nepůjčujte apod. Při používání chytrého telefonu do něj instalujte pouze důvěryhodné aplikace z důvodů možné přítomnosti trojských koní a jiného malware[20].
6. Při používání klientského přístupového certifikátu jej neukládejte na pevný disk počítače, ale na přenosné médium, např. flash disk. Klientský certifikát je také vhodné zašifrovat.
7. Kontrolujte stav svého účtu a nesrovnalosti konzultujte s bankou.
8. Po skončení práce s bankovním účtem se odhlašte a zavřete okno prohlížeče.
9. Pravidelně aktualizujte operační systém a prohlížeč.
10. Používejte antivirový program, anti spyware a firewall. I tyto systémy udržujte aktualizované. Všechny nestandardní situace konzultujte s bankou.
11. Nevyplňujte osobní údaje, jako heslo, PIN apod., do políček přímo v zaslaném e-mailu a neklikejte na odkazy, které jsou zaslané e-mailem. Banky nikdy nevyžadují osobní údaje v elektronické komunikaci.

Tento seznam byl vytvořen kompilační metodou ze všech aplikací internetového bankovnictví. Aplikace internetového bankovnictví byly prohledány za účelem nalezení bezpečnostních pokynů. Tyto pokyny mají téměř stejný základ, jenž sloužil pro formulování seznamu. V případě, že byla nalezena odchylka, tak byla do seznamu také zanesena. Nutnost používání bezpečnostních pokynů vychází ze zásad pro zabezpečení bankovních procesů, které jsou popsány v první části práce.

1.4. Trendy v bankovnictví

V současnosti probíhá modernizace v bankovním sektoru, který se vyznačoval velkou mírou konzervativnosti a tradicionality. Banky se stávají z klasických bankovních domů poskytovateli moderních služeb. S tím souvisí využití nových komunikačních kanálů. Zatímco dříve se komunikační kanály přizpůsobovaly bankám, dnes je tomu naopak (Budoucnost distribučních kanálů v České republice a na Slovensku: Trendy a nové vize, 2012). Jako příklad lze uvést vytváření aplikací pro internetové bankovnictví, určených primárně pro chytré telefony a tablety. Tyto aplikace mají jiné operační systémy než klasické počítače, jiné požadavky na grafické

[20] Více o malware v kapitole 2.1.4.

uživatelské rozhraní a jinou úroveň zabezpečení, která vychází z využití přístupu přes bezdrátové sítě a využití totožného zařízení pro přístup i dvoufaktorovou autentizaci (Bezpečnost mobilního bankovnictví a aplikace Mobilní eKonto, 2008).

Banky musí vytvářet aplikace pro správu osobních i firemních financí přímo na míru těmto specifickým kanálům. „Pro banky je kritické přijmout strategii využívání tabletů, která bude zahrnovat jak služby, jež mají být pomocí tabletů podporovány, tak typy tabletů (včetně použitých operačních systémů), pro něž budou aplikace vyvíjeny." (Moyer, 2013) Také věnují vyšší pozornost návodům, jak s aplikacemi pracovat, vytvářejí i videonávody. Společnost Gartner předpokládá ve své studii v roce 2016 nárůst používání tabletů na 800 mil.[21] Prostřednictvím tabletů přistupuje k internetovému bankovnictví 38 % uživatelů, ve srovnání s 51 % z notebooků a 64 % ze stolních počítačů (Moyer, 2013). Z toho vyplývá, že banky by neměly pole těchto zařízení a aplikací opominout.

Tato zařízení, jako chytré telefony nebo tablety, mají rozšířené možnosti služeb, vycházející z jejich mobility. Typickou ukázkou jsou bezkontaktní platby pomocí technologie NFC[22]. Tímto způsobem se dá platit u obchodníků pomocí mobilních telefonů nebo platebních karet, které obsahují čip. Uživatel nemusí platební kartu vkládat do čtecího zařízení, pouze ji k zařízení přiloží. Poté se platba uskuteční. Většinou je potřeba autorizovat pouze transakce, které jsou vyšší než 500 Kč[23]. Stejným způsobem probíhá také platba pomocí mobilního telefonu. Další výhodou jsou rychlé platby s předvyplněnými údaji, které se objevují např. po načtení QR kódu[24] na složence, faktuře a dalších platebních pokynech. Tuto platbu stačí poté pouze autorizovat[25]. Další využití nabízí také funkce lokalizace klienta pomocí GPS lokátoru v chytrém telefonu. Uživatel poté může vyhledávat pobočky nebo bankomaty ve svém okolí. Zajímavou službou, vázanou na mobilní telefony, je Mobito. To umožňuje díky propojení telefonu s bankovním účtem nebo platební kartou rychlé převody financí mezi známými, platby u obchodníka nebo v e-shopu či dobíjení kreditu (Mobito: Peníze v mobilu, [2012])

Novinku v bankovnictví představuje vznik nového typu bank, zaměřených na provozování přímého bankovnictví. V České republice jsou to tyto instituce: Air bank, Equa bank, Fio banka, mBank a ZUNO. Tyto banky bývají také označovány jako nízkonákladové. Bankovní pobočky slouží zejména jako konzultační a poradenská centra. ZUNO nebo Air Bank např. nabízí možnost vytvoření bankovního účtu přes internet, není tedy nutné navštívit pobočku. Poskytování služeb je díky tomu levnější, a banky tak mohou poskytovat i další výhody, jako např. bonusy za přivedení dalšího klienta, odpuštění splátek půjčky, vedení účtu zdarma apod. Tyto banky se nemusí spoléhat na zavedené systémy a infrastrukturu, mohou tedy využít moderní IT systémy. Využitím těchto systémů dojde k dalšímu snížení nákladů. Aplikace internetového bankovnictví těchto bank jsou díky tomu intuitivnější, graficky přitažlivější

---

[21] V roce 2012 to bylo 130 mil. tabletů.

[22] Near Field Communication

[23] Era, mBank

[24] QR kód je grafický kód, ve kterém jsou uvedeny informace podobným způsobem jako v čárovém kódu. Jeho výhodou je mj. možnost zakódovat daleko větší množství dat, která mohou mít různou podobu, např. písmena nebo číslice (What is a QR code?, 2013, překlad autorky).

[25] Komerční banka, ČSOB a Raiffeisen Bank

a celkově jednodušší. Mezi přínosy moderních IT systémů tedy patří kromě zmíněného snížení nákladů především: přizpůsobování nabídky klientům, rychlejší informování a zpětná vazba a flexibilnější služby (Moyer, 2013).

Banky také objevují nové distribuční kanály, např. sociální sítě. Finanční instituce mohou využít nové způsoby on-line distribuce svých produktů a služeb, a tak oslovit novou skupinu zákazníků. Např. ZUNO banka využívá pro zpětnou vazbu kromě klasických komunikačních kanálů, jako je e-mail, telefon, nebo pobočka, ještě Twitter, Facebook, chat a Skype. Air bank zase nabídla možnost chatu přímo s generálním ředitelem, kdy se uživatelé mohli vyjadřovat k novinkám, jako např. k mobilní aplikaci pro iPad, zlevnění služeb nebo novým úrokovým sazbám. Uživatelé mají na webových stránkách banky k dispozici záznam konverzace (Novinky: Erich Čomor odpovídal na vaše dotazy - dokončeno ve 20:00, 2013). Banky také začínají poskytovat přístup k on-line transakcím ze sociálních sítí a snaží se uživatele více zapojovat do tvorby produktů a služeb, např. prostřednictvím integrace bankovních funkcí a dalších prvků do sociálních sítí (Moyer, 2013).

V oblasti služeb internetového bankovnictví vznikají unie s nebankovními prvky, např. z oblasti energetiky, daní, správních poplatků nebo pojištění (Budoucnost distribučních kanálů v České republice a na Slovensku: Trendy a nové vize, 2012). Účelem je vytvoření jednoho bodu pro přístup k dalším službám. Klient tedy pro vyřízení všech těchto povinností potřebuje pouze přístup do systému internetového bankovnictví. Typickým příkladem je Raiffeisen bank, která nabízí na stránkách internetového bankovnictví sjednání pojištění od pojišťovny Uniqa či platbu pro Finanční nebo Celní úřad.

Banky podporují individuální přístup a důvěrnější vztahy s klienty a snaží se navazovat bližší vztahy za účelem zvyšování loajálnosti klientů a zamezení jejich odchodu k jiným institucím. Jedná se tedy o přidanou hodnotu, která může vyvážit i lepší nabídky konkurence. Metod, jak toho dosáhnout, je spousta: vytvoření služeb na míru, pramenící z lepšího poznání klienta, např. jeho nákupních preferencí nebo sociodemografických podmínek, vychování si svých klientů od nízkého věku nebo proklientské výhody, které může banka nabídnout. Bankovní skupiny vytváří nové subjekty, cílící na jinou skupinu uživatelů než mateřské instituce. „mBank vznikla v listopadu 2000 v Polsku jako retailová divize BRE Bank SA. Prvotní obchodní model mBank předpokládal, že cílovými uživateli budou zejména lidé, kteří považují nová technologická řešení (především internet) za efektivní a pohodlný způsob komunikace s bankou.” (O mBank, 2007) Další příklad je Air bank vytvořená skupinou PPF. Další finanční institucí této skupiny je PPF banka, která se zaměřuje na poskytování služeb klientům, jako jsou finanční instituce, podniky nebo komunální objekty (O PPF bance, 2013).

Z náčrtu bankovních trendů vyplývá, že banky spolu budou více soupeřit. Otázkou zůstává, jak budou banky flexibilní v přechodu na nové platformy, vytváření nových aplikací apod. Uživatel z tohoto souboje může získat další výhody, ať už v rozšíření nabídky komunikačních kanálů, v přizpůsobení bankovních produktů na míru klientům i zařízením, zjednodušení aplikací, větší intuitivnost jejich ovládání atd.

2. Útoky na internetové bankovnictví

Internetové bankovnictví je v současnosti jednou z ohrožených finančních služeb. Setkávají se zde dva motivační aspekty: na jedné straně to jsou finanční prostředky, na druhé nezabezpečené prostředí internetu, jakožto komunikačního kanálu, přes který uživatelé přistupují ke svým bankovním účtům. Internet je ideální prostředí pro virtuální krádež, protože, jak říká Wall: to je prostředí, kde jsou peníze. Jako další výhodu internetu uvádí, že web svou povahou umožňuje spáchat milion krádeží, která každá stojí jeden dolar. To je určitě jednodušší a méně odhalitelný způsob, než provést jednu bankovní loupež za milion dolarů (Wall, 2007). Útočníci také rychle změnili cíl útoků, když zjistili, že k penězům je lepší přístup ze strany zákazníků. Výsledkem bylo přesunutí zájmu ze serverů na koncové uživatele (James, 2007). Tento prvek je nejméně zabezpečený. Samotní uživatelé neznají bezpečnostní pravidla pro práci se službou, a tudíž je jednoduché je oklamat a přístupové údaje od nich prostě vylákat (Miko, 2009). Za zneužití svých počítačů navíc nesou odpovědnost sami klienti internetového bankovnictví[26]. Dalšími výhodami jsou: relativní jednoduchost útoku nebo nízká šance na dopadení útočníka.

Napadený může být každý prvek internetového bankovnictví, tedy banka, komunikační kanál nebo klient. Řazení kapitol, tj. útoků, odpovídá právě procesu internetového bankovnictví, který je popsán v první části[27]. V podkapitolách tedy budou rozebrány útoky na uživatele, útoky na komunikační kanál, útoky na webovou aplikaci internetového bankovnictví a útoky na bankovní server.

2.1. Útok na uživatele

Nejjednodušší metodou, jak zneužít internetové bankovnictví, je ukrást identitu uživatele pomocí podvodně získaných osobních přihlašovacích údajů, jako např. uživatelské jméno, heslo nebo PIN. Útočník se pomocí těchto údajů přihlásí do bankovního systému a z účtu klienta odcizí finanční prostředky. Jedná se tedy o narušení autentizačního procesu, který se útočník snaží překonat a přihlásit se do systému pod cizí identitou.

Možností, jak přihlašovací údaje od uživatele získat, je několik: hádání hesla, phishing, pharming nebo malware. Tyto metody bývají kombinovány za účelem jednoduššího a méně nápadného dosažení cíle[28]. Phishing nebo pharming tak může potřebovat pomocníka v podobě malware v počítači uživatele apod.

2.1.1. Útok na hesla

Systémy, které vyžadují pro přihlášení pouze uživatelské jméno a heslo, jsou náchylné k útokům na hesla, jako je třeba hádání hesel a útok hrubou silou. Z bank využívá k přihlášení pouze uživatelské jméno a heslo např. internetové bankovnictví Fio banky nebo mBanky. Uživatelské jméno a heslo se dá uhádnout několika způsoby:

---

[26] Více v kapitole 1.3.5.

[27] Proces je popsán v kapitole 1.1.

[28] Termín, označující tyto kombinace, zní: „smíšená hrozba“ („blended threat“). Více viz stranu 29.

útočník může mít k dispozici databázi uživatelů, poskytnutou insiderem, nebo může vědět, jak jsou uživatelská jména a hesla vytvářena[29] (Todorov, 2007).

Pokud útočník nezná způsob vytváření hesel, může použít útok hrubou silou za použití tzv. prolamovače. Tento nástroj zkouší kombinace znaků, které se v autentizačním procesu používají. Může používat buď známá slova z vlastní databáze, nebo všechny kombinace znaků, které mají potřebnou délku. Po zjištění správného hesla jej prolamovač pošle útočníkovi. Např. zjištění PIN, tj. kombinace číslic, která má délku čtyř znaků, by trvala několik sekund (Todorov, 2007). Jako optimální se jeví kombinovat velká a malá písmena s číslicemi, s minimální délkou hesla 8 znaků[30]. Prolomit takto vytvořené heslo by prolamovači trvalo přibližně 7 let (Jirovský, 2007).

Banky se proti těmto útokům brání časovým intervalem mezi pokusy o zadání hesla, požadavky na složitost hesel nebo omezením pokusů o autentizaci (Jirovský, 2007). Po překročení počtu pokusů je zpravidla vyžadována další informace, např. odpověď na bezpečnostní otázku, kterou klient zadal dříve. Další možností, jak lze bankovní účet odblokovat, je osobní návštěva bankovní pobočky. Na pobočce klient zpravidla musí předložit identifikační kartu (tedy občanský průkaz apod.). Některé banky umožňují odblokování internetového bankovnictví také telefonicky.

2.1.2. Phishing

Phishing je technika e-mailového útoku na citlivá data uživatelů, která využívá prvků sociálního inženýrství. Snaží se uživatele přesvědčit, aby provedl nějakou akci, např. klikl na odkaz v e-mailu. Phishing tedy cílí přímo na uživatele a jeho nepozornost nebo neschopnost rozlišit falešné zprávy od pravých (Wall, 2007). Z toho důvodu bývá označován také jako brand spoofing, tedy zneužití značky. Pojmenování metody vychází z anglického slova *„fishing"*, což znamená rybaření. Útočník totiž nahazuje oběti „háček", a snaží se ji přimět, aby se do něj „zakousla". Dále se rozlišuje specifická varianta phishingu, která se nazývá „spear phishing"[31]. Tato metoda se zaměřuje na specifické cíle, jako např. na uživatele internetového bankovnictví určité banky (Wall, 2007, str. 227).

Při phishingu útočník rozesílá falešné e-mailové zprávy, které se tváří jako odeslané pravou finanční institucí[32]. Tyto e-maily mohou oběť buď pomocí odkazu přesměrovat na falešné webové stránky, nebo jej mohou vyzvat k zadání údajů přímo do zprávy. Cílem je získat od oběti citlivé údaje, jako je uživatelské jméno a heslo, PIN, číslo a dobu platnosti platební karty apod., a poté napodobit virtuální identitu oprávněného uživatele. Výhodou tohoto typu útoku je, že při správné formulaci e-mailu pomocí sociálního inženýrství může oběť prozradit velké spektrum informací, počínaje výše uvedenými údaji a konče odpověďmi na bezpečnostní otázky.

---

[29] Raiffeisen Bank používá jako uživatelská jména rodná čísla. Dále to může být datum narození, začátek e-mailové adresy apod.

[30] Přesto se doporučuje používat hesla delší než 10 znaků a kombinovat také s dalšími typy znaků.

[31] Dále v textu budu používat pouze pojem "phishing".

[32] Útočník samozřejmě může zneužít i jinou instituci. Další napadené služby byly např. na PayPal, eBay apod.

Použitím metod sociálního inženýrství se útočník snaží oběť zmanipulovat, aby si myslela, že „musí poskytnout specifické informace nebo vykonat specifickou akci"[33] (Todorov, 2007). Útočník se zpravidla vydává za správce systému, vedoucího pracovníka pro bezpečnost apod. Uživatel je nejprve informován o zablokování účtu, o zamítnutí platební transakce atd., a poté je vyzván k aktualizaci přihlašovacích údajů nebo vybídnut k vyjádření spokojenosti s užíváním systému. Dále je na něj vyvinut nátlak pomocí formulací jako: „pokud do 24 hodin údaje nepotvrdíte/nezměníte, váš účet bude zablokován", apod. Další znaky phishingového e-mailu jsou: odkaz v e-mailu vede jinam, než na stránky banky (může být např. maskován použitím IP adresy), odkaz využívá nezabezpečený protokol (http) místo zabezpečeného (https) apod.

James dále uvádí tři typy útoku na uživatele, který klikne na odkaz v phishingovém e-mailu: útok pomocí falešné identity, útok přesměrováním a útok pomocí vyskakovacích oken (James, 2007). Útok pomocí falešné identity spočívá ve vytvoření kompletní falešné stránky napodobující pravou stránku společnosti včetně grafických prvků apod. Tento způsob je nejjednodušší, a tudíž nejoblíbenější. Při útoku přesměrováním se útočníci snaží uživatele přesvědčit k zadání svých údajů přímo do zprávy. Citlivé údaje se kliknutím odešlou útočníkovi, uživatel je následně přesměrován na pravou stránku. Systém jej mnohdy dokonce přihlásí díky využití prostředníka[34]. Uvedený postup připadá v úvahu u institucí, zasílající svým zákazníkům e-maily s výhodnými nabídkami nebo novými službami, např. eBay, PayPal nebo Amazon. Nevýhodou tohoto postupu je vysoké riziko odfiltrování e-mailu pomocí antispamových filtrů. Poslední jmenovaný útok, tzn. pomocí vyskakovacích oken, spočívá v tom, že po kliknutí na odkaz v e-mailu je klient přesměrován na stránku pravého internetového bankovnictví. Před ni je ale vloženo vyskakovací okno, které uživatele vyzve k zadání přihlašovacích údajů. Kvůli blokování vyskakovacích oken ve většině prohlížečů je tento útok nejméně efektivní (James, 2007).

Dalšími druhy phishingu, které využívají jiné komunikační kanály, jsou smishing, zneužívající textové zprávy, nebo vishing, zaměřující se na hlasové zprávy přenášené pomocí protokolu VoIP[35]. Uživatel tak může být opět naveden na falešné stránky internetového bankovnictví. Phishingový e-mail se používá také jako nosič pro přenos malware. Ten se může ukrývat buď v příloze e-mailu nebo v odkazu na stránku, obsahující malware[36] (Spear Phishing E-Mail, 1989).

Dalo by se očekávat, že bude procento phishingových útoků klesat, vezmeme-li v potaz opakované provádění útoků téměř nezměněným způsobem. Avšak výzkumy tento předpoklad nepotvrzují, phishingové e-maily si stále drží svou pozici (McAfee, 2013; European Comission, 2012; APWG, 2012). Nejnapadanější službou zůstává finančnictví, nepočítaje platební služby[37] (APWG, 2012).

Příčinou stálé pozice phishingových e-mailů je ten, že nejen uživatelé, ale i phisheři se stále učí. Zatímco dříve bylo jednoduché phishingový e-mail odhalit, např. díky špatné češtině, v současnosti jsou útoky daleko sofistikovanější a náročnější

---

[33] „Social engineering techniques involve the attacker tricking the user into believing that he (the user) needs to provide specific information or perform a specific action."

[34] Více o útoku pomocí prostředníka, neboli Man-in-the-middle, v kapitole 2.3.1.

[35] Voice over Internet Protocol

[36] Překlad autorky.

[37] Překlad autorky.

na pozornost uživatelů. Uživatelé by si nicméně měli při otvírání e-mailu od banky uvědomit, že banky tímto způsobem komunikují zřídka, zpravidla na vyžádání klienta, a nikdy nechtějí po klientech potvrzování nebo zadávání údajů do e-mailu. I James píše, že komunikace prostřednictvím e-mailu je pro obchodní účely již nevyužitelná (James, 2007).

2.1.3. Pharming

Pharmingem rozumíme automatizovanou podobu phishingu, která není založena na sociálním inženýrství. Klasický pharming napadá DNS[38] servery, převádějící jmennou adresu na IP adresu. IP adresa, tvořená číslicemi, slouží jako unikátní lokalizace webové stránky na internetu. IP adresy, určené strojům, plní především požadavek na strojovou srozumitelnost. Vzhledem k nesnadnému zapamatování IP adresy pro uživatele se využívá právě DNS adresa, tedy doménová adresa, tvořená názvem stránek a dalšími atributy, např. územní doménou[39]. Tyto adresy jsou pro klienty srozumitelnější, a jako takové lépe zapamatovatelné.

Při pharmingu tedy dojde k automatickému přesměrování uživatele po zadání webové adresy do prohlížeče na závadnou webovou stránku, využívající stejných vizuálních a dalších znaků jako ta pravá (Wall, 2007). Kvůli zneužití převaděče adres se v adresovém řádku prohlížeče také zobrazí správná adresa (Miko, 2009).

DNS cache poisoning je metoda, která napadá vyrovnávací paměť DNS. Ta se používá pro překládání DNS adresy pomocí záznamů uložených při předchozí relaci za účelem úspory času uživatele. V minulosti byly např. napadeny DNS cache poskytovatelů internetového připojení. Dále mohou být nakaženy lokální soubory, uložené v počítači uživatele a řídící vzdálené požadavky DNS. V tomto případě tedy dojde k napadení paměti počítače, v níž jsou uloženy dříve použité IP adresy, pomocí e-mailu obsahujícího malware. Malware změní uložené záznamy IP adres, tzn., že klient je při zadání adresy opět přesměrován na závadné stránky[40] (DNS poisoning, 2011).

Napadené mohou být také aplikace internetového bankovnictví. Banky se proti pharmingu brání využitím specifických prvků na stránkách internetového bankovnictví, např. personalizovaným loginem[41]. Falešné webové aplikace se chovají nestandardně a mohou vyžadovat více informací než normálně za účelem vylákání dalších údajů.

2.1.4. Malware

V předchozích kapitolách byla několikrát naznačena pomoc malware při útocích na internetové bankovnictví. Malware, neboli škodlivý software, má totiž mnoho způsobů využití, např. při pharmingu může měnit záznamy IP adres v počítači uživatele. Při phishingovém útoku bývá nakažený e-mail nosičem malware. Závadný program dále lze kombinovat s ostatními technikami útoků, např. XSS, za účelem efektivnějšího napadení systému. Tyto kombinace se označují jako „smíšené hrozby"

---

[38] Domain Name Server

[39] V České republice je to doména .cz.

[40] Překlad autorky.

[41] Viz stranu 18.

neboli „blended threats". Podle Walla určuje konkrétní kombinaci malware zamýšlený účel útoku (Wall, 2007, str. 225). James také definuje tento útok jako použití více metod vstupu, včetně trojského koně, červa i útoku XSS[42] (James, 2007, str. 129). „Smíšené hrozby" se také díky kombinování vlastností virů a červů dají v systému hůře odhalit.

Malware je definován jako software, který po svém spuštění v počítači zahájí škodlivou činnost za účelem poškodit, zničit nebo ukrást informace z napadeného systému. Jedno z možných dělení je podle způsobu šíření, kdy rozlišujeme červy a viry. Červi nepotřebují ke svému šíření sítí činnost uživatele ani nositele. Šíří se pomocí bezpečnostních chyb v systému. Viry naopak napadají statické soubory a vyžadují asistenci uživatele pro své šíření. Kromě virů a červů řadíme k malware trojské koně. Trojského koně si uživatel většinou stáhne z internetu jako skrytou součást jiného programu[43]. Tato část programu poté tajně vykonává škodlivou činnost, zatímco program funguje standardním způsobem.

Kromě otevření počítače pro útočníka je také důležité malware a jeho činnost v počítači skrýt. K tomu slouží rootkit, tedy soubor postupů a technik, používaný právě za tímto účelem. Tyto nástroje často tvoří součást malware a snaží se jeho činnost zamaskovat, aby nedošlo k jeho odhalení[44] (Paget, 2011).

Backdoors neboli zadní vrátka jsou kódy, umožňující útočníkovi vzdálenou správu počítače. Útočník tak může převzít ovládání počítače, zatímco oběť o tom nemá tušení. Tento kód je nesnadné v počítači odhalit. Backdoors využívají pro ovládání systému službu, spuštěnou na síťových portech počítače[45] s vysokým číslem, nebo se maskují na portech standardních síťových služeb. Maskování se používá proto, že díky němu nedochází k jejich odfiltrování firewally[46] (Jirovský, 2007).

Pro zjištění otevřených portů v systému, tedy i spuštěných služeb, se používají skenery. Tyto programy nejsou nelegální, a lze je tedy stáhnout nebo koupit. Útočník ale pomocí skeneru může získat základní informace o počítači, operačním systému apod. Bezpečnostní aplikace se snaží tyto skenery odhalovat a blokovat, neboť skenování portů může být následováno útokem na systém (Jirovský, 2007).

K šíření malwaru se mj. používají botnety, tedy sítě počítačů, které jsou infikovány trojskými koni, umožňujícími útočníkovi vzdálenou správu a ovládání počítače. Botnety slouží dále k rozesílání nebo předávání spamů nebo k útokům DDoS[47]. Vlastník nakaženého systému nemá o kontrole a využití svého počítače k těmto účelům ponětí (Wall, 2007).

Malware účinkuje po omezenou dobu, neboť se dá očekávat, že po odhalení bude následovat adekvátní reakce poskytovatelů antivirové ochrany (James, 2007). Proto jsou útočníci nuceni malware neustále modifikovat a vyvíjet. Uživatel si ale musí udržovat svůj antivirový a anti spyware program aktualizovaný, neboť aktualizace obsahují údaje o nových druzích malware.

---

[42] XSS útoky jsou popsány v kapitole 2.2.1.

[43] Většinou jsou trojské koně součástí bezplatných her, freeware utilit a programů a dalších souborů (Jirovský, 2007).

[44] Překlad autorky.

[45] Síťové porty slouží při komunikaci v počítačových sítích k rozpoznání aplikace. Např, protokol HTTP využívá port 80 nebo e-mailový protokol SMTP využívá port 25 (James, 2007).

[46] Více o firewallech a filtrování portů na straně 21.

[47] O DDoS útocích v kapitole 2.4.2.

Pro uživatele internetového bankovnictví představuje nejvyšší riziko spyware, který se snaží odhalit přihlašovací údaje uživatele nebo komunikační proces. Ostatní malware je důležitý jen v kombinacích, jejichž příklady jsou popsány výše.

2.1.4.1. Spyware

Jedním z typů malware, využitelného pro útok na internetové bankovnictví, je spyware neboli sledovací program. Spyware tajně prohlédne počítač uživatele, a poté z něj získá a odešle útočníkovi osobní informace uživatele. Může tedy najít přihlašovací certifikáty, sloužící k autentizaci uživatele v bankovním systému[48], které má uživatel uložené na pevném disku v počítači. Spyware dále sleduje chování uživatele či systému nebo navštěvované webové stránky (Jirovský, 2007). Spyware se také dokáže zaměřit na komunikaci mezi klientem a serverem. V tomto případě se označuje jako BHO, tedy Browser Helper Object. BHO je nástroj, který pomáhá např. se sledováním procesu stahování a s dalšími užitečnými službami v prohlížeči (James, 2007). Spyware komunikaci mezi klientem a serverem nahrává a monitoruje provoz dat po síti[49].

Jeden z typů spyware tvoří keylogger, což je nástroj monitorující úhozy na klávesnici. Z dat získaných keyloggerem může útočník rekonstruovat zadávaná hesla a další přístupové údaje (Wall, 2007). James uvádí, že keyloggingový malware je schopen vygenerovat velké množství dat, které je potřeba posléze přetřídit. V tomto automatizovaném procesu se tedy mohou užitečné údaje ztratit. Oběť také nemusí prozradit údaje, které útočník potřebuje (James, 2007). Proto keyloggery v současnosti dokáží sledovat jen údery kláves v souvislosti s určitými webovými stránkami. Získaná data se poté uloží v databázi a uschovají se pro pozdější offline analýzu (Todorov, 2007).

Útoky na internetové bankovnictví pomocí spyware proběhl např. v roce 2006, kdy došlo ke krádeži přístupových certifikátů a hesel do internetového bankovnictví Komerční banky. Následně byly z postižených účtů odcizeny finanční prostředky. Dále se objevil spyware Sinowal, který zobrazoval v prohlížeči uživatele falešné stránky Servis 24, tj. internetového bankovnictví České spořitelny (Matyáš a Krhovják, 2008). Tento program mohl krást osobní informace uživatele tím, že při přihlášení do internetového bankovnictví požadoval více údajů, než bylo obvyklé (Aktuality, 2008). Také mohl nahrávat další malware[50] (Trojan-PSW:W32/Sinowal.CP, 2009).

2.1.5. Operace High Roller

Tyto útoky jsou příkladem smíšené hrozby (blended threat), kombinující malware Zeus nebo SpyEye[51], webové injektáže a CSS útok. Tato smíšená hrozba se jmenuje High Roller a zaměřovala se na krádeže financí z bankovních účtů. Útoky se nejdříve objevily na přelomu let 2011 a 2012 v Evropské unii. Poté se změnilo zacílení

---

[48] Více o certifikátech v kapitole 1.3.2.

[49] Překlad autorky.

[50] Překlad autorky.

[51] Zeus a SpyEye jsou trojské koně, které kradou informace a monitorují údery kláves. Zeus se může sám aktualizovat a stahovat další programy díky propojení se vzdáleným serverem, a tím vlastně vytvoří zadní vrátka do napadeného počítače (Trojan.Zbot, 1995). SpyEye navíc monitoruje internetový provoz a umí přeposílat síťové pakety za účelem obejití firewallů (Trojan.Spyeye, 1996).

na Spojené státy a Kolumbii. Útočníci za pomoci dalších nástrojů instalují do počítače oběti malware Zeus a SpyEye, který dokáže kontrolovat počítač a aplikace. Dále jsou schopni do prohlížeče nainstalovat HTML injekce[52], odesílající údaje v přihlašovacích formulářích útočníkovi a měnící obsah toho, co uživatel vidí ve svém prohlížeči.

Inovativnost těchto útoků spočívala v tom, že dokázaly překonat dvoufaktorovou autentizaci, zaměřily se přímo na bohaté cíle a byly z velké části automatizované[53] (Flash note, 2012). Automatizace většiny procesů umožnila opakované krádeže financí, jakmile byl systém jednou spuštěn v internetovém bankovnictví. Dále útočníci přesunuli provedení podvodné transakce z klienta na útočný server za účelem lepšího zakrytí těchto transakcí a způsobu jejich provedení, jako je např. způsob interakce útočného serveru se systémem internetového bankovnictví. Přemostění dvoufaktorové autentizace se děje za pomoci samotného uživatele, který je vyzván k poskytnutí údajů potřebných k obejití autentizačního kalkulátoru[54]. Jako důvod se uvádí vytvoření jednorázového hesla nebo digitálního tokenu. Útočníci dále obchází autorizaci plateb tím, že si všechny údaje potřebné pro autorizaci platby vyžádají již při autentizaci pomocí rozsáhlého JavaScriptového útoku, vkládajícího do stránky webové injekce. Malware po přihlášení zdrží klienta pomocí falešné hlášky „Prosím počkejte" a na pozadí provede transakce pomocí legitimního digitálního tokenu. Způsob provedení útoku se může kopírovat mezi účty stejné bankovní platformy. Tyto procesy probíhají automatizovaně.

Balíček smíšené hrozby obsahuje také rootkit k zakrytí akcí malwaru před obranným software. Odkazy a kód ve webových injekcích byly zakódovány a zašifrovány za účelem prevence odhalení. Útočné servery se často stěhovaly, aby se zabránilo možnosti vystopování serveru a umístění serveru na blacklist. Komponenty na straně serveru byly také skryty. Malware na straně klienta dále vyhledával a mazal potvrzovací e-maily a odkazy na výpisy. Malware nakonec ještě měnil údaje o provedených bankovních transakcích apod., které se zobrazily na klientově obrazovce. Útočníci znali systémy on-line bankovnictví a vyhýbali se provedení podezřelých úkonů. Webové injekce napodobovaly chování uživatele v systému[55] (Marcus a Sherstobitoff, 2012).

Z popsaného útoku lze vidět, že útočníci mají k dispozici vysoce sofistikované nástroje, které je velmi obtížné odhalit. Pro uživatele tedy představují velké riziko.

2.2. Útoky proti webovým aplikacím

Útoky proti webovým aplikacím cílí na webové prohlížeče. Tyto útoky se spustí v prohlížeči uživatele, který chce k aplikaci přistoupit. Způsobů, jak lze aplikaci napadnout, je více: napadení skriptovacího jazyka pomocí XSS, odesílání škodlivých požadavků mezi webovými aplikacemi pomocí XSRF, vložení škodlivých rámů metodou clickjacking nebo vložení jiného obsahu pomocí HTML injekce[56].

---

[52] O útoku pomocí HTML injekce v kapitole 2.2.4.

[53] Překlad autorky.

[54] "smart card reader plus pin pad entry" (Marcus a Sherstobitoff, 2012)

[55] Překlad autorky.

[56] HTML injekce byla využita při útoku pomocí virů Zeus a SpyEye, viz předchozí kapitolu.

2.2.1. XSS útok

Útok XSS patří ke složitějším útokům na webové aplikace na straně uživatele[57]. Při útoku XSS útočník najde bezpečnostní chybu na stránkách webové aplikace a do té vloží škodlivý kód napsaný ve skriptovacím jazyce, např. v nejrozšířenějším JavaScriptu. Útočný kód je poté realizován v prohlížeči uživatele (Kümmel, 2012). Stránky internetového bankovnictví běžně využívají JavaScriptové prvky. V prohlížečích klientů dále musí být použití JavaScriptu povoleno, jinak není bankovní aplikace funkční. Tato slabá místa webové aplikace mohou být kromě JavaScriptu např. Flash nebo Java aplikace (Závodský, 2011). Také Javu využívá poměrně hodně aplikací internetového bankovnictví[58].

Při útoku XSS tedy nedochází k útoku přímo na webový server, ale na prohlížeče uživatelů, ve kterých dojde k vykonání útočného kódu. Pomocí skriptu lze změnit vzhled a obsah stránek, ukrást přihlašovací údaje uživatele nebo obejít bezpečnou komunikaci (Turek, [22.3.2009]).

Útok XSS se dělí na tři základní typy: trvalý, okamžitý a založený na DOM[59]. Trvalý XSS útok spočívá ve vložení škodlivého kódu do datového úložiště aplikace. Kód se tedy spustí při každém zobrazení webové stránky. Tento typ se objevuje v diskusních fórech a dalších stránkách, kde mohou uživatelé na web vložit svůj příspěvek, nebo v databázích[60].

U okamžitého útoku je skript vykonán okamžitě po odeslání požadavku na webové stránky a není nikde uložen. Skript tedy může být součástí webového odkazu jakožto jeden z jeho parametrů. Předávání nakaženého odkazu probíhá např. prostřednictvím e-mailu. Pro sbírání dat z přihlašovacích formulářů se používá metoda, při níž se skript nachází místo v parametru odkazu v těle HTTP požadavku. V tomto případě odkaz nevede na aplikaci přímo, ale přes webovou stránku útočníka. Útočník si tak může připravit např. stránku s chybovou hláškou, která uživatele vyzve k opětovnému zadání přihlašovacích údajů. Poté ho do aplikace přihlásí. Údaje jsou ale mezitím odeslány útočníkovi.

Při útoku založeném na DOM probíhá vložení klientského skriptu, např. cookies[61], na straně webového prohlížeče pomocí JavaScriptu. Útok se zobrazí v prohlížeči, kam je nahrán ze strany klienta. Samotná webová stránka se tedy nemění, ale na straně klienta se skript chová odlišně (Kümmel, 2012).

---

[57] Proto jej Lance James označuje jako útok proti uživateli (James, 2007, str. 122).

[58] S Rozhraním Java měla na přelomu roku 2012 a 2013 problémy Komerční banka. Stránky internetového bankovnictví této banky bez nové instalace Javy nebyly funkční.

[59] Document Object Model - určuje hierarchii objektů na stránce. "DOM umožňuje přistupovat k objektům na stránce pomocí programovacích jazyků, mezi které patří i JavaScript." (Kümmel, 2012, str. 24)

[60] V tom případě se nazývá SQL injection.

[61] Cookies jsou malé textové soubory, které jsou vytvářeny webovou stránkou. Ta je pošle do počítače uživatele, kde jsou uloženy, a odkud jsou při každém požadavku na danou webovou stránku odeslány. Cookies slouží k identifikaci uživatele, uložení preferencí apod.

2.2.1.1. Využití útoků XSS

Útok XSS lze využít ke krádeži cookies, k vytvoření XSS keyloggeru[62], k ukradení přihlašovacích údajů pomocí vyskakovacího okna a mnoha dalším. Zde se ale budu zabývat pouze těmito, neboť jiné (např. útok na vnitřní síť nebo zjištění navštívených stránek) mají pouze okrajové využití pro útok na internetové bankovnictví. V těchto útocích jde hlavně o krádež přihlašovacích údajů. XSS nacházejí své uplatnění také v instalaci malware do počítače uživatele nebo se objevují v kombinaci s jinými technikami, jako např. právě malware.

Aplikace internetového bankovnictví běžně používají cookies pro zapamatování si klienta. Bez povolení cookies v prohlížeči nemusí být webové stránky plně funkční. Pomocí JavaScriptu lze ukrást cookie z vlastnosti document.cookie[63]. Skript, vložený útočníkem, se snaží hodnotu vlastnosti přečíst a odeslat na svůj server. Poté může cookie buď využít k odeslání požadavku na aplikace (viz XSRF) nebo k zakomponování do svého prohlížeče. V tom případě by útočník byl přihlášen jako pravý uživatel (Zahradnický, 2009).

Útočníci se dále snaží ukrást údaje zadávané do přihlašovacích formulářů. Na webové stránky je vložen skript, který odešle přihlašovací údaje útočníkovi. Skript může uživatele po odeslání údajů přihlásit zpět do webové aplikace. Uživatel tak nepozná, že mu údaje byly ukradeny. Přihlašovací údaje mohou být odcizeny pomocí vyskakovacích oken. Tento útok spočívá v umístění okna před webové stránky. Napadení neuniknou ani webové stránky finanční instituce atd. Uživatel se na stránku dostane pomocí odkazu v e-mailu. Vyskakovací okno se žádostí o vyplnění citlivých údajů se poté otevře během přesměrovávání uživatele na skutečné stránky. Využitím JavaScriptu se snižuje možnost odhalení. Většina prohlížečů ale vyskakovací okna blokuje, tím je efektivita tohoto útoku snížena (James, 2007). Skript může také zaznamenávat stisknuté klávesy. Keylogger ovšem běží pouze v okně webového prohlížeče, které daný skript obsahuje. Nezaznamenává tak údaje ze všech webových aplikací (Kümmel, 2012).

2.2.2. Cross-site request forgery

Tento útok označuje odeslání HTTP požadavku útočníkem z jedné webové aplikace do druhé pod identitou oběti. Útočník se tak snaží uživateli podstrčit odkaz (např. e-mailem nebo na svých webových stránkách) s takovými hodnotami v proměnných, které má uživatel na server odeslat, a tím provést určitý úkon právě ve prospěch útočníka. Uživatel sám by takovou akci neprovedl. Tuto zranitelnost můžeme nalézt ve většině webových aplikací (Kümmel, 2012).

Veškerý pohyb a vykonávání akcí na internetu spočívá v odesílání HTTP požadavků. Jedná se tudíž o základní způsob práce s webem. Z tohoto pohledu dochází k širokému uplatnění XSRF[64] útoků. Vzhledem k tomu, že je protokol HTTP bezstavový, nedochází k zapamatování údajů nebo akcí uživatele webové aplikace. Z tohoto důvodu se po autentizaci uživatele do aplikace vytváří tzv. sezení (session),

---

[62] Více informací o funkci keyloggeru lze nalézt na straně 31.

[63] Vlastnost document.cookie je vlastností objektu document, specifikovaného pomocí Objektového modelu dokument (DOM).

[64] Občas bývá také označován jako CSRF.

během kterého si aplikace pamatuje identitu uživatele a jeho předchozí akce. Uživatel tak nemusí svoji identitu a oprávnění pro přístup do aplikace opakovaně potvrzovat při každém zadání požadavku HTTP. K tomu slouží identifikátor sezení (session id), uložený na straně serveru a zároveň odeslaný klientovi, jehož identita se tímto při každém zaslání potvrzuje. V internetovém bankovnictví je session id šifrováno.

Strany si mohou session id vyměnit jednak přímo v URL nebo pomocí cookies. Útočník se snaží identifikátoru zmocnit např. pomocí XSS[65] nebo útoku ze středu[66], a poté donutit uživatele, aby odeslal škodlivý požadavek. Tento způsob se označuje jako session hijacking, tedy krádež relace.

Zmocnění se session id bývá označováno také jako session riding, kdy musí být pro provedení akce uživatel k webové aplikaci v okamžiku útoku přihlášen. V tomto případě útočník naláká oběť na odkaz, který má v parametrech příkaz k provedení falešné transakce. Kliknutím na odkaz nebo otevřením závadných stránek se příkaz v bankovní aplikaci vykoná. Zranitelnost vůči tomuto útoku se objevila např. v roce 2009 na stránkách americké banky Capital One (Dobiáš a Říha, 2009).

Jako ukázka provedení XSRF útoku na on-line bankovnictví může posloužit příklad, který uvádí Tomáš Zahradnický: v tomto případě se session id, jakožto nezbytná součást bankovní transakce, ukládá do cookies. Poté, po spuštění škodlivého kódu od útočníka, je díky přítomnosti cookies se správnou autentizací a zadání příkazu z počítače uživatele provedena bankovní transakce. Tato transakce převádí finance na účet útočníka (Zahradnický, 2011).

2.2.3. Clickjacking

Při clickjackingu se útočník snaží přimět samotného uživatele, aby provedl určitou akci. Na stránku, kterou chce útočník napadnout, jsou vloženy rámy zakrývající plochy stránky kromě interaktivního prvku, okna formuláře apod. V rámech, zakrývajících stránku, se poté uvádějí informace, které mají uživatele přimět k využití prvku. Útočník tak v podstatě stránku natolik modifikuje, aby přiměl uživatele provést právě tuto akci.

Podle testu, provedeného Rastislavem Turkem, byly v roce 2009 pouze tři bankovní stránky v ČR odolné proti clickjackingu, a to stránky Komerční banky, Citibank a mBank (Turek, 2009).

2.2.4. HTML Injection

HTML injection je útok, při kterém dojde k vložení HTML obsahu do webových stránek. Tento obsah není v podobě skriptů, ale dalších HTML tagů, jako např. pro obrázky nebo rámy. Jinak se ale postupuje stejně, jako když vkládáme skripty při Cross Site Scripting útoku.

Vložení HTML obsahu bylo využito při kombinovaném útoku „High Roller", popsaného v kapitole 2.1.5.

---

[65] Viz kapitolu 2.2.1.

[66] Viz kapitolu 2.3.1.

2.3. Útok na komunikaci

Při tomto útok, konkrétně při útoku ze středu, dojde k napadení komunikačního procesu na cestě mezi uživatelem a bankovním systémem. Útočník může zneužít kterýkoli prvek, nejjednodušší je napadnout např. hotspot[67] v kavárně, kde se uživatelé připojí ke svému bankovnímu kontu (Pletzer, 2008).

2.3.1. Útok ze středu

Při útoku ze středu, který bývá také označován jako Man-in-the-middle, se útočník snaží o zachycení a převzetí kontroly komunikace mezi klientem a serverem. Předpokladem útoku je nedostatečné ověření komunikujících stran nebo nedostatečné zabezpečení komunikace. Při útoku ze středu útočník díky umístění do středu komunikace odposlouchává zprávy, které si uživatel a server vymění. Při předávání zpráv mezi stranami lze zprávy pozměňovat v útočníkův prospěch. Může také navázat spojení s oběma stranami a v dialogu vystupovat jako protistrana (Doseděl, 2007). Todorov tento způsob nazývá session hijacking, kdy útočník převezme identitu jedné z komunikujících stran[68] (Todorov, 2007).

James uvádí čtyři způsoby, jak lze převzít komunikaci: oklamání ARP, oklamání DNS[69], vychýlení URL nebo HTML[70] a malware[71]. ARP, tedy Adress Resolution Protocol, překládá IP adresu na adresu hardwarového rozhraní. Útok cílí na lokální paměť ARP klienta, a proto se nazývá také ARP cache poisoning. Útočník se snaží oklamat ARP paměť tím, že vysílá požadavky a odpovědi, ARP klienta si poté do své paměti zaznamená adresu hardwarového rozhraní útočníka. Útok tak spočívá v tom, že se útočník usadí v lokální síti a snaží se vydávat za směrovač nebo přístupový bod k internetu. Veškerá komunikace klienta se následně přesměruje přes počítač útočníka (James, 2007). Pro aplikace internetového bankovnictví je nebezpečné, pokud se klient přihlašuje do bankovního systému v nezabezpečených bezdrátových sítích, např. v kavárně.

Útočník může překonat také zabezpečenou komunikaci, a to vytvořením dvou samostatných zašifrovaných relací. V případě, že se mu to podaří, prohlížeč uživatele informuje o neplatnosti certifikátu. Uživatelé ale mají sklon tato varování ignorovat, protože nedokážou obsáhnout důsledky takové hrozby (Man-in-the-middle attack, 2009).

Jako obrana proti útokům ze středu se používá oboustranná autentizace, šifrování a ochrana integrity dat[72] (Todorov, 2007).

---

[67] Místo, kde mají uživatele k dispozici bezdrátové připojení k internetu.

[68] O session hijacking jsem psala v souvislosti s útoky XSS na straně 34. Při útoku ze středu lze session ID ukrást také, ale používá se jiný způsob (Session hijacking, 2011).

[69] Tato technika se nazývá pharming. Blíže ji popisuji na straně 29.

[70] Jedná se o phishing, který je popsán v kapitole 2.1.2.

[71] Více o malware v kapitole 2.1.4.

[72] Autentizace je popsána v kapitole 1.3.3., šifrování a ochrana integrity dat v kapitole 1.3.2.

2.4. Útok na bankovní server

Dalším možným cílem útoku může být bankovní server. Útočníci se spíše než o provedení podvodů snaží o krádež databáze klientských přihlašovacích údajů apod. (Miko, 2009). Útočníci ale mohou databázi využít i v případě, že obsahuje pouze seznam klientů. Tyto údaje totiž lze posléze využít jako zdroj informací pro lepší cílení phishingových e-mailů apod. Bankovní server lze napadnout zevnitř pomocí insiderů. Předpokladem útoků jsou organizační nebo aplikační chyby (Vorlíček a Suchý, 2005), tj. např. soustředění správy systému pouze do jedněch rukou. To svádí správce k provedení útoku na systém. Na straně banky mohou selhat kontrolní mechanismy, tedy např. metoda čtyř očí[73].

K napadení bankovního serveru dochází i z vnějšího prostředí. Opět se jedná o zanedbání základních bezpečnostních pravidel. Jako příklad lze použít nastavení slabých hesel - systémoví a bezpečnostní architekti zapomenou změnit slabé heslo, nastavené při konfigurování systému, které většinou nesplňuje nároky na složitost hesla. Útočník může prolomením dosáhnout přístupu do systému a k autentizačním procesům[74] (Todorov, 2007).

Přidanou hodnotou útoků na internetové bankovnictví je poškození image banky. Z toho důvody mají banky snahu útoky utajit a s oběťmi se vyrovnat jinou cestou. Útoky spáchané insidery také na veřejnost neproniknou. Výjimku tvoří banky v USA, konkrétně v Kalifornii, kde byla bankám stanovena povinnost zveřejňovat narušení jejich informačních systémů (James, 2007, str. 38). Pro klienty bank je toto samozřejmě výhoda, neboť nejsou odkázáni pouze na média jako na informační zdroj o útocích na banky. Média totiž slouží jako zprostředkovatel, a ne zdroj primárních informací, může tedy dojít k jistému zkreslení[75]. V USA platí také Regulace E, která odpovědnost za útoky, i ty na koncovém zařízení, tj. u klienta, dává bankám (Matyáš a Krhovják, 2007). Tyto zákony taktéž slouží k větší transparentnosti poskytování bankovních služeb.

Uživatel se tedy o těchto útocích zpravidla nedozví, neboť banky za účelem udržení dobrého image organizace o útocích veřejnost neinformují. Tyto útoky proto nebývají hlášeny vyšetřovacím orgánům, banky je raději vyřeší samy (Matějka, 2002).

2.4.1. Případ Citibank

Jako příklad útoku na systém banky, při němž došlo k odcizení financí pomocí požadavků na počítačový systém řízení účtů klientů banky, můžeme použít útok na Citibank, který se uskutečnil v roce 1994. Při tomto útoku bylo z banky odcizeno přes 10 milionů dolarů. Pachatelem byla hackerská skupina vedená Vladimírem Levinem. Tento útok byl natolik významný, že v odborné literatuře se občas označuje jako počátek hackerského novověku (Matějka, 2002). Také byl nazván první mezinárodní

---

[73] Více o metodě čtyř očí na straně 22.

[74] Prolomení bankovního systému tímto způsobem se uskutečnilo v březnu 2013, kdy hackeři napadli server UniCredit Bank. Heslo správce systému údajně bylo "Banka123". Informace o tomto útoku nejsou oficiálně potvrzené (Unicredit Bank úpěla pod náporem hackerů, na web dali prohlášení, 2013). Přesto však internetové bankovnictví bylo chvíli mimo provoz (Krátkodobé omezení internetového bankovnictví, 2013).

[75] Více viz kapitolu 3.

bankovní loupeží provedenou přes síť (Internet Fraud Case - Citibank - Vladimir Levin, 2004).

Levin se nejprve dostal do počítačů Citibanky a zde získal seznam zákaznických čísel a hesel. Poté vnikl do počítačového systému pro řízení hotovosti[76] a provedl tam několik ilegálních transakcí. Celkem se přihlásil osmnáctkrát do tří korporátních účtů, a mezi červnem a říjnem 1994 z nich převedl finance.

V otázce přístupu do počítačového systému Citibanky instituce uvedla, že se Levin do systému dostal díky údajům z existujících účtů, které nebyly chráněny šifrováním. Zároveň existuje eventualita, že měl uvnitř bankovního systému komplice, tato možnost se ale nikdy nepotvrdila.

Levin byl později zatčen na letišti v Londýně a v roce 1998 byl odsouzen na tři roky a k pokutě 240 tis. dolarů. Citibank zvládla nahradit svým klientům téměř celou částku, ale stejně přišla o 20 nejlepších klientů. Také přijala bezpečnostní opatření, aby se tento případ už nemohl opakovat[77] (Internet Fraud Case - Citibank - Vladimir Levin, 2004).

2.4.2. DDoS

Narušit funkčnost internetového bankovnictví lze vyřazením provozu této služby pomocí DDoS útoku. DDoS útok je útok na webové služby, při kterém dojde kvůli vysílání velkého množství požadavků v krátkém čase (v řádu sekund) k zahlcení, a tím pádem k nedostupnosti služeb. Požadavky vysílá síť napadených počítačů (zombies), tzv. botnet[78] (Wall, 2007). Klienti se v případě přetížení webových stránek nedostanou na svůj účet, a tedy nemohou disponovat svými finančními prostředky přes internet. Útočníci se tímto způsobem snaží zviditelnit, neboť útokem na on-line bankovnictví bude poškozeno velké množství lidí. Výhody tohoto typu útoku tvoří jednoduchost a nízké náklady. Botnet lze totiž na internetu pořídit za nízké náklady.

Tento způsob útoku byl použit při vlně útoků na síťovou infrastrukturu České republiky v březnu 2013. V rámci tohoto útoku došlo nejprve k napadení zpravodajských serverů, jako např. Novinky.cz, iDnes.cz apod. Poté byl vyřazen webový portál Seznam.cz. Následně proběhl útok na webové stránky a internetové aplikace velkých bank. V případě útoků na banky nefungovaly kromě internetového bankovnictví také platební terminály u obchodníků (Aktuality: Informace o dočasné nedostupnosti on-line služeb, 2013). Nakonec byly vyřazeny weby mobilních operátorů. Podle zdrojů přicházely útočné požadavky z Ruska (Kybernetickými útoky se začala zabývat kontrarozvědka, 2013).

---

[76] „computerized cash management systém“

[77] Překlad autorky.

[78] Botnety jsou blíže popsány na straně 30.

3. Úloha médií v zobrazování kyberkriminality

Nejprve popíšu mediální kampaně a nutnost zobrazování bezpečnostních hrozeb a útoků v médiích, potom vybrané funkce médií relevantních pro mou práci. Následně se s přihlédnutím k zaměření praktické části diplomové práce budu věnovat popisu zpravodajství, poté specifikům on-line zpravodajství. Právě internetová zpravodajství tvoří výběrový soubor mého výzkumu.

Uživatele dále vychovávají mediální kampaně, které se snaží o větší opatrnost a obezřetnost při používání elektronických komunikačních prostředků při správě a manipulaci s financemi. Jako příklad lze uvést kampaně Bezpečný internet, což je nekomerční projekt velkých firem o bezpečnosti na internetu, nebo Jak na internet. „Seriál Jak na Internet je jedním z osvětových projektů sdružení CZ.NIC, správce národní domény .CZ a provozovatele služby mojeID." (CZ.NIC, 2012) Tento seriál byl vysílán Českou televizí, ale uživatelé se s ním mohou setkat i na webových stránkách kampaně. Další kampaně vytváří státní instituce, např. Ministerstvo vnitra ČR nebo Policie ČR. Na stránkách Policie ČR lze také projev kyberkriminality nahlásit.

Porozumění hrozbám, které kyberprostor ukrývá, je pro uživatele klíčové, protože vede k lepší obraně proti těmto hrozbám. Uživatelé tak mohou ovlivnit své chování směrem k větší bezpečnosti práce s bankovní aplikací. Důležitý zdroj informací o útocích na internetové bankovnictví tvoří internetová zpravodajství.

Média tak vytvářejí bezpečnostní mediální realitu, když se zajímají o bezpečnostní problémy současné doby. Bezpečnostní realita se zabývá existencí reálných bezpečnostních hrozeb a obranou proti těmto hrozbám. Jako taková se tedy věnuje rizikům a naopak zabezpečením vůči hrozbám, které se nacházejí v okolním světě. „Zobrazováním ‚odvrácené strany' bezpečí, tzn. osvětlováním ‚tmavých koutů' společnosti, průnik do různých forem násilí, kriminality (…), ale i do sofistikovaných podvodů (…) může být z hlediska potřeby poznávání bezpečnostní reality velmi užitečné." (Murdza in Urban a spol., 2011, str. 172) Média shledávám jako ideální prostředek pro zprostředkování takovýchto informací a zobrazování kyberkriminálních útoků více než žádoucí[79]. Proto je důležité, aby média přejala tato témata do své agendy.

Masová média tedy mohou uživatele určitým způsobem vychovávat, neboť „jako víme z mnohých výzkumů masové komunikace, čím častěji a nápadněji média o určité zprávě informují, tím se daná zpráva jeví pro čtenáře, posluchače nebo diváky významnější, a tím větší je i její vliv." (Hagen in Schulz a kol., 2011) Tato vlastnost médií se nazývá nastolování agendy a určuje, o čem se mluví. Na otázku, jak se o tématu mluví, potom odpovídá teorie rámování, což je proces ovlivňování veřejnosti a jeho průběh. Teorie rámování tudíž popisuje vztah médií a veřejnosti. Pracuje se s rámci, což jsou mantinely, v nichž uživatelé o události nebo jevu uvažují. Tyto rámy potom tvoří složitější a propracovanější struktury, do kterých jsou informace zařazovány. Určitá témata je možné vyzdvihnout, a tím jim určit v očích veřejnosti větší význam, a naopak jiná zase opomenout. Odlišnou formulací lze dosáhnout odlišného pochopení události. Tímto způsobem dochází k ovlivňování veřejnosti a k upření pozornosti na popisovaná témata (Tabery, 2009). Z toho vyplývá, že pokud bude

[79] Bohužel pro média je atraktivnější zobrazování vražd a násilných kriminálních činů. Tento fakt vyplývá ze zahraničních výzkumů (Murdza in Urban a kol., 2011).

pozornost zpravodajství určena právě na internetové bankovnictví a útoky na něj, dá se očekávat větší pozornost uživatelů zaměřená na prevenci a zabezpečení bankovních účtů. Teorie filtrování informací veřejnosti se nazývá gatekeeping. Ta říká, že média určují témata, kterým se budou věnovat a kterým ne. Pokud se tedy média rozhodnou, že problém kyberkriminálních útoků pro ně není zajímavý, mohou se rozhodnout tyto informace nezprostředkovat (Urban, 2011). To samozřejmě není pro uživatele žádoucí, z důvodů naznačených výše.

Média mají zprostředkovatelskou a informační funkci, kdy uživatelům přináší informace z dalších zdrojů, jako jsou tiskové agentury, státní instituce, nebo při zneužívání internetového bankovnictví vyšetřovací orgány a tiskové zprávy bank. Média v tomto případě zprostředkovávají obraz události, ke které veřejnost nemá přístup. Vytvářejí tedy vlastní konstrukci reality. Je třeba k tomu přistupovat s tímto vědomím a nahlížet na mediální sdělení kriticky.

Další úloha médií je výchovně-vzdělávací (Urban, 2011). „Je to cesta, jak širokou veřejnost seznamovat s novými poznatky a možnostmi, které vývoj přináší“ (Musil, 2003). Službu internetového bankovnictví lze zcela určitě považovat za novou možnost, vzdělávání pomocí médií je tedy žádané. Klienti by se měli z médií dozvědět, v čem je jim tato služba užitečná. Dále by měli nalézt základní návody, jak s touto službou pracovat. Mediální komunikační platforma se tak jeví jako vhodný nosič pro informování a vzdělávání uživatelů.

3.1 Zpravodajství

„Nejčastěji diskutovaným žánrem s vysokou informační hustotou a předpokládaným vlivem na diváky80 je v oblasti žurnalistiky bezpochyby zpravodajství.“ (Urban, 2011) Funkce zpravodajství je zejména informační a definiční, „snaží se aktuální události bez prodlení zachytit, popsat a předat (za pomoci technických prostředků) různě diferenciovanému publiku“ (Osvaldová, 2001, str. 14). Dále má veřejnosti poskytnout dostatečný materiál, aby si mohla vytvořit vlastní názory. Z toho vyplývá, že prvním zdrojem informací o uskutečněných napadeních internetového bankovnictví je právě zpravodajství.

Zpravodajství označuje jednak novinářský proces sběru, výběru a sdělování informací, a také výsledek celého tohoto procesu. V tomto případě se jedná o mediální produkt81, tedy o výstup, produkovaný médii a přijímaný a konzumovaný uživateli (Jirák, Köpplová, 2009). Dále se takto označuje i část médií, kde se objevují aktuální zprávy. Rozlišuje se zpravodajství v tištěných médiích, rozhlasové, televizní a on-line.

3.1.1 On-line zpravodajství

Zpravodajství přenášené on-line kanály bylo umožněno díky technickému pokroku, větší počítačové gramotnosti uživatelů, rozšíření sítě internetového připojení a dalším předpokladům. Na on-line zpravodajství lze pohlížet jako na formální obdobu klasického zpravodajství. Váží se k němu totiž stejná pravidla pro obsah a jeho kvalitu

---

[80] Stať je zaměřena na televizní zpravodajství, nicméně se domnívám, že definici lze vztáhnout i na zpravodajství přenášené po jiných platformách.

[81] Právě mediální produkt je předmětem výzkumné analýzy, což je výzkumná metoda použitá v praktické části práce.

(pomocí žurnalistické kvality a dalších ukazatelů rozlišujeme skutečné zpravodajství od různých fan-zinů a podobných produktů). Na druhé straně on-line prostředí poskytuje specifické možnosti, ať už se jedná o text, podobu nebo šíření zpravodajství. Tyto předpoklady mají vliv na celkovou podobu zpravodajství (Šmíd in Osvaldová, 2001). Díky kombinování těchto prvků se dá očekávat, že internetová zpravodajství budou jedním z nejdůležitějších informačních zdrojů pro uživatele. Tomuto předpokladu odpovídají i další důvody, uvedené v dalších odstavcích.

Internetová periodika můžeme podle propojení s tištěnými médii rozdělit do tří skupin:

1. zrcadla existujících médií, tj. periodika, totožná s tištěnými nebo jinými tituly, jsou pouze převedena do digitální podoby (tento druh periodika se již v podstatě nevyskytuje).
2. On-line suplementy, kdy jsou obsahy existujících médií obohaceny o další, multimediální, rozměry a přizpůsobeny prostředí internetu (Novinky.cz, iDnes.cz, iHNed.cz apod.).
3. Periodika, vytvořena speciálně pro internet - např. Aktuálně.cz (Šmíd in Osvaldová, 2001).

Prostředí internetu má určitá specifika, která lze ve zpravodajství využít pro zvýšení přínosu pro uživatele. Jedním z nich je délka zpravodajského článku (Šmíd in Osvaldová, 2001). Článek není potřeba omezovat maximální délkou příspěvku, neboť internetová periodika nepracují s omezeným rozsahem (na rozdíl např. od novin). Dále lze díky hypertextu vkládat do těchto bloků odkazy na další informace, např. archivní materiály, a vkládat multimediální obsah, tj. zvukové a zvukově-obrazové stopy, a tím jej obohacovat a rozšiřovat v historické i tematické perspektivě. V případě útoků na internetové bankovnictví může být názornější, např. místo slovního popisu škodlivého e-mailu vložit obrázek e-mailu s popisky. V současnosti se začíná přidávat také tzv. infografika, tedy publikování informací v grafické podobě (Internetová žurnalistika, 2013). Pomocí infografiky lze sledovat např. časové řady útoků.

Druhým specifikem internetu je distribuce a přístupnost zpravodajství v prostoru a čase. Geograficky uživatele omezuje pouze existence internetového připojení. Tato možnost internetového zpravodajství zajišťuje širší pokrytí populace zprávou kyberkriminální činnosti. Významnější změnu ale představuje překonávání časových hranic. On-line zpravodajství je možné kdykoli aktualizovat a zprávy o události uvádět v těsném časovém odstupu od uskutečnění události. Aktuálnost informací umožňuje uživatelům internetového bankovnictví v případě útoku rychle reagovat. Navíc se ke zprávám lze kdykoli vrátit a vývoj událostí si připomenout, na rozdíl od televize nebo rozhlasu (Šmíd in Osvaldová, 2001). Jednou vydané informace může uživatel jednodušeji vyhledat, nemusí do knihovny nebo vyhledávat v archivech televizních nebo rozhlasových pořadů. Uživatel se díky snadnější rekapitulaci událostí může ke zprávám vracet a připomínat si základní znaky útoků. Tím se zvyšuje vzdělávací funkce médií.

Výhoda internetu spočívá také v možnosti poskytovat různorodé formáty zpravodajství pro různá čtecí zařízení. Kromě klasického zpravodajství na webové stránce periodika, určené pro počítače, se jedná o rozhraní pro chytré telefony a tablety, dále zasílání zpravodajství ve formě SMS nebo MMS výpisů, využití kanálu

RSS pro softwarové čtečky nebo e-mailové newslettery (Internetová žurnalistika, 2011). Aspekt technologické neomezenosti, stejně jako geografické neomezenosti, napomáhá širšímu dosahu zpráv o útocích na internetové bankovnictví.

3.1.2 Kvalita zpravodajství

Zpravodajství by mělo plnit základní požadavky na kvalitu poskytovaných informací (Hagen in Schulz a kol., 2011). Wall také zdůrazňuje nutnost spolehlivého zdroje o kyberkriminalitě, určeného pro laiky. Média se jeví jako optimální zprostředkovatel těchto informací. V současnosti ale média využívají spíše emocionální vyjádření než racionální konstrukce. Tato okolnost je v rozporu s požadavkem na pochopení podstaty problémů a vytvoření dobré politiky veřejnosti (Wall, 2007).

Základní požadavky kvalitního zpravodajství jsou:

- vyváženost,
- aktuálnost,
- včasnost (nutnost nabídnout co nejrychleji od uskutečnění události relevantní informace uživatelům) a
- objektivita (volně podle Osvaldová in Osvaldová, 2001).

„Zpráva by měla odpovědět na šest základní otázek: kdo, co, kde, kdy, případně u delších zpráv jak a proč[82]“ (Osvaldová in Osvaldová a kol, 2001, str. 24). Tento základní žurnalistický požadavek se v anglickém prostředí nazývá 5 W a 1 H[83], tedy Who? What? Where? When? Why? How?[84] (Porter, 2010) Četnost důležitých informací by měla být největší na začátku zprávy, ke konci se postupně snižovat (tzv. princip obrácené pyramidy). V on-line zpravodajství se ale díky možnosti přidat další rozměry zprávy hovoří o síťové struktuře (Internetová žurnalistika, 2011). Další požadavek na zpravodajský článek je, že by neměla obsahovat více než jednu zprávu. Tento požadavek se u internetových zpravodajství často nedodržuje[85]. Zprávy (tj. poskytované informace) by dále měly být:

- „ověřené (z toho vychází spolehlivost) více důvěryhodnými zdroji,
- přesné,
- jasné,
- úplné a
- srozumitelné“ (Osvaldová in Osvaldová, 2001).

---

[82] Právě tento faktor zkoumám v praktické části práce.

[83] Jiné podoby názvu pravidla jsou např. 6 W.

[84] Překlad autorky.

[85] To můžeme vidět v příloze č. 2, kde je ve zpravodajském článku v jednotlivých kategoriích často zakódována více než jedna proměnná, tzn., že článek obsahuje více než jednu zprávu.

4. Metodologická část

Ve svém výzkumu se budu věnovat mediálním obsahům spojeným s útoky na internetové bankovnictví. Důležitost výzkumu mediálních produktů spočívá v tom, že média slouží jako zprostředkovatel informací veřejnosti. V případě útoků na internetové bankovnictví je potřeba, aby média zprostředkovávala dostatečné množství informací a pokrývala celou šíři způsobů útoku. Informování médií o útocích na internetové bankovnictví slouží jako důležitá složka pozdější prevence těchto útoků a obecně pro zvyšování bezpečnostní gramotnosti. Uživatelé tak budou očekávat zranitelnost bankovních systémů i svoji, a budou tedy moci spíše pochopit odůvodnění bezpečnostních zásad a nutnost jejich dodržování.

Mediální agenda dokáže témata buď vyzdvihnout, a tím jim dodat význam, nebo je upozadit. V takovém případě informace zůstane nepovšimnuta. Jak říká také Etický kodex novináře: „novináři realizují právo občanů na informace a na objektivní obraz skutečnosti (…) a proto nemají deformovat zprávy vyzdvižením nebo naopak zamlčením dat“ (Etický kodex novináře, 1998). V tomto případě je existence mediální agendy nutná za účelem přenosu významných témat do veřejné agendy, tj. témat významných a zajímavých pro veřejnost[86]. Uživatelé si mohou při existenci této agendy rámce tématu kyberkriminality a útoků na internetové bankovnictví zařadit do širší struktury veřejné agendy.

4.1 Cíl výzkumu

Cíl výzkumu je prozkoumat kvalitu obsahové stránky informací o útocích na internetové bankovnictví, poskytovaných on-line zpravodajstvími. Jako měřítka kvality využiji tři měřítka: přítomnost všech odpovědí na šest základních otázek, vyváženost zpravodajství, tj. informace o útocích na všechny prvky a přítomnost pozdější prevence, jakožto přidané hodnoty informace pro uživatele. Ve výzkumu byly tedy vytyčeny tři hlavní výzkumné cíle. Prvním z nich je zjistit, jestli lze v obsahu zpráv nalézt odpovědi na šest základních otázek, tzn. kdo, co, kde, kdy, a u delších zpráv jak a proč[87] se stalo. Jedině kvalitní zpráva může mít pro uživatele přínos z důvodů popsaných výše. Druhý cíl výzkumu spočívá ve snaze změřit v informacích poskytovaných médii četnost jednotlivých typů útoků. Budu se tedy soustředit na vyváženost zpravodajství. V rámci posledního výzkumného cíle dojde ke zkoumání, zda se uživatel může z útoku do budoucna poučit, tedy jestli zprávy poskytují popis budoucí prevence. V pozitivním případě budou tato opatření blíže upřesněna.

Na mediálním obrazu mě nezajímá formální stránka zpráv, tedy např. zdroje zpráv nebo emoční a citová neutrálnost zpráv. Nezabývám se ani strukturou zpráv o útocích, doprovodným fotografickým materiálem, informacemi z diskusí apod. Zaměřuji se čistě na obsahovou stránku zpráv.

---

[86] Více o agenda-setting na straně 40.

[87] Více o šesti kvalitativních otázkách na straně 43.

4.2 Metodologie

Jako výzkumnou metodu jsem zvolila obsahovou analýzu mediálních produktů, konkrétně obsahů internetových zpravodajství. Obsahová analýza je "kvantitativní výzkumnou metodou pro systematický a intersubjektivně ověřitelný popis komunikačních obsahů, vycházející z vědecky podloženého kladení otázek." (Scherer in Schulz, 2011). Její výsledky jsou "málo detailní, zobecňující data, která vypovídají (…) o poměru kvant výskytu sledovaných jevů ve vybraném souboru mediálních produktů". (Jirák, Köpplová, 2009, str. 283) Jako kvantitativní metodu ji shledávám vhodnou pro zkoumání velkého množství textů. Výsledky se dají statisticky zpracovat formou grafů a tabulek.

Tato metoda mi umožní prozkoumat texty, které popisují provedené útoky na internetové bankovnictví. Takto budu moci prověřit, jestli jsou informace o útocích kvalitní, tzn., jestli odpovídají na šest základních otázek kvality zpravodajství. Navíc by mělo dojít k odhalení toho, jaké útoky se nejčastěji objevují, a zda se popis útoků spojuje s popisem prevence proti těmto útokům v budoucnosti.

4.2.1 Výběrový soubor

Jako soubor pro výběr výzkumného vzorku jsem zvolila zprávy z internetových zpravodajství. On-line zpravodajství bylo vybráno kvůli předpokladu, že kromě odborně zaměřených médií v klasické, tj. tištěné[88] nebo elektronické podobě nebo kromě útoků s velkým dopadem se zprávy o útocích do médií nedostanou. To souvisí s omezeností těchto médií rozsahem vysílání nebo rozsahem a množstvím článků oproti on-line médiím[89] (Šmíd in Osvaldová, 2001). Další důvod pro výběr internetových zpravodajství byl, že uživatelům internetového bankovnictví slouží jako hlavní zdroj informací znovu internet.

Výběrový soubor tedy tvoří internetová média, konkrétně zpravodajství stránek Novinky.cz, iDnes.cz a Aktualne.centrum.cz, které jsou podle výzkumu NetMonitor nejnavštěvovanější, jak ukazuje tabulka 2. Kritérium návštěvnosti bylo vybráno za účelem největšího dopadu mediálních sdělení, publikovaných v těchto médiích. Požadavek na kvalitní informace je tedy v těchto sděleních zásadní.

Vzorek jsem doplnila stránkami iHNed.cz, jakožto odborného zpravodajství zaměřeného na ekonomiku a finance. Tento zdroj může výsledek výzkumu zkreslit, protože se dá očekávat, že bude obsahovat více zpráv, které budou problematiku útoků na internetové bankovnictví pokrývat v širších souvislostech (právě díky zaměření média). Tomuto zkreslení se pokusím vyhnout tím, že po vyhodnocení sběru dat ze všech zpravodajství budu nejprve hodnotit jednotlivá média. Komparace poté proběhne s ohledem na specifika jednotlivých médií.

---

[88] Např. Hospodářské noviny, které se zaměřují mj. na informace ze světa ekonomiky a financí, nebo odborné periodikum Bankovnictví. Jako média v elektronické podobě je zde míněna televize nebo rozhlas (Osvaldová, 2001).

[89] Více o internetovém zpravodajství a jeho specifikách v kapitole 3.1.1.

Tabulka 2 Počet návštěvníků internetových zpravodajství, zdroj: Měsíční zpráva: Březen 2013, 2013

Pořadí	Webové stránky	Počet všech návštěvníků (reálných uživatelů) za březen 2013
1.	novinky.cz - rubrika Zpravodajstvi	3 317 573
2.	idnes.cz - Zpravy	1 450 731
3.	centrum.cz - Aktualne.cz - Zprávy Aktualne.cz	1 164 741
8.	ihned.cz - Zpravodajstvi iHNed	451 070

Novinky.cz jsou „on-line magazín deníku Právo a Seznam.cz“ (Novinky.cz, 2013). Poskytují komplexní zpravodajství i magazínové rubriky. Rozcestník Seznam.cz navštěvuje z českých webů nejvíce uživatelů, např. v březnu 2013 jej navštívilo přes 5 milionů reálných uživatelů (Měsíční zpráva: Březen 2013, 2013). Díky zobrazení zpravodajství Novinky.cz na hlavní stránce rozcestníku, a také díky faktu, že Novinky.cz jsou nejnavštěvovanějším zpravodajstvím, jak vidíme v tabulce 2, se tedy dá předpokládat dopad zpravodajství na největší procento uživatelů.

Aktuálně.cz patří mezi stránky společnosti Centrum Holdings. Na stránkách média se uvádí, že je “první čistě on-line deník v České republice” (Tiráž, 1999). Jako takový funguje nezávisle na tištěných nebo elektronických médiích. Kromě zpravodajství a magazínových rubrik lze na stránkách nalézt např. blogy, kam pravidelně přispívají známé české osobnosti ze všech oblastí.

Zpravodajský server iDnes.cz se řadí mezi členy vydavatelské skupiny Mafra. iDnes.cz je internetová varianta deníku MF Dnes a poskytuje „všeobecné zpravodajství s důrazem na klíčové události u nás i ve světě“ (Internetová žurnalistika, 2013). Kromě zpravodajství se na portálu vyskytují další, oborově zaměřené servery nebo komunitní a specializované stránky, např. jízdní řády, úložiště pro fotografie apod.

Zpravodajský server iHNed.cz má přímou vazbou na Hospodářské noviny. Vydavatelem je nakladatelství Economia. „Nabízí objektivní a nezávislé zpravodajství a komentáře z oblasti ekonomiky, businessu a financí.“ (Divize Nová média, 2013) I na těchto stránkách můžeme nalézt další, oborově zaměřené webové stránky.

Zkoumané období bylo stanoveno na interval od 1. 1. 2008 do 30. 4. 2013. Začátek období jsem zvolila v souvislosti s počátkem většího rozvoje internetového bankovnictví v ČR, kdy došlo k poskytování lepších webových aplikací bankami a jejich většímu uživatelskému využití[90]. Studie společnosti Softec zmiňuje jako milník internetového bankovnictví rok 2007 (konkrétně listopad), ve kterém do České republiky pronikla banka mBank. Poté se na trhu objevily další nízkonákladové banky, sázející na jednodušší ovládání, levnější služby, a také na poskytování služeb elektronickými kanály (Budoucnost distribučních kanálů v České republice a na Slovensku: Trendy a nové vize, 2012). Počátek zkoumaného období byl ale stanoven na 1. 1. 2008 za účelem srovnání na začátek roku.

[90] Počty uživatelů internetového bankovnictví jsou zobrazeny na obrázku č. 1 na straně 11.

Relevantní příspěvky jsou takové, které lze vyhledat pomocí fráze "internetové bankovnictví". Tato metoda vyhledávání zpráv mi umožňuje vyhledávat články efektivněji a dále v čase, než kdybych k vyhledání použila archiv zpráv[91].

Články budu poté filtrovat podle toho, jestli se jedná o:

- záměrný útok. Toto kritérium bylo zvoleno za účelem odfiltrování údajů o výpadcích proudu a dalších nezamýšlených událostí.
- Kriminální čin nebo kriminální záměr, tzn., jestli byli uživatelé internetového bankovnictví činem poškozeni (kriminální čin) nebo ne (kriminální záměr). Důležitý je ale cíl útoku, tedy poškození uživatelů. Poškození mohlo proběhnout např. ve formě zamezení přístupu, finanční ztráty, ukradení přístupových údajů k internetovému bankovnictví apod.
- Uskutečněný útok. Tím se rozumí, jestli útok již proběhl nebo právě probíhá.
- Typu poškozené webové služby, kterou je aplikace internetového bankovnictví.

Při filtrování výzkumného vzorku není rozhodující, zda se v rámci zpravodajského článku jedná primárně o zprávu o útoku na internetové bankovnictví nebo jestli se útoku týká pouze část článku. V případě, že útok popisuje část zpravodajského článku, dojde k aplikaci výzkumné metody jen na tuto část.

Z výzkumného vzorku budou tedy vyloučeny reklamy na internetové bankovnictví, zprávy o útocích na jiné bankovní služby, jako např. platební karty, nebo zprávy o potencionálních útocích atd. Tímto způsobem dosáhnu relevantního vymezení výzkumného vzorku.

4.2.2 Kódovací jednotka

Kódovací jednotkou rozumím článek nacházející se v internetovém zpravodajství. Zpravodajský článek začíná titulkem a končí uvedením autora nebo zdrojů. Součástí kódovací jednotky není diskuse uživatelů. Ve výzkumu budu analyzovat pouze text bez obrazových a jiných příloh.

4.2.3 Stanovení výzkumných otázek

Hlavní výzkumná otázka zní: Zprostředkovávají internetová zpravodajství uživatelům kvalitní informace o útocích na internetové bankovnictví?

Výzkumná otázka č. 1: Odpovídají informace o útocích na internetové bankovnictví na 6 základních otázek kvalitního zpravodajství?
Výzkumná otázka č. 2: Jaký je nejčastější typ útoku na internetové bankovnictví, uváděný v médiích?
Výzkumná otázka č. 3: Je popisována následná prevence proti budoucím útokům?
Výzkumná otázka č. 4: Jaká preventivní opatření jsou popisována ve zprávě?

[91] Použít elektronický archiv jsem se rozhodla také proto, že při vyhledávání zpráv přímo ve zpravodajství bylo nutné procházet více rubrik (Zprávy, Domácí, Krimi). Tím by došlo ke zkreslení výsledku.

Kódování výzkumné otázky č. 1 vychází z šesti kvalitativních otázek. Pro kategorie je možné zvolit více proměnných podle toho, kolik zpravodajský článek obsahuje zpráv. Kódovací kategorie a proměnné jsou uvedeny v příloze č. 1.

Kvalitní zpravodajství obsahuje odpověď na šest základních otázek:
KDO? Odpovědí na tuto otázku bude napadená bankovní instituce. V této kategorii jsem nejprve vydělila banky s největším počtem klientů, tj. Českou spořitelnu, Komerční banku a ČSOB, jakožto nejvýznamnější instituce. Dále byla vybrána skupina nízkonákladových bank (ZUNO, Air Bank, Equa bank, mBank a Fio banka), které mají nízké nároky na zabezpečení, jak je vidět v tabulce použitých autentizačních metod na straně 16. Na závěr jsem ještě ustanovila kategorii zahraničních bank.
CO? Zde se zajímám o prvek internet bankingu, který se stal terčem útoku. Tato kategorie vychází z popisu procesu internetového bankovnictví, blíže vysvětleného na obrázku č. 2.
KDE? Nyní vymezuji, zda se útok stal v České republice nebo v zahraničí.
KDY? Při stanovení proměnných pro tuto otázku popisuji, jestli byla ve zpravodajském článku stanovena doba provedení útoku. Jako dostatečné shledávám formulace "v minulých dnech", "nedávno", "v poslední době" apod.
JAK? Zde se dostávám ke stanovení typu útoku, vycházejícího z kategorií v druhé části práce.
PROČ? Touto otázkou zkoumám účel útoku – jako hlavní důvody útočníků byly identifikovány finanční a nefinanční záměry. V druhém bodě jde zejména o poškození image banky nebo zamezení uživatelům v přístupu do aplikace. Dopad na uživatele bude upřesněn podle počtu poškozených[92] a podle množství ukradených financí[93].

Kódování druhé výzkumné otázky má základ v kategorie „Typ útoku". Jde tedy o odpověď na otázku „Jak?" z předešlého výčtu.

Ve třetí otázce bude uvedena pouze jedna kategorie se dvěma proměnnými, a to:

1. Pozdější prevence byla zobrazena.
2. Pozdější prevence nebyla zobrazena.

Poslední výzkumná otázka upřesňuje předchozí. V rámci této otázky budou popsány nejčastější znaky následné prevence po útoku na internetové bankovnictví, pomocí kterých by mělo dojít k zamezení dalších podobných útoků.

Identifikační proměnné jsem zvolila následujícím způsobem:

1. Internetové zpravodajství
2. Název článku
3. Datum
4. Čas
5. URL

[92] Při sestavování souboru proměnných vycházím z klientských základen bank, poskytujících internetové bankovnictví - viz proměnnou „Instituce" v příloze č. 1. V této proměnné můžeme vidět, že se vydělily pouze tři banky, které mají klientskou základnu vyšší než jeden milion uživatelů, proto je pro 1 mil. a více stanovena pouze jedna proměnná.
[93] Toto číslo, poskytnuté bankou, musí být konečné. Banka tedy musí mít informace, kolik klientů bylo poškozeno. Formulace „zřejmě", „zatím" apod. budou kódovány jako „Neuvedeno".

5. Analytická část

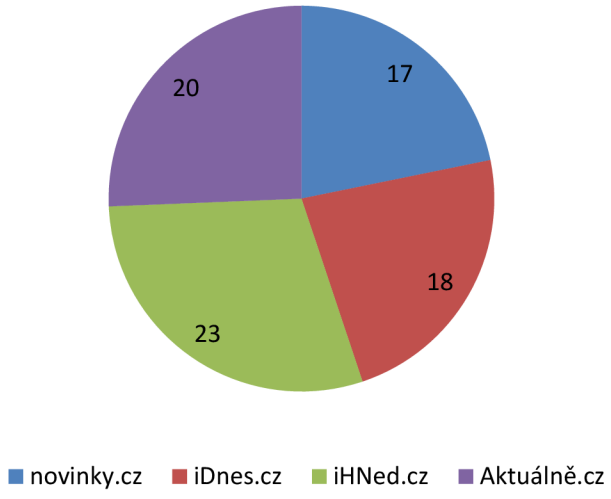
V této části budu nejprve analyzovat množství zpráv v médiích a poté se pokusím určit hlavní události, zobrazené v médiích. Následně vyhodnotím výsledky zjištěné obsahovou analýzou, a vyvodím z nich odpovědi na výzkumné otázky. U otázky č. 1 uvedu celkový počet uvedených proměnných z jednotlivých kategorií, rozdělený podle zkoumaného zpravodajství. V rámci této otázky, tzn., jestli informace v médiích odpovídají na šest otázek kvalitního zpravodajství[94], budu ještě interpretovat dílčí výsledky upřesňující dopad útoku[95].

Data, získána obsahovou analýzou, jsou prezentována ve formě tabulek a grafů. K nim jsem potom vložila popis, ve kterém se snažím stávající situaci blíže popsat a určit její příčiny.

5.1 Počet zpráv

V internetových zpravodajstvích bylo ve sledovaném období objeveno 78 článků, zabývajících se tematikou útoku na internetové bankovnictví. Seznam článků uvádím v příloze č. 1, kde je rovněž uvedeno kódování podle kódovacího schématu.

Jedním z předpokladů, ze kterých jsem při analýze vycházela, byl, že z odborněji zaměřeného zpravodajství (iHNed.cz) získám větší množství článků než z ostatních[96]. Jak vidíme na obrázku č. 5, tento předpoklad se nenaplnil. Hlavní důvod může být ten, že iHNed.cz se věnovalo napadením on-line bankovnictví pouze výjimečně. Kromě dvou vln útoků: na Českou spořitelnu v roce 2008 (13 článků) a DDoS útokům na českou republiku v roce 2013 (5 článků) se zde objevil pouze 1 článek o útoku na jihokorejské banky a 4 články o útocích pomocí malware.



Obrázek 2 Rozložení relevantních zpráv podle internetových zpravodajství

[94] Více o těchto otázkách na straně 43.

[95] Jedná se o kategorie „Úspěšnost útoku podle počtu poškozených a podle množství zcizených financí“, uvedené v metodologické části na straně 48.

[96] Viz stranu 45.

Tabulka 3 Časové rozložení zpráv

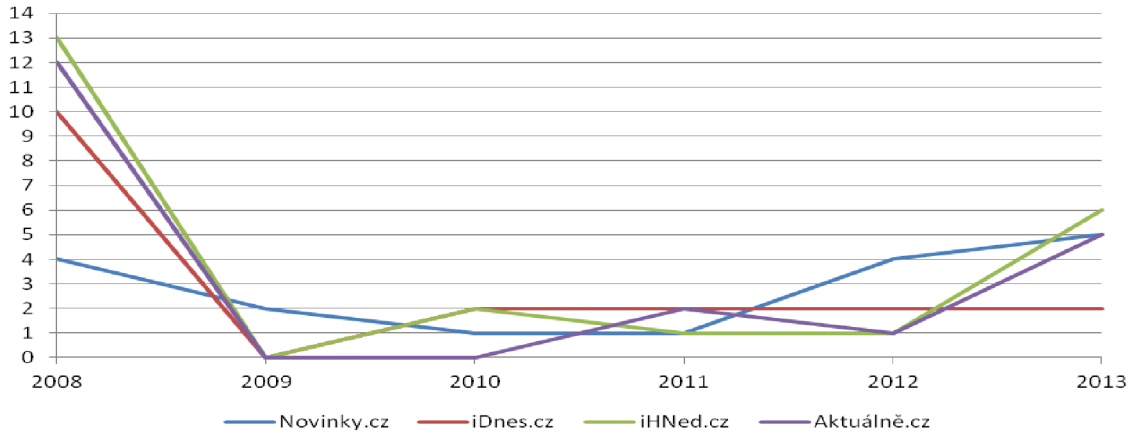
	2008	2009	2010	2011	2012	2013
Novinky.cz	4	2	1	1	4	5
iDnes.cz	10	0	2	2	2	2
iHNed.cz	13	0	2	1	1	6
Aktuálně.cz	12	0	0	2	1	5
počet zpráv celkem	**39**	**2**	**5**	**6**	**8**	**18**
počet zpráv			**78**			

Tabulka 3 zobrazuje časové rozložení zpráv. Z této tabulky vyplývá, že zpráv o útocích na internetové bankovnictví se objevilo výrazně více v letech 2008, kdy probíhal vytrvalý phishingový útok na Českou spořitelnu, a 2013, ve kterém proběhl rozsáhlý útok DDoS na síťovou infrastrukturu České republiky. Množství zpráv bylo poté vyrovnané, až na rok 2009. V tomto roce se žádný útok na on-line bankovnictví neobjevil, pouze Novinky.cz poskytly shrnutí zahraničního výzkumu a připomněly phishingové útoky z předchozího roku.

Hlavní události, zobrazené v médiích, je tedy možné identifikovat následujícím způsobem:

1. phishingový útok na Českou spořitelnu v roce 2008 (všechna zpravodajství),
2. hackerský útok na bankovní účet francouzského prezidenta Sarkozyho na konci roku 2008 (iDnes.cz),
3. odhalení 2 botnetů[97], jednoho ve Velké Británii a druhého v Americe, v roce 2010 (iDnes.cz a iHNed.cz),
4. útok na Českou spořitelnu pomocí viru, vytvářejícího falešné převody, v roce 2012 (Novinky.cz a iDnes.cz),
5. DDoS útoky na síťovou infrastrukturu ČR v březnu 2013 (všechna zpravodajství) a
6. hackerský útok na Jižní Koreu v roce 2013 (iDnes.cz, iHNed.cz a Aktuálně.cz).

Tyto vlny jsou zobrazeny na obrázku č. 6.



Obrázek 3 Časová řada útoků na on-line bankovnictví

[97] Botnety charakterizuji na straně *30*.

5.2. Výzkumná otázka č. 1

Tato otázka odpovídá na jeden ze základních kvalitativních požadavků na zpravodajské články, tj. že by se měly ve zpravodajských článcích objevit odpovědi na 6 otázek - co, kdo, kde, kdy a u delších zpráv jak a proč. V případě, že se ve zpravodajském článku odpověď neobjevila, byla proměnná v příslušné kategorii zakódována jako „0. Neuvedeno".

Získaná data jsem tedy nejprve zakódovala pomocí kódovacího schématu, uvedeného v příloze 2. Poté byl určen celkový počet uvedených proměnných[98]. Tento počet vytvořil sto procent pro danou kategorii. Následně jsem určila, kolik procent v dané kategorii tvoří proměnná „Neuvedeno". Výslednou odpověď na tuto otázku jsem potom získala tím, že jsem sečetla procenta pro příslušné kategorie a vydělila jsem je počtem kategorií.

5.2.1. Analýza zpravodajství Novinky.cz

V tomto zpravodajství bylo identifikováno 17 článků, zabývajících se útoky na internetové bankovnictví[99]. Novinky.cz tedy poskytly svým uživatelům nejmenší počet zpráv.

Tabulka 4 Počet proměnných v jednotlivých kategoriích ve zpravodajství Novinky.cz

Kategorie	0	1	2	3	4	5	6	7	8
1. Banky	5	9	1	1	0	3	4		
2. Napadený prvek	1	12	0	0	0	4	0		
3. Lokace cíle	x	13	5						
4. Časové vymezení	2	15	x						
5. Způsob provedení	0	0	7	6	0	0	0	0	5
6. Účel útoku	1	12	4	0					

Z tabulky č. 4[100] a pohledu na počet odpovědí zakódovaných jako „Neuvedeno" je zřejmé, že toto zpravodajství nebude patřit mezi nejkvalitnější[101]. Novinky.cz se soustředí na rekapitulaci událostí souvisejících s hlavní zprávou ve svých článcích. Z toho vyplývá, že při opakování nebyly uváděny všechny informace, ale jenom jedna nebo dvě věty s odkazem na hlavní zprávu. Např. vysoký počet neuvedených bank v proměnné 1 je způsoben opakovaným popisováním DDoS útoků z března 2013. V těchto zprávách totiž útoky figurovaly pouze v seznamu všech cílů útočníků a jako takové nebyly blíže konkretizovány. Na hlavní zprávu o útocích na internetové bankovnictví potom odkazoval titulek této zprávy.

[98] Na výsledku se tak promítl i počet článků, které jsem ze zpravodajství vytěžila.

[99] Více viz přílohu 2.

[100] Začerněná pole v tabulkách odpovídají neexistujícím proměnným v dané kategorii. Např. v kategorii „Lokace cíle" jsou možné proměnné pouze „1. Česká republika" nebo „2. Zahraničí". Více viz přílohu č. 1.

[101] Tomu napovídají i terminologické chyby, které se ve zpravodajství občas objeví. Příkladem může být pojmenování viru SpyEye, které se ve článku „Nebezpečný počítačový virus vykrádá lidem bankovní účty" změnilo na „SpyEve".

Tabulka 5 Analýza zpravodajství Novinky.cz podle odpovědí na 6 otázek kvalitního zpravodajství

Kategorie	Celkem proměnných	Z toho nula	Z toho nula (v procentech)	Výsledek
1. Banky	23	5	22%	8% nekvalitní
2. Napadený prvek	17	1	6%	
3. Lokace cíle	18	0	0%	
4. Časové vymezení	17	2	12%	
5. Způsob provedení	18	0	0%	
6. Účel útoku	17	1	6%	

Tabulka č. 5 ukazuje analýzu kvality zpravodajství Novinky.cz z hlediska kvantifikace záporných odpovědí. Z této tabulky dále vyplývá, že v informacích o útocích poskytovaných Novinkami.cz se v 8 procentech neobjevily odpovědi na otázky kvalitního zpravodajství. Tento zdroj bych tedy označila jako nejméně kvalitní ze zkoumaných.

5.2.2. Analýza zpravodajství iDnes.cz

Ve zpravodajství iDnes.cz jsem vyselektovala 18 článků, popisujících útoky na on-line bankovnictví. Tyto články byly již více různorodé než z předchozího zdroje. Kromě útoků, uvedených na straně 50, dále popisovaly kyberkriminální příklady v České republice i ve světě. Tento faktor má za následek i objevení proměnné „Neuvedeno“ v kódovací kategorii „Banky“ v tabulce 6. V těchto dvou případech popisují objevení botnetu v Americe a dopadení slovinského hackera, zodpovědného za vytvoření malware kradoucího přihlašovací údaje k internetovému bankovnictví. Vysoký počet neuvedených časových údajů je způsoben nedostatkem informací (jako u výše uvedeného případu slovinského hackera) nebo pravděpodobně předpokladem žurnalistů, že v případě útoků na české banky si uživatel uvědomí, že jde o aktuální informace.

Tabulka 6 Počet proměnných v jednotlivých kategoriích ve zpravodajství iDnes.cz

Kategorie	0	1	2	3	4	5	6	7	8
1. Banky	2	10	1	1	1	2	4		
2. Napadený prvek	0	14	0	0	0	4	0		
3. Lokace cíle	x	12	6						
4. Časové vymezení	7	11	x						
5. Způsob provedení	0	0	10	5	0	0	0	2	1
6. Účel útoku	0	16	1	1					

Tabulka 7 Analýza zpravodajství iDnes.cz podle odpovědí na 6 otázek kvalitního zpravodajství

Kategorie	Celkem proměnných	Z toho nula	Z toho nula (v procentech)	Výsledek
1. Banky	21	2	10%	7% nekvalitní
2. Napadený prvek	18	0	0%	
3. Lokace cíle	18	0	0%	
4. Časové vymezení	18	7	40%	
5. Způsob provedení	18	0	0%	
6. Účel útoku	18	0	0%	

Vysoký počet neuvedených odpovědí na otázku „Kdy?“, který jsem zmínila u popisu předchozí tabulky, je také příčinou nízkého procenta hodnocení kvality zpravodajství podle šesti otázek. Tento fakt se zobrazil v tabulce 7.

5.2.3. Analýza zpravodajství iHNed.cz

Jak bylo již naznačeno na straně 49, ve zpravodajství iHNed.cz se objevilo pouze 23 zpráv o útocích na on-line bankovnictví. To byl nižší počet, než jsem při stanovení výzkumného vzorku očekávala.

Tabulka 8 Počet proměnných v jednotlivých kategoriích ve zpravodajství iHNed.cz

Kategorie	0	1	2	3	4	5	6	7	8
1. Banky	4	14	1	2	0	5	3		
2. Napadený prvek	0	17	0	0	0	6	0		
3. Lokace cíle	X	19	4						
4. Časové vymezení	6	17	X						
5. Způsob provedení	0	1	13	4	0	0	0	1	5
6. Účel útoku	0	17	1	5					

Počet proměnných „Neuvedeno“ má v případě tohoto zpravodajství stejnou příčinu jako u předchozích – nedostatek informací a předpoklad autorů o aktuálnosti u vymezení doby provedení útoků. U kategorie „Banky“ je to opět rekapitulace cílů napadení u DDoS vlny v roce 2013.

Tabulka 9 Analýza zpravodajství iHNed.cz podle odpovědí na 6 otázek kvalitního zpravodajství

Kategorie	Celkem proměnných	Z toho nula	Z toho nula (v procentech)	Výsledek
1. Banky	29	4	14%	6% nekvalitní
2. Napadený prvek	23	0	0%	
3. Lokace cíle	23	0	0%	
4. Časové vymezení	23	6	21%	
5. Způsob provedení	24	0	0%	
6. Účel útoku	23	0	0%	

Navzdory vyššímu počtu neuvedených odpovědí na některou z šesti otázek kvalitního zpravodajství je díky rovněž vyššímu počtu uvedených článků zpravodajství

iHNed.cz druhé nejkvalitnější z výzkumného vzorku. Poskytované informace neodpovídají na tyto otázky pouze z 6 procent, jak je vidět v tabulce 9.

5.2.4. Analýza zpravodajství Aktuálně.cz

Aktuálně.cz přispělo do výzkumného vzorku 20 články. V tabulce č. 10 můžeme vidět nízký počet proměnných „Neuvedeno“. Tato proměnná se objevila hlavně u jednoho souhrnného článku, který popisoval hackerské útoky za posledních pět let.

Tabulka 10 Počet proměnných v jednotlivých kategoriích ve zpravodajství Aktuálně.cz

Kategorie	0	1	2	3	4	5	6	7	8
1. Banky	2	14	3	2	2	5	3		
2. Napadený prvek	1	15	0	0	0	4	0		
3. Lokace cíle		17	4						
4.Časové vymezení	3	17							
5.Způsob provedení	0	0	12	3	0	0	0	2	3
6. Účel útoku	0	15	3	2					

V tabulce č. 11 se zobrazil nízký počet neuvedených odpovědí na každou ze šesti otázek kvalitního zpravodajství. Z tohoto pohledu poskytuje Aktuálně.cz nejkvalitnější informace o útocích na internetové bankovnictví z výzkumného vzorku.

Tabulka 11 Analýza zpravodajství Aktuálně.cz podle odpovědí na 6 otázek kvalitního zpravodajství

Kategorie	Celkem proměnných	Z toho nula	Z toho nula (v procentech)	Výsledek
1. Banky	31	2	6%	4 % nekvalitní
2. Napadený prvek	20	1	5%	
3. Lokace cíle	21	0	0%	
4. Časové vymezení	20	3	15%	
5. Způsob provedení	20	0	0%	
6. Účel útoku	20	0	0%	

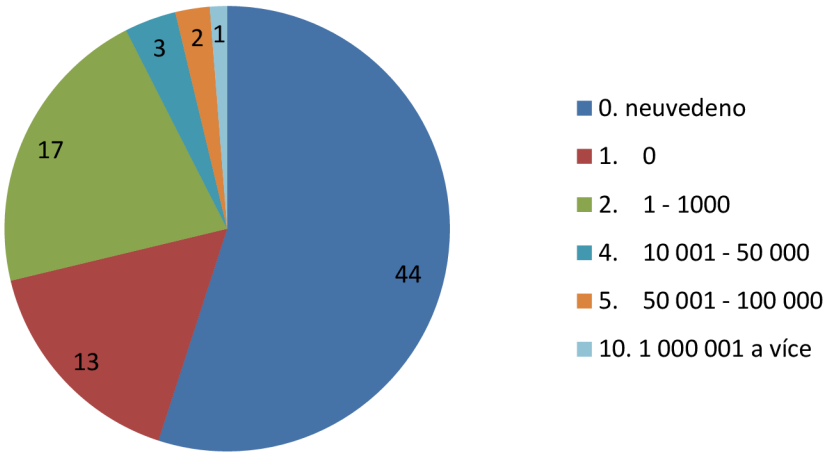
5.2.5. Odpověď na výzkumnou otázku č. 1

Každá zpráva by měla odpovědět na šest základních otázek: Kdo? Co? Kde? Kdy? Jak? Proč? Na tuto základní žurnalistickou poučku jsem se zaměřila v první výzkumné otázce. Z výzkumu vyplynulo, že internetová zpravodajství poskytují poměrně kvalitní informace. Jako zdroj informací bych nicméně doporučila Aktuálně.cz, které ve svých článcích zodpovědělo na nejvíce otázek kvalitního zpravodajství (neodpovědělo pouze na 4 % otázek). Naopak bych rozhodně nenavrhla hledat tyto informace ve zpravodajství zprostředkovávaném Novinkami.cz (8 %). Kromě nízkého procenta odpovědí na mě při kódování zpráv toto zpravodajství nepůsobilo dojmem přehlednosti textů, a z toho vyplývající sdělnosti a rychlé zpracovatelnosti textu (Šebesta in Osvaldová, 2001). Z toho důvodu se tyto zprávy kódovaly špatně.

Překvapil mě výsledek zpravodajství iHNed.cz, od kterého jsem očekávala vyšší žurnalistickou kvalitu (z 5 % se neobjevily odpovědi na základní otázky). Také jsem očekávala vyšší návratnost článků o ekonomické kyberkriminalitě z důvodu zaměření média na finance a ekonomiku. Přesto byla návratnost vyšší, než u ostatních médií, a díky tomu došlo ke snížení celkového procenta odpovědí na šest základních žurnalistických otázek.

5.2.6. Dílčí otázky

Nyní popíšu další informace, získané obsahovou analýzou internetových zpravodajství. Jedná se zejména o výsledky kódovacích kategorií upřesňujících dopad na uživatele[102]. První z nich, tj. počet poškozených uživatelů, lze vidět na obrázku č. 7[103]. Celkem se v této kategorii objevilo 80 proměnných. Z grafu vyplývá, že média většinou informace o množství poškozených uživatelů neupřesňují. Přesto se jednou objevila kategorie 1 mil. a více, kdy se jednalo o případ poškození uživatelů, rozmístěných po celém světě, pomocí malware Mariposa, odesílajícím přihlašovací údaje k on-line bankovnictví. Tento malware byl použit při vytvoření většího botnetu. I v dalších kategoriích šlo o největší poškození uživatelů zahraničních bank botnety. Naopak ve vlně útoků na Českou spořitelnu v roce 2008 se ve zprávách objevily nejprve informace, že nikdo nepřišel k újmě. Posléze ale byly zjištěny ojedinělé případy postižených uživatelů.



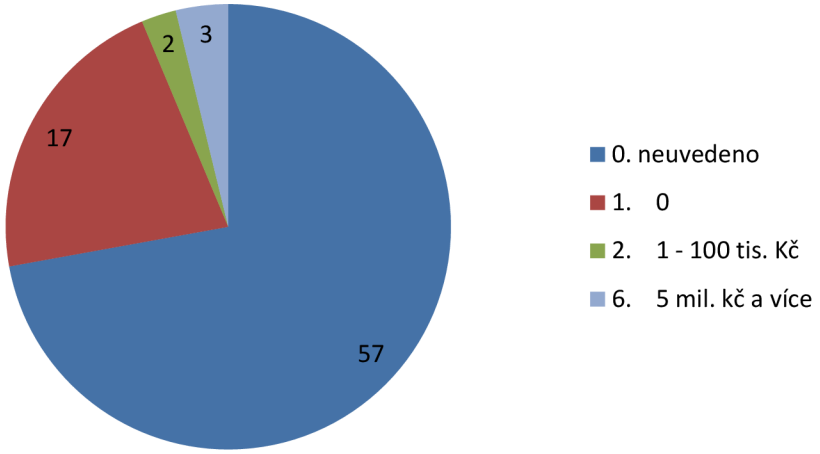
Obrázek 4 Množství informací o poškozených uživatelích podle počtu proměnných

V druhé upřesňující kategorii, tedy úspěšnost útoku podle množství ukradených peněz, byla média ještě méně konkrétní, jak je vidět na obrázku č. 8. Stejně jako v předchozí kategorii, i zde hlavně uváděla informace o phishingových útocích na ČS, při kterých banky neměly zprávy ukradení žádných financí. Na druhé straně

[102] Konkrétní výsledky viz přílohu č. 3.

[103] V grafu jsem uvedla pouze proměnné, které se v obsahové analýze objevily. Z toho důvodu chybí proměnné 3 a 6 – 9.

zpravodajství přinesla zprávy o třech zahraničních útocích s velkým dopadem – ve dvou případech se jednalo o malware Zeus[104] a v jednom o malware Eurograbber.



Obrázek 5 Množství informací o zcizených financích podle počtu proměnných

5.3. Výzkumná otázka č. 2

V této otázce jsem se zajímala o nejvíce zobrazovaný typ útoku. Vycházela jsem z předpokladu, že média zobrazují nejčastěji útok na uživatele[105]. Odborníci se totiž shodují, že banky nebudou poskytovat informace o útocích, aby nedošlo k poškození jejich mediálního obrazu. To by totiž vedlo ke snížení klientské základny, a tím pádem ke snížení zisků. Banky by dále musely investovat více do zabezpečení svého systému, tomu se tyto instituce radši vyhnou.

Tabulka 12 Četnost zobrazených typů útoku v jednotlivých zpravodajstvích

	Novinky.cz	iDnes.cz	iHNed.cz	Aktuálně.cz
2. phishing + pharming	7	10	13	12
3. malware	6	5	4	3
7. DDoS	5	1	5	3
1. Hacking	0	2	2	2
0. Neuvedeno	0	0	0	0
4. XSS, XSRF a clickjacking	0	0	0	0
5. Útok ze středu	0	0	0	0
6. Smíšená hrozba	0	0	0	0

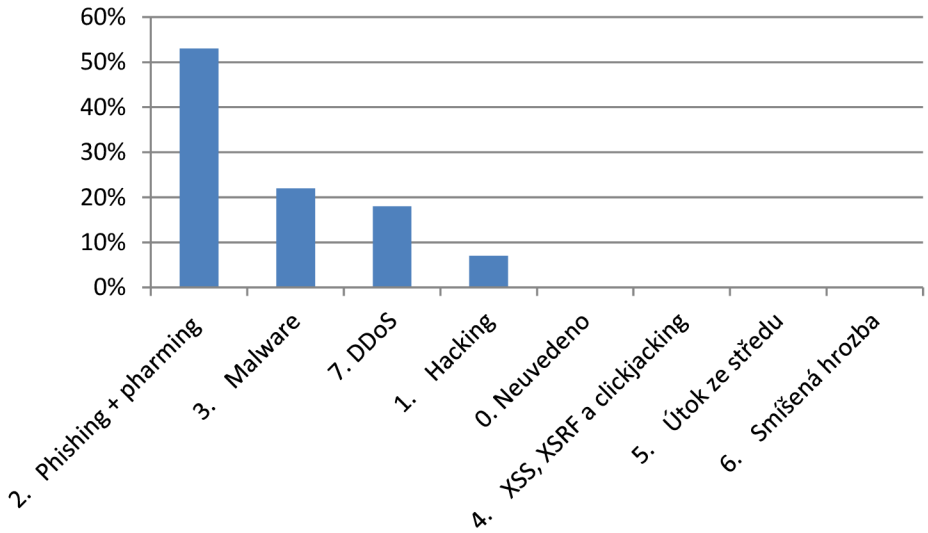
V tabulce č. 12 jsou zaznamenány útoky na internetové bankovnictví, které byly zprostředkovány jednotlivými zpravodajstvími. Tato tabulka sloužila jako východisko pro procentuální výpočet četnosti útoků.

[104] V jednom případě se Zeus nazývá celý botnet. I to je příklad terminologické nesprávnosti zpravodajství Novinky.cz, o které jsem psala v poznámce 94. Více o trojském koni Zeus na straně 31.

[105] Tyto útoky jsem v teoretické části své práce definovala jako: útok na hesla, phishing, pharming, a útok pomocí malware.

5.3.1. Odpověď na výzkumnou otázku č. 2

Z obrázku č. 9 vyplývá, že nejčastěji zobrazovaným typem útoku jsou opravdu útoky na uživatele (celkem 75 %). Přesto se poměrně často zobrazil i útok na bankovní server, ať už ve formě hackingu nebo DDoS. V roce 2013 se totiž uskutečnil rozsáhlý útok DDoS na síťovou infrastrukturu České republiky a média tento fakt hojně zobrazovala. Příčinou vysokého procenta zobrazení hackingových útoků je vykradení účtu francouzského prezidenta Nicolase Sarkozyho a kybernetický útok na Jižní Koreu. Zpravodajství iHNed.cz také jako jediné přineslo informace o útoku pomocí prolomení hesla administrátora na bankovní server Unicredit bank[106]. Tento útok způsobil výpadek internetového bankovnictví a jiných bankovních služeb.



Obrázek 6 Četnost typů útoku v procentech

Z obrázku dále můžeme usoudit, že se ostatní útoky neodehrávají nebo banky opravdu neposkytují informace o útocích na webové aplikace nebo na bankovní servery. Zpravodajství poté nemohou tyto informace převzít a zprostředkovat je veřejnosti. Vzhledem k tomu, že se tyto útoky v mediální agendě nezobrazí, nemohou být ani přejaty do veřejné agendy. To mě vede k otázce, jestli tyto hrozby uživatelé vnímají. Další otázkou zůstává, zda kybernetické útoky na bankovní servery nemohou být příčinou náhlých výpadků bankovních systémů, o kterých se můžeme ve zpravodajstvích dočíst. Tato domněnka je ale pouhou spekulací.

5.4. Výzkumná otázka č. 3

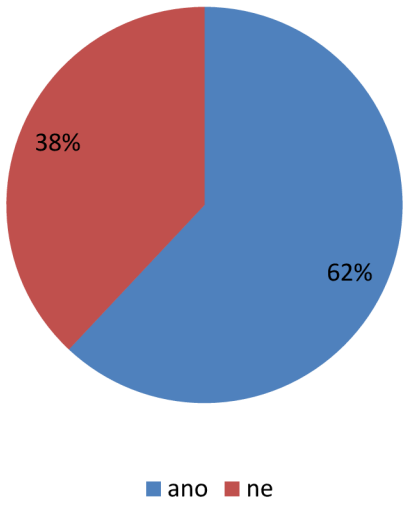
V této otázce jsem se zabývala zobrazením pozdější prevence proti útokům na internet banking ve zpravodajských článcích. Tato prevence je pro uživatele zpravodajství přidanou hodnotou, neboť je zároveň učí bezpečnostní gramotnosti. Její zprostředkování médii je proto velice žádoucí pro zamezení podobných útoků v budoucnosti.

[106] O tomto útoku více v poznámce č. 70.

Prevence byla zobrazena u 48 článků z celkového počtu 78 zkoumaných článků, přičemž u jednoho článku z Novinky.cz se zobrazila u článku se dvěma proměnnými v kategorii typu útoku, a naopak u jednoho článku z iHNed.cz chyběla opět u článku se dvěma proměnnými v té samé kategorii.

5.4.1. Odpověď na výzkumnou otázku č. 3

Odpověď na výzkumnou otázku lze vidět na obrázku č. 10. Z toho vyplývá, že média téměř ze dvou třetin prevenci útoků zobrazují. Přesto se domnívám, že by pozdější bezpečnostní opatření měla být zobrazena daleko častěji.



Obrázek 7 (Ne)zobrazení prevence v médiích (v procentech)

Fakt, že prevence nebyla v článcích zobrazena, vyplývá zejména z cíle útoků. Uživatel se nemůže poučit z útoku typu DDoS[107] nebo hackingu[108], z důvodů, že tyto útoky na něj nejsou zacíleny[109]. Z výzkumu nicméně vyplynulo, že média poměrně často (z 44 %) nepopisují prevenci proti malware, což je zarážející. Tento fakt můžeme vidět na obrázku č. 11. V tomto případě bych očekávala, že média budou uživatele informovat o základních bezpečnostních opatřeních, jako např. aktualizace operačního systému a antivirového systému, a o dalších pravidlech bezpečného chování na internetu[110]. Zpravodajské články také mohou obsahovat přehled antivirových nástrojů, které může uživatel využít. Tyto přehledy se objevily v jednom článku z celkových osmi popisujících příslušná bezpečnostní opatření.

Dále bych očekávala, že ve článku věnujícímu se prolomení hesel, bude informace o nutnosti tvorby silných hesel. Tento útok se sice týkal bankovního serveru,

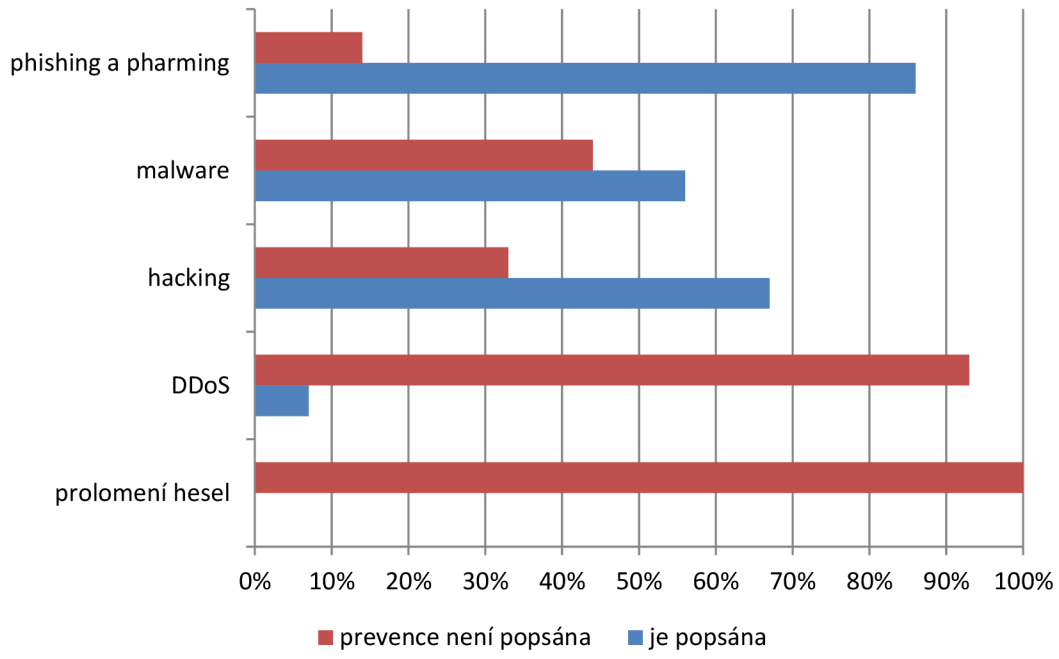
[107] Uživatel se může bránit pouze tím, že zabrání svému počítači, aby se z něj stala zombie (více v kapitole 2.1.4). Zde se nicméně jedná o obranu proti malware. Útočníci si ale pravděpodobně najdou dostatek jiné výpočetní kapacity, aby mohli tento útok provést.

[108] Kromě popisu tvorby silných hesel, viz další odstavec.

[109] Jak je popsáno v další otázce, v některých zpravodajstvích byla prevence proti těmto útokům přesto blíže definována.

[110] Tyto zásady jsou blíže popsány v kapitole 1.3.5.

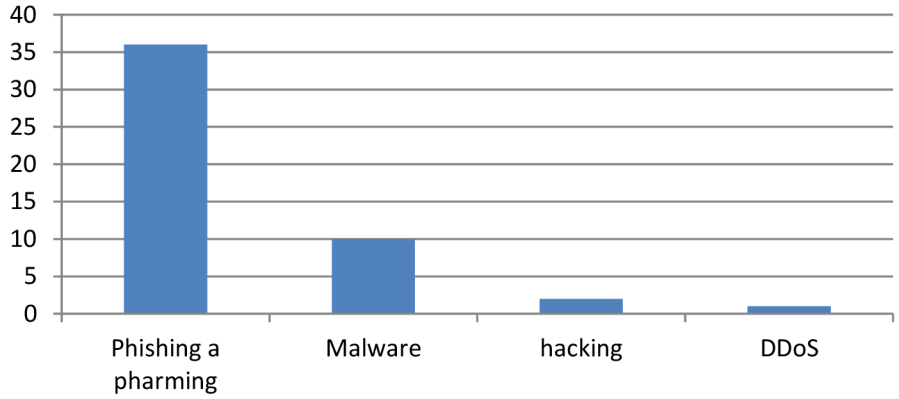
nicméně uživatelé také musí vytvářet hesla, např. pro přístup do internetového bankovnictví.



Obrázek 8 Rozložení popisu preventivních opatření u jednotlivých typů útoků

5.5. Výzkumná otázka č. 4

Tato výzkumná otázka rozvíjí předchozí, protože se v ní zaměřuji na popis pozdější prevence proti útokům na internetové bankovnictví. Jak bylo popsáno v předchozí kapitole, prevence byla zobrazena u 48 zpravodajských článků z celkových 78. Obrázek č. 12 ukazuje typy útoků, u kterých byla prevence zobrazena. Jak z tohoto grafu vyplývá, nejvíce pozornosti se věnuje prevenci proti phishingu a pharmingu, což koresponduje s faktem, že tyto útoky jsou v médiích nejčastěji zobrazovány[111].



Obrázek 9 Typy útoků, u nichž byla zobrazena prevence

[111] Viz odpověď na výzkumnou otázku č. 2 v kapitole *5.3.1.*

5.5.1. Odpověď na výzkumnou otázku č. 4

Odpověď na tuto otázku rozdělím do podkapitol podle typů útoku popsaných výše. Objeví se tedy následující podkapitoly: phishing a pharming, malware a hacking, který jsem se z důvodů nízkého počtu článku rozhodla spojit s útokem DDoS. Zobrazené pokyny jsem vytvořila kompilační metodou, kdy byly vypsány společné znaky pokynů.

5.5.1.1. Phishing a pharming

Bezpečnostní opatření se v tomto případě věnují chování uživatelů při komunikaci s bankou prostřednictvím e-mailu. V pokynech je zdůrazňováno, že banka s klienty nekomunikuje pomocí e-mailu, a tedy po nich nemůže vyžadovat žádné údaje pomocí e-mailu. Zprávy obecně vyzývaly klienty k opatrnosti při poskytování svých přihlašovacích a jiných osobních údajů. Zpravodajství iHNed.cz využilo falešné e-maily, aby na nich demonstrovalo znaky podvodných e-mailů. Klienti, používající službu internet bankingu, by neměli na tyto zprávy reagovat, eventuálně by o nich měli informovat svou banku.

Dále se pokyny týkaly odkazů, obsažených v e-mailu. Např. zpráva ve zpravodajství iDnes.cz uvedla, aby klienti zvýšili svou pozornost v případě, že se v e-mailu objevila pouze IP adresa internetového bankovnictví místo doménové. Dále se doporučuje pečlivě zkontrolovat URL adresu aplikace uvedenou v e-mailu. Novinky.cz zprostředkovaly bezpečnostní opatření od FBI, kde bylo mj. uvedeno, aby uživatelé neotvírali přílohy e-mailů a ověřovali pravost zpráv.

iHNed.cz také zdůraznilo nutnost zabezpečení autentizace uživatele. Jako optimální řešení bylo uživatelům doporučeno použití autentizačních kalkulátorů a čipových karet, obsahujících kryptografické klíče.

Při pharmingu útočníci využívají také virus v počítači uživatele, který jej přesměruje na falešné stránky. V případě, že uživatel ví o přítomnosti viru v počítači, neměl by již z tohoto přístroje přistupovat k bankovní aplikaci. Proti zamezení nákazy články mj. doporučují navštěvovat pouze známé a důvěryhodné webové stránky a přistupovat k účtu ze zabezpečených počítačů s aktualizovaným operačním systémem. Rozhodně se nedoporučuje využívat k přístupu do bankovní aplikace veřejné počítače nebo stahovat do počítače soubory z podezřelých webových stránek.

Uživatelé by celkově měli věnovat pozornost jakékoli odchylce od standardního chování aplikace internetového bankovnictví. Dále by měli využívat kvalitní antivirové programy na ochranu svého počítače a ty by měli udržovat aktualizované. V příspěvku „Spořitelna čelí nové hrozbě“ se dokonce objevila formulace Radka Smolíka, generálního ředitele firmy Symantec: „Nechci-li investovat do zabezpečení, měl bych radši chodit do banky pěšky“ (Záluský a kol., 2008).

5.5.1.2. Malware

Proti malware celkově články vyzdvihovaly zejména nutnost kvalitního antivirového programu, který by měl být pravidelně aktualizován. Ve zpravodajství Novinky.cz byl dokonce uveden přehled těchto programů. Při útoku pomocí viru, který dokázal obejít i autorizační SMS, byla jako opatření doporučena kontrola těchto zpráv.

Uživatelé dále neměli zadávat do internetového bankovnictví autorizační údaje k platbě, kterou sami neiniciovali.

Stejně jako v předchozí kapitole i zde byla zdůrazněna opatrnost uživatelů a sledování jakýchkoli změn v postupech v internetovém bankovnictví. Tyto změny se mohou týkat např. přihlašovacích formulářů, opakovaných výzev k zadání hesla apod.

5.5.1.3. Hacking a DDoS

Opatření proti hackingu a DDoS se téměř neobjevila. Některá média přesto prevenci proti těmto útokům zobrazila, konkrétně iDnes.cz, kde bylo uvedeno, jak se proti hackingu bránit využíváním klientských certifikátů a ověřovacích SMS. Ve zpravodajství Aktuálně.cz se uživatelé mohou dočíst, že obrana proti DDoS útokům ze strany serveru je možná, a to pomocí blokování internetového provozu firewallem a poučením z předchozích útoků DDoS na jiné servery.

Závěr

Ve své práci jsem se soustředila na provedení výzkumu mediálních obsahů, popisujících útoky na internetové bankovnictví. Zkoumané informace jsou uživatelům zprostředkovávány internetovými zpravodajstvími, kde jsem předpokládala více článků než v ostatních médiích. On-line média totiž nejsou omezena počtem ani rozsahem příspěvků, tudíž by se zde mohlo nacházet více informací. Zprávy nicméně měly poměrně malou návratnost (celkem 78 článků ze 4 zpravodajství)[112]. Zpravodajství se totiž soustředí většinou na domácí zprávy, a Česká republika pravděpodobně nabízí pro kyberzločince doposud malý trh[113]. Je ale možné, že se ČR stane po zvýšení rezistence uživatelů větších trhů perspektivnější cílovou lokací útoků.

Každá žurnalistická zpráva by měla odpovědět na šest základních otázek: Kdo? Co? Kde? Kdy? Jak? Proč? Na tuto základní žurnalistickou poučku jsem se zaměřila v první výzkumné otázce. Po provedení výzkumu jsem zjistila, že média poskytují uživatelům relativně vysoký počet odpovědí. Přesto bych jako informační zdroj nedoporučila zpravodajství Novinky.cz, které nezodpověděly tyto otázky z 8 %. Důvodem je časté rekapitulování uskutečněných útoků na internetové bankovnictví ve zprávách o jiných jevech. Označení Novinek.cz za nejméně kvalitní odpovídá i můj subjektivní názor na zpravodajství, kdy se v průběhu výzkumu zprávy kódovaly hůře než u jiných zdrojů. Naopak nejkvalitnější zprávy se nacházely na serveru Aktuálně.cz, kde se neobjevily odpovědi na pouhá 4 % otázek. Zpravodajství iHNed.cz, vyprofilované jako odborné periodikum, nedosáhlo očekávané žurnalistické kvality (z 5 % se neobjevily odpovědi na základní otázky) ani návratnosti článků o ekonomické kyberkriminalitě.

Druhá otázka ukázala zaměření periodik na útoky na uživatele. Jeden z možných důvodů je, že banky neposkytují informace o útocích cílících na jiné prvky bankovního procesu. Média tedy nemají uživatelům co zprostředkovat. V tom se shodují odborné zdroje, např. monografie autorů Vaška Matyáše a Jana Krhovjáka (Matyáš a Krhovják, 2008) nebo Michala Matějky (Matějka, 2002) a další. Zprávy následně v očích veřejnosti vzbuzují dojem, že není potřeba posilovat bezpečnost internetového bankovnictví na straně banky. Mediální obraz bankovních institucí proto vypadá tak, že banky jsou důvěryhodné a zabezpečené, útoky na ně jako velice složité. Banky se neposkytováním informací snaží vyhnout ztrátě klientů[114] a zároveň většímu investování do aplikací internetového bankovnictví a jejich zabezpečení. Teoreticky je také možné, že útoky na bankovní servery jsou schovány pod hlavičkou „náhlý výpadek systému" apod. Těchto zpráv je totiž v internetovém zpravodajství více, než zpráv o útocích na internetové bankovnictví. Dalšími možnými příčinami jsou: buď útoky opravdu neprobíhají, nebo se nedostanou z vnitřního prostředí banky, jak bylo uvedeno výše[115].

---

[112] Tato nízká návratnost je důvodem, proč jsem se odchýlila od svého projektu. V něm jsem uvedla, že obsahová analýza bude jádrem mojí práce, ale tento cíl se nedal aplikovat na nízký počet článků.

[113] Menší procento využívání internetového bankovnictví celkovou populací má v Evropské unii Bulharsko, Itálie, Kypr, Maďarsko, Portugalsko, Rumunsko a Řecko (Informační technologie v domácnostech a mezi jednotlivci, 2013).

[114] To se stalo např. při útoku na Citibank v roce 1994, který je popsán v kapitole 2.4.1.

[115] Příkladem „ochoty" bank poskytovat informace o útocích nebo zranitelnostech mohou být problémy s uveřejněním výzkumu Rastislava Turka o bezpečnosti certifikátů SSL, používaných českými a slovenskými bankami (Turek, 2008; Turek, 2009).

Preventivní opatření byla zobrazena v méně než dvou třetinách článků. Pokyny se většinou týkaly phishingu a pharmingu, kdy uživatelům doporučily nereagovat na e-maily od banky, neklikat na odkazy v e-mailech a nezadávat do e-mailu žádné údaje. Výjimečně byly uvedeny znaky podvodných e-mailů nebo přímo ukázky e-mailů. Dále by uživatelé měli přistupovat k internetovému bankovnictví ze známých počítačů s aktualizovaným operačním systémem a antivirovým programem, aby nedošlo k nakažení počítače malwarem. Co se týče malware, zprávy obsahovaly poměrně málo doporučení, převážně se týkajících nutnosti kvalitního antivirového nástroje. Obecně se doporučovalo sledovat jakékoli odchylky od standardního chování aplikace. Zprávy tedy víceméně nevyužily příležitost přidat článkům další informační hodnotu pro uživatele.

Přitom je posilování mediální agendy o útocích na on-line banking důležité proto, že finanční ztráty, způsobené úspěšným útokem, banka nemusí nahradit z důvodu přenesení zodpovědnosti za správu koncového prvku na klienta. Tento fakt je ale málo známý[116]. Další informační zdroje, např. právě zpravodajství, by tudíž měly posilovat v klientech zodpovědnost. Mediální agenda by se měla rozšiřovat také proto, aby se předešlo možným obavám uživatelů z této služby, pramenící z nedostatku informací uživatelů mj. o používání a zabezpečení on-line bankingu. Kdyby došlo k rozšíření mediální agendy o internetovém bankovnictví a související kyberkriminalitě, možná by došlo také k většímu využívání této užitečné služby uživateli.

Oblast, na kterou by se dalo zaměřit v dalších výzkumech, je hermeneutická kvalitativní analýza zpravodajských textů, týkajících se kyberkriminálních činů. Také by bylo přínosné prozkoumat dopady těchto textů na uživatele, např. pomocí dotazníkového šetření. Výzkumníci by se také mohli orientovat na formální stránku článků, např. zdroje článků, terminologickou správnost nebo citovou neutrálnost zpráv[117]. Z výzkumu zdrojů by se dalo vypozorovat, jestli se novináři spoléhají na tiskové zprávy banky nebo čerpají informace z dalších zdrojů, a tedy jestli se snaží poskytovat kvalitní zprávy ověřené dalšími zdroji.

[116] Zde vycházím ze svého zjištění, formulovaného na základě dokumentové analýzy, kdy jsem informace o této zodpovědnosti nalezla pouze v monografii „Autorizace elektronických transakcí a autentizace dat i uživatelů“ autorů Matyáše a Krhovjáka. Dále v pokynech několika málo bank, např. PPF banky apod.

[117] Dva poslední jsou faktory, ovlivňující vnímání zprávy uživateli.

Seznam zkratek, obrázků a tabulek

Seznam zkratek

ARP - Adress Resolution Protocol
ČR – Česká republika
ČS – Česká spořitelna
ČSOB – Československá banka obchodní
DNS - Domain Name Server
HTML - HyperText Markup Language
HTTP - HyperText Transfer Protocol
ISP – Internet Service Provider (poskytovatel internetového připojení)
NFC – Near Field Communication
QR kód – Quick Response kód
SSL - Secure Socket Layer
TLS – Transport Layer Security
TCP/IP – Transmission Control Protocol / Internet Protocol
URL - Uniform Resource Locator

Seznam obrázků

Obrázek 1 Uživatelé internetového bankovnictví v ČR (v procentech), zdroj: Informační technologie v domácnostech a mezi jednotlivci, 2012 ... 11
Obrázek 5 Rozložení relevantních zpráv podle internetových zpravodajství ... 47
Obrázek 6 Časová řada útoků na on-line bankovnictví ... 48
Obrázek 7 Množství informací o poškozených uživatelích podle počtu proměnných ... 53
Obrázek 8 Množství informací o zcizených financích podle počtu proměnných ... 54
Obrázek 9 Četnost typů útoku v procentech ... 55
Obrázek 10 (Ne)zobrazení prevence v médiích (v procentech) ... 56
Obrázek 11 Rozložení popisu preventivních opatření u jednotlivých typů útoků ... 57
Obrázek 12 Typy útoků, u nichž byla zobrazena prevence ... 57

Seznam tabulek:

Tabulka 1 Používané autentizační metody ... 16
Tabulka 2 Počet návštěvníků internetových zpravodajství, zdroj: Měsíční zpráva: Březen 2013, 2013 ... 44
Tabulka 3 Časové rozložení zpráv ... 48
Tabulka 4 Počet proměnných v jednotlivých kategoriích ve zpravodajství Novinky.cz. 49
Tabulka 5 Analýza zpravodajství Novinky.cz podle odpovědí na 6 otázek kvalitního zpravodajství ... 50
Tabulka 6 Počet proměnných v jednotlivých kategoriích ve zpravodajství iDnes.cz ... 50
Tabulka 7 Analýza zpravodajství iDnes.cz podle odpovědí na 6 otázek kvalitního zpravodajství ... 51
Tabulka 8 Počet proměnných v jednotlivých kategoriích ve zpravodajství iHNed.cz ... 51
Tabulka 9 Analýza zpravodajství iHNed.cz podle odpovědí na 6 otázek kvalitního zpravodajství ... 51

Tabulka 10 Počet proměnných v jednotlivých kategoriích ve zpravodajství Aktuálně.cz 52
Tabulka 11 Analýza zpravodajství Aktuálně.cz podle odpovědí na 6 otázek kvalitního zpravodajství 52
Tabulka 12 Četnost zobrazených typů útoku v jednotlivých zpravodajstvích 54

Použitá literatura

Monografie:

1. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

2. JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

3. JIRÁK, Jan a Barbara KÖPPLOVÁ. *Masová média*. Vyd. 1. Praha: Portál, 2009, 413 s. ISBN 978-807-3674-663.

4. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

5. KÜMMEL, Roman. *XSS: Cross-Site Scripting v praxi : o reálných zranitelnostech ve virtuálním světě*. Zlín: Tigris, 2011, 330 s. ISBN 978-80-86062-34-1.

6. MÁČE, Miroslav. *Platební styk: klasický a elektronický*. 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.

7. MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

8. MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008, 125 s. ISBN 978-802-1045-569.

9. MUSIL, Josef. *Elektronická média v informační společnosti*. Praha: Votobia, 2003, 261 s. ISBN 80-722-0157-3.

10. OSVALDOVÁ, Barbora a Alena LÁBOVÁ. *Zpravodajství v médiích*. Vyd. 1. Praha: Karolinum, 2001, 155 p. ISBN 80-246-0248-2.

11. PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy : vše o používání karet, banka po telefonu a v počítači, je to opravdu bezpečné, pohledy do zákulisí - jak to dělá banka, co nás čeká zítra?, praktické informace pro všechny případy*. Vyd. 1. Praha: Computer Press, 2000, xii, 166 s. Praxe manažera. ISBN 80-7226-328-5.

12. SCHULZ, Winfried. *Analýza obsahu mediálních sdělení*. 3. nezměněné vyd. Překlad Barbara Köpplová. Praha: Karolinum, 2011, 149 s.:. ISBN 978-802-4619-804.

13. URBAN, Lukáš, Josef DUBSKÝ a Karol MURDZA. *Masová komunikace a veřejné mínění*. Vyd. 1. Ilustrace Zdeněk Prošek. Praha: Grada, 2011, 230 s. Žurnalistika a komunikace. ISBN 978-802-4735-634.

14. WALL, David S. *Cybercrime the transformation of crime in the information age*. reprint. Cambridge, UK: Polity, 2008. ISBN 07-456-2736-6.

Online zdroje:

1. Aktuality: Informace o dočasné nedostupnosti online služeb. *Česká spořitelna* [online]. 06.03.2013 [cit. 2013-05-21]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_1837.xml?archivePage=news_archive_subportal03&navid=

2. Aktuality: Pomoc klientům s virem Sinowal/Mebroot - update komunikace. *Česká spořitelna* [online]. 17.07.2008 [cit. 2013-05-10]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_474.xml

3. Bezpečnost mobilního bankovnictví a aplikace Mobilní eKonto. *Raiffeisen Bank* [online]. 2008 [cit. 2013-06-16]. Dostupné z: https://www.rb.cz/osobni-finance/bezne-ucty/prime-bankovnictvi/mobilni-bankovnictvi/bezpecnost-mobilniho-bankovnictvi/

4. Budoucnost distribučních kanálů v České republice a na Slovensku: Trendy a nové vize. In: *Softec CZ* [online]. 2012 [cit. 2013-03-07]. Dostupné z: http://www.softec.cz/files/bankovni_studie/softec_bankovni_studie_cz_2012.pdf

5. Cyber Security: Report. *European Comission* [online]. 2012 [cit. 2013-06-19]. Dostupné z: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

6. CZ.NIC, z.s.p.o. *Jak na internet* [online]. 2012 [cit. 2013-03-31]. Dostupné z: http://www.jaknainternet.cz/page/1264/datove-schranky/

7. Divize Nová média. *IHNed.cz* [online]. 1996 [cit. 2013-04-19]. Dostupné z: http://eol.ihned.cz/o-nas/

8. DNS poisoning, aka pharming, makes the headlines in november's news. In: *EMC2* [online]. 2013 [cit. 2013-04-16]. Dostupné z: http://www.rsa.com/solutions/consumer_authentication/intelreport/11624_Online_Fraud_report_1211.pdf

9. DOBIÁŠ, Jaromír a Zdeněk ŘÍHA. Session Riding. *Zpravodaj ÚVT MU: bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě* [online]. Brno: Ústav výpočení techniky MU, 2009, č. 1 [cit. 2013-05-16]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/625.html

10. Etický kodex novináře. *Syndikát novinářů České republiky* [online]. 2008 [cit. 2013-04-19]. Dostupné z: http://syndikat-novinaru.cz/1/5/36/etika/eticky-kodex

11. Flash note: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps. *ENISA: European Network and Information Security Agency* [online]. 2012 [cit. 2013-05-15]. Dostupné z:

https://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps

12. Informační technologie v domácnostech a mezi jednotlivci. *Český statistický úřad* [online]. 2013 [cit. 2013-06-16]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci

13. Internet Fraud Case – CitiBank – Vladimir Levin. In: *College of Agricultural Banking* [online]. [2004] [cit. 2013-04-20]. Dostupné z: http://www.cab.org.in/Lists/Knowledge%20Bank/Attachments/64/InternetFraud-VL.pdf

14. Internetová žurnalistika: Praktický pohled na práci novináře v online médiu. In: *Katedra hospodářské a sociální politiky* [online]. 2000 [cit. 2013-04-19]. Dostupné z: http://khp.vse.cz/wp-content/uploads/2011/08/Internetova_zurnalistika.pdf

15. Krátkodobé omezení internetového bankovnictví. In: *Vítejte v UniCredit Bank: Novinky* [online]. 2013 [cit. 2013-05-08]. Dostupné z: http://www.unicreditbank.cz/web/novinky/kratkodobe-omezeni-internetoveho-bankovnictvi

16. Kybernetickými útoky se začala zabývat kontrarozvědka. *Česká televize* [online]. 7.3.2013 [cit. 2013-05-21]. Dostupné z: http://www.ceskatelevize.cz/ct24/media-it/217880-kybernetickymi-utoky-se-zacala-zabyvat-kontrarozvedka/

17. Man-in-the-middle attack. In: *OWASP: The Open Web Application Security Project* [online]. 2009 [cit. 2013-05-16]. Dostupné z: https://www.owasp.org/index.php/Man-in-the-middle_attack

18. MARCUS, Dave a Ryan SHERSTOBITOFF. Dissecting Operation High Roller. *McAfee* [online]. 2012 [cit. 2013-05-15]. Dostupné z: http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

19. MCAFEE LABS. McAfee Threats Report: Third Quarter 2012. In: *McAfee* [online]. 2003 [cit. 2013-01-16]. Dostupné z: http://www.mcafee.com/uk/about/newsroom/research-reports.aspx

20. Měsíční zpráva: Březen 2013. In: *SPIR - NetMonitor: Výzkum návštěvnosti internetu v České Republice* [online]. 2013 [cit. 2013-05-08]. Dostupné z: http://www.netmonitor.cz/sites/default/files/vvnetmon/2013_03_netmonitor_offline_report.pdf

21. MIKO, Karel. Internet Banking Attacks. In: BRESLIN, John G a DECKER. *Slideshare* [online]. 2009 [cit. 2013-03-16]. Dostupné z: http://www.slideshare.net/DCIT/internet-banking-attacks-karel-miko?from=ss_embed

22. *Mobito: Peníze v mobilu* [online]. [2012] [cit. 2013-06-18]. Dostupné z: http://www.mobitoplatito.cz/

23. MOYER, Kristin R. Globální trendy v bankovnictví. *Bankovnictví* [online]. 2013, č. 2 [cit. 2013-04-17]. Dostupné z: http://bankovnictvi.ihned.cz/c1-59391610-globalni-trendy-v-bankovnictvi

24. Novinky.cz. *Seznam.cz: O nás* [online]. 1996 [cit. 2013-04-17]. Dostupné z: http://onas.seznam.cz/cz/novinky-cz.html

25. O mBank. *MBank* [online]. [2007] [cit. 2013-06-19]. Dostupné z: http://www.mbank.cz/mbank/

26. O PPF bance. *PPF banka* [online]. 2013 [cit. 2013-06-19]. Dostupné z: http://www.ppfbanka.cz/cz/o-nas/o-ppf-bance.html

27. PAGET, Francois. Financial Fraud and Internet Banking: Threats and Countermeasures. [online]. 2009 [cit. 2013-01-16]. Dostupné z: http://www.mcafee.com/uk/resources/reports/rp-financial-fraud-int-banking.pdf

28. Phishing Activity Trends Report. *Anti-Phishing Working Group* [online]. 2012 [cit. 2013-04-16]. Dostupné z: http://anti-phishing.org/reports/apwg_trends_report_q2_2012.pdf

29. PLETZER, Valentin. Odhalený phishing. *Chip* [online]. 2008, č. 5 [cit. 2013-06-14]. Dostupné z: http://earchiv.chip.cz/cs/earchiv/rubriky/praxe/odhaleny-phishing-10-tipu-pro-bezpecne-internetove-bankovnictvi.html

30. PORTER, Jeremy. Five Ws and One H: The Secret to Complete News Stories. In: *Journalistics* [online]. 5.8.2010 [cit. 2013-06-06]. Dostupné z: http://blog.journalistics.com/2010/five-ws-one-h/

31. Přehled Udělených akreditací. *Ministerstvo vnitra České republiky* [online]. 2010 [cit. 2013-03-30]. Dostupné z: http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx

32. Session hijacking. In: *OWASP: The Open Web Application Security Project* [online]. 2011 [cit. 2013-05-16]. Dostupné z: https://www.owasp.org/index.php/Session_hijacking_attack

33. Seznamy regulovaných a registrovaných subjektů finančního trhu. *Česká národní banka* [online]. 2003 [cit. 2013-03-07]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB07.INTRO_PAGE?p_lang=cz

34. Sm@rt-TAN plus. VOLKSBANK LÖBAU-ZITTAU EG. *CZ Internetový portál banky Löbau-Zittau eG* [online]. 2013 [cit. 2013-04-20]. Dostupné z: http://www.vr-bank.cz/service/anleitung-online-banking/smrt-tan-plus.html

35. Spear-Phishing Email: Most Favored APT Attack Bait. TREND MICRO INCORPORATED. *Trend Micro* [online]. 1989 [cit. 2013-04-25]. Dostupné z: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

36. Symmetric Cryptography: DES and RC4. *Winlab* [online]. 2004 [cit. 2013-03-15]. Dostupné z: http://www.winlab.rutgers.edu/~trappe/Courses/AdvSec05/SymmetricCrypto.pdf

37. TABERY, Paulína. Nastolování agendy a proces rámování. *SOCIOweb: Sociologický webzin* [online]. 2009, č. 3 [cit. 2013-04-15]. Dostupné z: http://www.socioweb.cz/index.php?disp=teorie&shw=385&lst=112

38. Tiráž. *Aktuálně.cz* [online]. 1999 [cit. 2013-06-19]. Dostupné z: http://aktualne.centrum.cz/autori/

39. Trojan-PSW:W32/Sinowal.CP. F-SECURE CORPORATION. *F-Secure* [online]. 2009 [cit. 2013-04-20]. Dostupné z: http://www.f-secure.com/v-descs/trojan-psw_w32_sinowal_cp.shtml

40. Trojan.Spyeye. *Symantec* [online]. 1995 [cit. 2013-05-02]. Dostupné z: http://www.symantec.com/security_response/writeup.jsp?docid=2010-020216-0135-99&tabid=2

41. Trojan.Zbot. *Symantec* [online]. 1995 [cit. 2013-05-02]. Dostupné z: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

42. TODOROV, Dobromir. *Mechanics of user identification and authentication: fundamentals of identity management*. Boca Raton: Auerbach Publications, c2007. ISBN 1420052195.Chapter 1: User Identification and Authentication Concepts. Dostupné z: http://www.infosectoday.com/Articles/AU5219_C01.pdf

43. TUREK, Rastislav. Cielené útoky na klientov banky. *Slideshare* [online]. [2009] [cit. 2013-05-01]. Dostupné z: http://www.slideshare.net/synopsi/clen-toky-na-klienty-banky

44. Typy digitálních certifikátů. *Business Communication* [online]. 2003 [cit. 2013-04-25]. Dostupné z: http://www.certifikaty.com/certifikaty/typy-digitalnich-certifikatu

45. Unicredit Bank úpěla pod náporem hackerů, na web dali prohlášení. In: *Česká televize* [online]. 2013 [cit. 2013-05-08]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/218473-unicredit-bank-upela-pod-naporem-hackeru-na-web-dali-prohlaseni/

46. VORLÍČEK, Jaroslav a Ondřej SUCHÝ. Útok na uživatele internetového bankovnictví. *Logios* [online]. 2005 [cit. 2013-06-19]. Dostupné z: http://enlogit.com/dl/whitepapers/utok-na-internetbanking.pdf

47. What is a QR code?. DENSO WAVE INC. *QR Code.com* [online]. [cit. 2013-06-03]. Dostupné z: http://www.qrcode.com/en/about/

48. ZAHRADNICKÝ, Tomáš. Bezpečnost a bezpečné programování: 10. Bezpečnost webových aplikací. *EDUX.FIT.CVUT.CZ* [online]. 2011 [cit. 2013-05-15]. Dostupné z: https://edux.fit.cvut.cz/oppa/MI-BPR/prednasky/bpr-10.pdf

49. ZÁLUSKÝ, Jan, Olga SKALKOVÁ a Otakar SCHÖN. Spořitelna čelí nové hrozbě. *IHNed.cz* [online]. 2008 [cit. 2013-06-05]. Dostupné z: http://vyhledavani.ihned.cz/?p=00000S_d&article[id]=23467080&article[sklonuj]=on&article[what]=internetov%E9+bankovnictv%ED

50. ZÁVODSKÝ, Petr. XSS stále na scéně. *Root.cz* [online]. 2011 [cit. 2013-04-30]. Dostupné z: http://www.root.cz/clanky/xss-stale-na-scene/

Přílohy

Příloha č. 1 - Kódovací schéma

Napadená instituce (podle počtu klientů)

0. neuvedeno
1. ČS (5 mil. klientů)
2. ČSOB (3 mil. klientů)
3. KB (1,6 mil. klientů)
4. Air Bank, Equa bank, mBank a Fio banka a ZUNO
5. jiné české banky
6. zahraniční banky

Napadený prvek systému:

0. neuvedeno
1. uživatel (koncové zařízení)
2. poskytovatel ISP
3. komunikační kanál
4. webová aplikace
5. bankovní server
6. jiné

Lokace cíle útoku:

1. ČR
2. zahraničí

Čas, kdy byl útok proveden. Stačí formulace “v minulých dnech”, “nedávno”, “v poslední době” apod.

1. uvedeno
0. neuvedeno

Způsob provedení útoku

Vychází z kategorií útoků v druhé části.

0. Neuvedeno
1. Hacking – např. prolomení hesel
2. phishing a pharming (přesměrování)
3. malware
4. XSS, XSRF a clickjacking
5. Útok ze středu
6. Smíšená hrozba (útok za použití více metod vstupu)[118]
7. DDoS

[118] O smíšené hrozbě, neboli „Blended threat“, píšu na straně 29.

Účel útoku

0. neuvedeno
1. finanční - krádež financí
2. zamezení přístupu uživatelů
3. poškození image banky

Následující dvě kategorie upřesňují poškození uživatelů internetového bankovnictví.

Počet poškozených uživatelů IB.

0. neuvedeno
1. 0
2. 1 - 1000
3. 1 001 - 10 000
4. 10 001 - 50 000
5. 50 001 - 100 000
6. 100 001 - 300 000
7. 300 001 - 500 000
8. 500 000 - 750 000
9. 750 001 - 1 000 000
10. 1 000 001 a více

Úspěšnost útoku podle množství zcizených financí

0. neuvedeno
1. 0
2. 1 - 100 tis. Kč
3. 100 tis kč - 500 000 kč
4. 500 001 - 1 mil. kč
5. 1 mil. - 5 mil. kč
6. 5 mil. kč a více

Proměnné k otázce č. 3

Preventivní opatření:

1. byla zmíněny
0. nebyla zmíněny

Příloha č. 2 - Provedená obsahová analýza

Novinky.cz				analytická část									
identifikační část													
Datum	čas	Název	odkaz	Přítomnost proměnných								Bezp. prevence	Popis prevence
6.1.2008	17:34	Česká spořitelna se stala terčem internetového útoku	http://www.novinky.cz/ekonomika/130068-ceska-sporitelna-se-stala-tercem-internetoveho-utoku.html	1	1	1	1	2	1	1	1	1	Klienti by na tuto výzvu podle ní neměli reagovat, protože banka takovým způsobem nekomunikuje. = nereagovat na e-maily
26.2.2008	13:54	Česká spořitelna varuje před podvodnými e-maily	http://www.novinky.cz/ekonomika/134050-ceska-sporitelna-varuje-pred-podvodnymi-e-maily.html	1	1	1	0	2	1	2	1	1	Klienti by na tyto zprávy neměli vůbec reagovat.
4.3.2008	18:19	Česká spořitelna kvůli podvodným e-mailům podá trestní oznámení	http://www.novinky.cz/ekonomika/134600-ceska-sporitelna-kvuli-podvodnym-e-mailum-poda-trestni-oznameni.html	1	1	1	1	2	1	0	1	1	Spořitelna přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a tyto údaje od nich nikdy nevyžaduje.
17.3.2008	20:51	Phishingová kampaň na klienty České spořitelny má první oběti	http://www.novinky.cz/ekonomika/135545-phishingova-kampan-na-klienty-ceske-sporitelny-ma-prvni-obeti.html	1,5	1	1	1	2	1	0	0	1	Spořitelna přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a tyto údaje od nich nikdy nevyžaduje.
16.4.2009	10:30	Čtyři z pěti virů chtěly loni ukrást uživatelům data, tvrdí analýza	http://www.novinky.cz/internet-a-pc/software/166520-ctyri-z-peti-viru-chtely-loni-ukrast-uzivatelum-data-tvrdi-analyza.html	6	1	2	1	2,3	1	0	0	1	emaily - neklikat na přílohy a odkazy, ověřit pravost e-mailu, nevyplňovat údaje do e-mailu, zadávat odkaz ručně
11.5.2009	UPDATE 11:50	České spořitelně nefungovalo dvě hodiny internetové bankovnictví	http://www.novinky.cz/internet-a-pc/168423-ceske-sporitelne-nefungovalo-dve-hodiny-internetove-bankovnictvi.html	1	1	1	1	2	1	0	0	0	
2.12.2010	16:41	Počítačoví piráti berou Vánoce útokem	http://www.novinky.cz/internet-a-pc/testy/218558-pocitacovi-pirati-berou-vanoce-utokem.html	6	1	2	1	3	1	0	6	1	Přehled antivirových programů
23.4.2011	19:03	České banky ohrožují hackeři, z klientů lákají data o účtech	http://www.novinky.cz/internet-a-pc/bezpecnost/231629-ceske-banky-ohrozuji-hackeri-z-klientu-lakaji-data-o-uctech.html	1,5	1	1	1	2	1	0	0	1	Klienti by na tyto zprávy neměli vůbec reagovat.

8.1.2012	7:13	Nebezpečný počítačový virus vykrádá lidem bankovní účty	http://www.novinky.cz/internet-a-pc/bezpecnost/255595-nebezpecny-pocitacovy-virus-vykrada-lidem-bankovni-ucty.html	0	1	2	1	3	1	0	0	0	
27.6.2012	10:10	Zákeřný program ukradl loni přes internet 1,6 miliardy korun	http://www.novinky.cz/internet-a-pc/bezpecnost/271643-zakerny-program-ukradl-loni-pres-internet-1-6-miliardy-korun.html	6	1	2	1	3	1	0	6	0	
20.8.2012	12:34	Hackeři se snaží vylákat peníze z klientů České spořitelny	http://www.novinky.cz/ekonomika/276460-hackeri-se-snazi-vylakat-penize-z-klientu-ceske-sporitelny.html	1	1	1	0	3	1	0	0	1	nezadávat autorizační kód pro transakci, neprovedenou uživatele IB; kontrola autorizačních SMS,
21.12.2012	13:15	Zákeřný virus se snaží z klientů České spořitelny vylákat peníze	http://www.novinky.cz/internet-a-pc/bezpecnost/288474-zakerny-virus-se-snazi-z-klientu-ceske-sporitelny-vylakat-penize.html	1,6	1	1,2	1	3	1	0,4	0,6	1	nezadávat autorizační kód pro transakci, neprovedenou uživatele IB; kontrola autorizačních SMS,
6.3.2013	UPDATE 12:10	Internetové bankovnictví zkolabovalo, další kybernetický útok mířil na banky	http://www.novinky.cz/internet-a-pc/295187-internetove-bankovnictvi-zkolabovalo-dalsi-kyberneticky-utok-miril-na-banky.html	1,2,3,5	5	1	1	7	2	0	0	0	
6.3.2013	UPDATE 12:35	Český internet čelí nejmasivnějším pirátským útokům v historii	http://www.novinky.cz/internet-a-pc/bezpecnost/295218-cesky-internet-celi-nejmasivnejsim-piratskym-utokum-v-historii.html	0	5	1	1	7	2	0	0	0	
7.3.2013	UPDATE 10:49	Další vlně masivních kybernetických útoků čelí mobilní operátoři	http://www.novinky.cz/internet-a-pc/bezpecnost/295325-dalsi-vlne-masivnich-kybernetickych-utoku-celi-mobilni-operatori.html	0	5	1	1	7	2	0	0	0	
7.3.2013	11:47	Dalším cílem útoků hackerů může být i správce českých domén .cz	http://www.novinky.cz/internet-a-pc/bezpecnost/295349-dalsim-cilem-utoku-hackeru-muze-byt-i-spravce-ceskych-domen-cz.html	0	5	1	1	7	2	0	0	0	
7.3.2013	UPDATE 21:50	České televizi přestaly fungovat internetové stránky	http://www.novinky.cz/internet-a-pc/295417-ceske-televizi-prestaly-fungovat-internetove-stranky.html	0	0	1	1	7	0	0	0	0	

iDnes.cz						
identifikační část				analytická část		
Datum	čas	Název	odkaz	Přítomnost proměnných	Bezp. prevence	Popis prevence

6.1.2008	17:33	Klienty spořitelny atakují další podvodné e-maily	http://ekonomika.idnes.cz/klienty-sporitelny-atakuji-dalsi-podvodne-e-maily-fwd-/ekonomika.aspx?c=A080106_173631_ekonomika_zra	1	1	1	1	2	1	1	0	1	Česká spořitelna žádnou takovou zprávu nerozesílala a s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je zabezpečení,
10.3.2008	UPDATE 20:13	Drahoušci České spořitelny vyhrávají 50 dolarů. Podvodné dopisy opět kolují	http://technet.idnes.cz/drahousci-ceske-sporitelny-vyhravaji-50-dolaru-podvodne-dopisy-opet-koluji-16o-/sw_internet.aspx?c=A080310_184512_sw_internet_NYV	1	1	1	1	2	1	1	0	1	Česká spořitelna s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je např. zabezpečení.
14.3.2008	UPDATE 12:35	Josef Džubák: Phishing není žádná novinka. Ignorujte ho	http://ekonomika.idnes.cz/josef-dzubak-phishing-neni-zadna-novinka-ignorujte-ho-pfk-/test.aspx?c=A080312_232855_spotrebitel_maf	1	1	1	1	2	1	0	0	1	Česká spořitelna s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je např. zabezpečení.
14.3.2008	8:45	Útoky internetových podvodníků se stupňují	http://ekonomika.idnes.cz/utoky-internetovych-podvodniku-se-stupnuji-fnc-/ekonomika.aspx?c=A080314_934072_ekonomika_vem	1,5	1	1	1	2	1	1	0	1	Česká spořitelna s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je např. zabezpečení.
18.3.2008	1:03	Internetoví podvodníci se zlepšují. Ochrana účtů je stále těžší	http://ekonomika.idnes.cz/internetovi-podvodnici-se-zlepsuji-ochrana-uctu-je-stale-tezsi-pw1-/test.aspx?c=A080317_205010_spotrebitel_mia	1	1	1	1	2	1	2	0	1	Zástupci bank, které působí na českém trhu, se shodují v tom, že klienti by měli mít především důkladně zabezpečený počítač. Doporučují také, aby se klienti nikdy nehlásili na svůj účet z cizího počítače. Tedy ani z internetové kavárny. Klíčové je i maximální možné zabezpečení počítačů a pravidelná aktualizace operačních systémů.
20.3.2008	17:08	Piráti začali přesměrovávat weby služeb internetového bankovnictví	http://ekonomika.idnes.cz/pirati-zacali-presmerovavat-weby-sluzeb-internetoveho-bankovnictvi-12t-/test.aspx?c=A080320_170832_spotrebitel_maf	1	1	1	0	2	1	1	0	1	Uživatelé internetbankingu by proto měli dávat pozor, zda se jejich počítač nechová nestandardně či zda nežádá údaje, které obvykle nechce. Pokud taková situace nastane, radí spořitelna okamžitě internetové bankovnictví ukončit a banku zkontaktovat.
23.5.2008	17:00	Na internetu se objevily podvodné stránky	http://mobil.idnes.cz/na-internetu-se-objevily-podvodne-stranky-unicreditu-pochazi-z-ceska-1k2-	6	1	2	0	2	1	0	0	1	upozornění na závadné stránky + Obecně platí, že žádná banka nežádá klienty

		Unicreditu. Pochází z Česka	/mobilni-operatori.aspx?c=A080523_115932_mob_operatori_hro										prostřednictvím e-mailů o zaslání přihlašovacích údajů do internetového bankovnictví ani PINů platebních karet či dalších podobných údajů. V případě, že se na vás někdo s podobným dotazem obrátí, jde s největší pravděpodobností o podvod a měli byste okamžitě kontaktovat svoji banku. Stejně tak je nepravděpodobné, že by některá ze seriózních bank přesunula své servery na domény označené pouze IP adresou a nikoli doménovým jménem.
17.8.2008	2:24	Česká spořitelna musela potřetí zvýšit zabezpečení účtů, piráti přitvrdili	http://ekonomika.idnes.cz/ceska-sporitelna-musela-potreti-zvysit-zabezpeceni-uctu-pirati-pritvrdili-1vi-/ekonomika.aspx?c=A080716_213012_ekonomika_mia	1	1	1	0	2	1	2	1	1	Vyplatí se navštěvovat jen známé weby a přihlašovat se k účtu z dobře zabezpečených počítačů.
19.10.2008	15:48	Hackeři ukradli Sarkozymu peníze z účtu	http://zpravy.idnes.cz/hackeri-ukradli-sarkozymu-penize-z-uctu-fdl-/zahranicni.aspx?c=A081019_154829_zahranicni_dp	6	5	2	1	1	1	2	2	1	Experti se totiž shodují, že při opatrnosti a využití certifikátů či verifikačních SMS se dá útokům předejít.
22.10.2008	8:54	Policie dopadla hackery, kteří měli Sarkozymu krást peníze z účtu	http://zpravy.idnes.cz/policie-dopadla-hackery-kteri-meli-sarkozymu-krast-penize-z-uctu-py0-/zahranicni.aspx?c=A081022_085414_zahranicni_stf	6	5	2	0	1	1	2	2	1	Experti se totiž shodují, že při opatrnosti a využití certifikátů či verifikačních SMS se dá útokům předejít.
29.7.2010	3:07	Slovinci dopadli nebezpečného hackera, infikoval 12 milionů počítačů	http://zpravy.idnes.cz/slovinci-dopadli-nebezpecneho-hackera-infikoval-12-milionu-pocitacu-1pz-/zahranicni.aspx?c=A100728_203827_zahranicni_vel	0	1	2	0	3	1	10	0	0	
18.10.2010	16:50	Byla odhalena síť 75 000 kompromitovaných počítačů. Napadeny jsou i vládní organizace	http://technet.idnes.cz/byla-odhalena-sit-75-000-kompromitovanych-pocitacu-napadeny-jsou-i-vladni-organizace-gj6-/software.aspx?c=A100218_165019_software_vse	0	1	2	1	3	1	5	0	0	
4.1.2011	15:03	Zloději se v e-mailech snažili vylákat data z klientů Raiffeisenbank	http://ekonomika.idnes.cz/zlodeji-se-v-e-mailech-snazili-vylakat-data-z-klientu-raiffeisenbank-11x-/ekoakcie.aspx?c=A110104_153411_ekoakcie_fih	5	1	1	1	2	1	1	1	1	Raiffeisenbank upozornila, že nikdy neoslovuje své klienty prostřednictvím e-mailu s žádostí o poskytnutí jakýchkoli citlivých dat umožňující přístup k účtu. "Na podobné maily proto nikdy nereagujte, případně o podobných mailech informujte

													banku," varoval Kofroň.
31.1.2011	13:15	Hacker dostal šest let za pokus vysát 3,2 milionu z účtů České spořitelny	http://zpravy.idnes.cz/soud-ulozil-6-let-hackerovi-ktery-napadl-ceskou-sporitelnu-poc-/krimi.aspx?c=A110131_131742_krimi_cen	1	1	1	1	3	1	2	0	0	
4.5.2012	UPDATE 10:59	Česko zasáhly krádeže identit. Podvodníci si zřídí účet na vaše jméno	http://ekonomika.idnes.cz/cesko-zasahly-kradeze-identit-dkl-/ekonomika.aspx?c=A120504_085107_ekonomika_neh	4	1	1	0	2	1	2	0	1	vyzývá k maximální obezřetnosti při jakémkoliv poskytování osobních údajů a kopií průkazů či výpisů z účtu.
20.8.2012	13:54	Na klienty České spořitelny útočí nový virus. Snaží se vylákat kód	http://ekonomika.idnes.cz/na-klienty-ceske-sporitelny-utoci-novy-virus-fof-/ekonomika.aspx?c=A120820_140405_ekonomika_neh	1	1	1	0	3	1	2	0	1	Spořitelna vyzvala klienty, aby kontrolovali obdržené SMS zprávy (účet příjemce, částku a měnu). Nikdy by také neměli zadávat zaslaný kód z autorizační SMS na operaci v internetovém bankovnictví, kterou sami nezadali.
6.3.2013	UPDATE 11:02	Kybernetické útoky dnes pokračovaly. Terčem byly servery českých bank	http://technet.idnes.cz/vypadek-serveru-bank-0r8-/sw_internet.aspx?c=A130306_094423_sw_internet_jw	1,2,3,4,5	5	1	1	7	2	0	0	0	
21.3.2013	UPDATE 15:28	Velký hackerský útok na Jižní Koreu přišel z Číny, ukazuje na KLDR	http://zpravy.idnes.cz/hackersky-utok-na-jizni-koreu-prisel-z-ciny-fe2-/zahranicni.aspx?c=A130321_120006_zahranicni_pps	6	5	2	1	3	3	0	0	0	

iHNed.cz				**analytická část**									
identifikační část													
Datum	Čas	Název	Odkaz	Přítomnost proměnných								Bezp. prevence	Popis prevence
7.1.2008	8:50	Spořitelna je opět cílem internetového útoku	http://vyhledavani.ihned.cz/109-22712390-on-internetov%E9+bankovnictv%ED-00000S_d-bd	1	1	1	1	2	1	0	1	1	Klienti by na výzvu podle ní neměli reagovat, protože banka takovým způsobem nekomunikuje.
4.3.2008	18:49	Podvodné e-maily bude Česká spořitelna řešit	http://vyhledavani.ihned.cz/109-23102750-on-internetov%E9+bankovnictv%ED-00000S_d-93	1	1	1	0	2	1	0	1	1	aktualizace antivirů a dodržování dalších bezpečnostních pravidel

		trestním oznámením											
5.3.2008	17:21	Podvodné e-maily útočící na Českou spořitelnu. Takto vypadají	http://vyhledavani.ihned.cz/109-23111050-on-internetov%E9+bankovnictv%ED-00000S_d-b9	1	1	1	0	2	1	1	1	1	aktualizace antivirů a dodržování dalších bezpečnostních pravidel
11.3.2008	10:19	Útok na klienty spořitelny vrcholí	http://vyhledavani.ihned.cz/109-23196570-on-internetov%E9+bankovnictv%ED-00000S_d-da	1,3,5	1	1	1	2	1	4,2	0	1	ukázky falešných e-mailů
12.3.2008	14:26	Falešné e-maily na ČS pokračují. Varují samy před sebou	http://vyhledavani.ihned.cz/109-23236820-on-internetov%E9+bankovnictv%ED-00000S_d-56	1	1	1	1	2	1	4	0	1	ukázky falešných e-mailů
14.3.2008	19:47	Podvodný mail na Českou spořitelnu má novou podobu	http://vyhledavani.ihned.cz/109-23307950-on-internetov%E9+bankovnictv%ED-00000S_d-3e	1	1	1	1	2	1	0	0	1	S klienty nikdy prostřednictvím e-mailu nekomunikujeme o tak zásadních záležitostech, jako je například zabezpečení. Nikdy nevyžadujeme zadání osobních bankovních údajů jako je například PIN ke kartě či klientské číslo a heslo.
17.3.2008	13:51	ČNB varuje před další sérií podvodných e-mailů	http://vyhledavani.ihned.cz/109-23358400-on-internetov%E9+bankovnictv%ED-00000S_d-fb	5	1	1	1	2	1	0	0	1	Nejsnáze se podvodný e-mail pozná tak, že obsahuje odkaz na internetovou stránku a uživatel je žádán o verifikaci. Když tak učiní, jsou po něm požadovány přihlašovací údaje - jméno a heslo - k internetovému bankovnictví. Banky od svých klientů takové informace nikdy prostřednictvím e-mailů nepožadují.
20.3.2008	16.:00	Hackeři útočí na spořitelnu: Již ne e-maily, ale přímo na web	http://vyhledavani.ihned.cz/109-23452570-on-internetov%E9+bankovnictv%ED-00000S_d-a5	1	1	1	1	2	1	0	1	1	Doporučují přitom lidem, aby si opatřili kvalitní antivirové programy, které jejich počítače před nám ochrání. "Další možností je instalovat zařízení pro elektronický podpis.
21.3.2008	02.:25	Nový útok na spořitelnu	http://vyhledavani.ihned.cz/109-23467800-on-internetov%E9+bankovnictv%ED-00000S_d-b4	1	1	1	1	2	1	1	1	0	
21.3.2008	01:34	Spořitelna čelí nové hrozbě	http://vyhledavani.ihned.cz/109-23467080-on-internetov%E9+bankovnictv%ED-00000S_d-fc	1	1	1	1	2	1	1	1	1	Odborníci doporučují mít kromě nainstalovaných antivirových programů také obousměrný firewall a blokování USB

													portů. Varují před přílišným šetřením. "Nechci-li investovat do zabezpečení, měl bych radši chodit do banky pěšky," říká Radek Smolík, generální ředitel softwarové firmy Symantec. Profesionálové varují také před používáním internetbankingu, který jako přihlašovací údaj používá číslo účtu, či bezpečnostním certifikátem uloženým na pevném disku. Nejlepší řešení je podle nich bezpečnostní kalkulačka a certifikát uložený na čipové kartě. Klasickým doporučením je nenavštěvovat webové stránky s pochybným obsahem. "Útočníci se ale zaměřují i na weby velkých fotbalových klubů či stránky vládních institucí," varuje Obluk.
21.3.2008	8:07	Spořitelna má podezření na druhý pokus o vyloupení účtů	http://vyhledavani.ihned.cz/109-23485930-on-internetov%E9+bankovnictv%ED-00000S_d-3f	1	1	1	1	2	1	1	0	0	
22.3.2008	19:11	Zrádný trojský kůň napadl počítač. Spořitelna peníze uhájila	http://vyhledavani.ihned.cz/109-23489980-on-internetov%E9+bankovnictv%ED-00000S_d-ec	1	1	1	1	2	1	1	0	1	Zavřít okno internetového prohlížeče, na které se přihlašoval a z tohoto počítače se do internetového bankovnictví už nepřihlašovat. + kontaktovat ČS.
27.3.2008	22:57	Spořitelna vyšetřuje dalších 8 pokusů o vykradení účtu	http://vyhledavani.ihned.cz/109-23611950-on-internetov%E9+bankovnictv%ED-00000S_d-d7	1	1	1	1	2	1	1	0	0	
26.3.2010	15:26	Uživatelé on-line bankovnictví by se měli mít na pozoru. Je tu nová hrozba	http://vyhledavani.ihned.cz/109-41902100-on-internetov%E9+bankovnictv%ED-00000S_d-5e	6	1	2	0	3	1	0	0	1	„Jako vždy se internetovým uživatelům důrazně doporučuje, aby při provádění operací on-line bankovnictví dbali zvýšené opatrnosti,“
8.5.2010	15:11	Trojan umožňující bankovní podvody zasáhl ve Velké Británii počítače sta tisíc lidí	http://vyhledavani.ihned.cz/109-45462870-on-internetov%E9+bankovnictv%ED-00000S_d-25	6	1	2	0	3	1	5	0	1	Klein uvedl, že se podvod obtížně odhaluje, ale že by lidé měli být podezíraví, pokud náhle došlo ke změně přihlašovacích postupů na stránky jejich

													internetového bankovnictví nebo pokud byli vyzváni, aby znovu uvedli heslo a další podrobnosti.
14.7.2011	20:13	Mobilní vir krade SMS s potvrzovacími kódy internetového bankovnictví	http://vyhledavani.ihned.cz/109-52304060-on-internetov%E9+bankovnictv%ED-00000S_d-d1	5	1	2	0	3	1	0	0	0	
20.8.2012	20:14	Hackeři napadli internetové bankovnictví České spořitelny. Kvůli autorizačním kódům	http://vyhledavani.ihned.cz/109-57093840-on-internetov%E9+bankovnictv%ED-00000S_d-36	1	1	1	0	3	1	1	0	1	kontrola autorizačních SMS a nezadávání údajů k nepožadované platbě
6.3.2013	18:03	Největší banky v Česku napadli hackeři. Vyřadili jim z provozu internetové bankovnictví	http://vyhledavani.ihned.cz/109-59450640-on-internetov%E9+bankovnictv%ED-00000S_d-31	1,2,3,5	5	1	1	7	2	0	0	0	
6.3.2013	17:25	Bezpečnostní experti už vědí více o kyberútocích. Detaily ale zatím tají	http://vyhledavani.ihned.cz/109-59452500-on-internetov%E9+bankovnictv%ED-00000S_d-89	0	5	1	1	7	3	0	0	0	
7.3.2013	18:25	Kvůli kyberútokům zažíváme černý týden českého internetu, říká počítačový expert	http://vyhledavani.ihned.cz/109-59451940-on-internetov%E9+bankovnictv%ED-00000S_d-51	0	5	1	1	7	3	0	0	0	
7.3.2013	11:35	Týden hackerských útoků: Po médiích a bankách přišli na řadu mobilní operátoři	http://vyhledavani.ihned.cz/109-59459250-on-internetov%E9+bankovnictv%ED-00000S_d-d6	0	5	1	1	7	3	0	0	0	
12.3.2013	16:05	Autory kyberútoků se nám pravděpodobně nepodaří vypátrat, připustil šéf NBÚ	http://vyhledavani.ihned.cz/109-59486950-on-internetov%E9+bankovnictv%ED-00000S_d-05	0,5	5	1	1	1;7	3	0	0	0	
20.3.2013	14:21	Hackeři napadli jihokorejská média a banky. Z počítačů mizely soubory	http://vyhledavani.ihned.cz/109-59542350-on-internetov%E9+bankovnictv%ED-00000S_d-3b	6	5	2	1	1	3	0	0	0	

Aktuálně.cz				analytická část									
identifikační část													
Datum	Čas	Název	Odkaz	Přítomnost proměnných								Bezp. prevence	Popis prevence
7.1.2008	10:43	Klienti České spořitelny se stali terčem podvodníků	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=517885	1	1	1	1	2	1	0	1	1	Banka s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je zabezpečení
10.1.2008	12:51	Klienti České spořitelny opět dostali podvodné emaily	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=518260	1	1	1	1	2	1	2	1	1	Banka s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je zabezpečení
12.1.2008	15:25	Nový virus tajně krade hesla k účtům	http://aktualne.centrum.cz/ekonomika/svetova-ekonomika/clanek.phtml?id=518385	0	1	2	1	3	1	2	0	1	antivirové programy
4.3.2008	10:24	Na klienty České spořitelny opět útočí podvodníci	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=522950	1	1	1	1	2	1	2	0	1	banka s klienty nikdy prostřednictvím e-mailu nekomunikuje o tak zásadních záležitostech, jako je zabezpečení
4.3.2008	20:40	ČS vytáhne proti podvodným mailům. Povolá policii	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=523055	1	1	1	1	2	1	0	1	0	
5.3.2008	10:50	Na klienty České spořitelny znovu zaútočili podvodníci	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=523103	1	1	1	1	2	1	0	1	*1*	Banka přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a takové údaje od nich v žádném případě nevyžaduje
11.3.2008	11:01	Chodí vám podivné e-maily? Možná je to phishing	http://aktualne.centrum.cz/finance/prilohy/clanek.phtml?id=523663	1	1	1	0	2	1	0	0	1	banka přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a takové údaje od nich v žádném případě nevyžaduje
12.3.2008	12:45	Klienty České spořitelny si podvodníci oblíbili nejvíce	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=523799	1,2,5	1	1	1	2	1	2	1	1	Dbát bezpečnostních doporučení banky, nepřihlašovat se do služby z neznámých nebo veřejně dostupných počítačů, chránit své přihlašovací údaje, nestahovat do svých počítačů soubory z neznámých zdrojů a věnovat pozornost aktuálnímu antivirovému nastavení na svém

													počítači - to jsou základní pravidla, kterými by se měl klient banky řídit.
12.3.2008	15:55	Útoky na klienty České spořitelny neberou konce	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=523791	1	1	1	1	2	1	2	0	1	banka přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a takové údaje od nich v žádném případě nevyžaduje
17.3.2008	20:36	Phishing: Podvodné e-maily chodí i z adresy ČNB	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=524242	5	1	1	0	2	1	2	0	0	
26.3.2008	12:50	Podvodné maily útočí i na klienty Slovenské spořitelny	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=600703	1,6	1	1,2	1	2	1	0	0	1	banka přitom s klienty e-mailem nikdy o tak zásadních záležitostech, jako je například zabezpečení, nekomunikuje a takové údaje od nich v žádném případě nevyžaduje
29.3.2008	15:15	Viry útočí na bankovní konta, u klientů ČS uspěly	http://aktualne.centrum.cz/finance/penize-a-investice/clanek.phtml?id=600898	1	1	1	0	2	1	2	0	1	A zároveň doporučuje ihned jakoukoli činnost na stránce ukončit a odhlásit se z aplikace. Rozhodně je potřeba také kontaktovat banku a nahlásit jí problém.
31.1.2011	19:43	Hacker napadl 79 účtů České spořitelny, dostal 6 let	http://aktualne.centrum.cz/domaci/regiony/moravskoslezsky/clanek.phtml?id=689717	1	1	1	1	3	1	2	1	0	
15.11.2011	14:07	Další podvodný mail chce údaje k vašemu bankovnímu účtu	http://aktualne.centrum.cz/finance/penize/clanek.phtml?id=721647	5	1	1	1	2	1	0	0	1	správná URL, nekomunikace po mailu
20.8.2012	17:15	Nový podvod: Vir odesílá peníze z účtů ve spořitelně	http://aktualne.centrum.cz/finance/penize/clanek.phtml?id=754955	1	1	1	1	3	1	0	0	1	"Pečlivě kontrolujte obdržené SMS zprávy (účet příjemce, částku a měnu). Nikdy nezadávejte zaslaný kód z autorizační SMS na operaci v internetovém bankovnictví, kterou jste sami nezadali,"
6.3.2013	13:02	Hackerské útoky v Česku za posledních 5 let	http://aktualne.centrum.cz/domaci/grafika/2013/03/06/hackerske-utokyv-cesku-za-poslednich-5-let/	0	0	1	1	7	2	0	0	0	
6.3.2013	14:19	Hackeři znovu zaútočili,	http://aktualne.centrum.cz/domaci/zivot-v-	1,2	5	1	1	7	2	0	0	1	firewally apod., Je tak podle něj nutné,

		tentokrát padaly servery bank	cesku/clanek.phtml?id=773205	,3, 4,5									aby se ostatní weby z útoku poučily, sledovaly, jak probíhá, a připravily plán, jak při něm postupovat.
7.3.2013	20:03	Hackeři opět útočí. Pravděpodobně napadli i web ČT	http://aktualne.centrum.cz/domaci/zivot-v-cesku/clanek.phtml?id=773306	1,2 ,3, 4,5	5	1	1	7	2	0	0	0	
20.3.2013	14:22	Hackeři udeřili v Jižní Koreji, cílili na banky a média	http://aktualne.centrum.cz/zahranici/asie-a-pacifik/clanek.phtml?id=774649	6	5	2	1	1	3	0	0	0	
27.3.2013	21:42	Soul napadli hackeři. Zaútočil nepřítel ze severu?	http://aktualne.centrum.cz/zahranici/asie-a-pacifik/clanek.phtml?id=775157	6	5	2	1	1	3	0	0	0	

Příloha č. 3 - Podklady ke grafům

Tabulka 13 Množství informací o poškozených uživatelích (podklad k obrázku č. 7)

Počet poškozených uživatelů	Novinky.cz	iDnes.cz	iHNed.cz	Aktuálně.cz	Celkem	Celkem procent
0. neuvedeno	15	4	13	12	44	55%
1. 0	1	5	7	0	13	16%
2. 1 - 1000	1	7	1	8	17	21%
3. 1 001 - 10 000	0	0	0	0		
4. 10 001 - 50 000	1	0	2	0	3	4%
5. 50 001 - 100 000	0	1	1	0	2	3%
6. 100 001 - 300 000	0	0	0	0		
7. 300 001 - 500 000	0	0	0	0		
8. 500 000 - 750 000	0	0	0	0		
9. 750 001 - 1 000 000	0	0	0	0		
10. 1 000 001 a více	0	1	0	0	1	1%
celkem	**18**	**18**	**24**	**20**	80	100%

Tabulka 14 Množství informací o zcizených financích (podklad k obrázku č. 8)

Množství zcizených financí	Novinky.cz	iDnes.cz	iHNed.cz	Aktuálně.cz	Celkem	Celkem procent
0. neuvedeno	12	14	17	14	57	72%
1. 0	3	2	6	6	17	22%
2. 1 - 100 tis. Kč	0	2	0	0	2	2%
3. 100 tis kč - 500 000 kč	0	0	0	0		0%
4. 500 001 - 1 mil. kč	0	0	0	0		0%
5. 1 mil. - 5 mil. kč	0	0	0	0		0%
6. 5 mil. kč a více	3	0	0	0	3	4%
celkem	**18**	**18**	**23**	**20**	**79**	**100%**

Tabulka 15 Procentuální vyjádření četnosti útoku (podklad ke grafu č. 9)

Typ útoku	Počet proměnných	Počet proměnných (v procentech)
2. Phishing + pharming	42	53%
3. Malware	18	22%
7. DDoS	14	18%
1. Hacking	6	7%
0. Neuvedeno	0	
4. XSS, XSRF a clickjacking	0	
5. Útok ze středu	0	
6. Smíšená hrozba	0	
Celkem	**80**	100%

Tabulka 16 Zobrazení preventivních opatření (podklad ke grafu č. 10)

Prevence	ano	ne	ano u útoku	ne u útoku	ano (v procentech)	ne (v procentech)
iHNed.cz	13	10	2,2,2,2,2,2,2,2,2,2,3,3,3	1,1,,2,2,2,3,7,7,7,7,7	**62%**	**38%**
Novinky.cz	9	8	2,2,2,2,2,2,3,3,3,3	2,3,3,7,7,7,7,7		
Aktuálně.cz	13	7	2,2,2,2,2,2,2,2,2,2,3,3,7	1,1,2,2,3,7,7		
iDnes.cz	13	5	1,1,2,2,2,2,2,2,2,2,2,2,3	3,3,3,3,7		
celkem	**48**	**30**				
78			=	100%		

Tabulka 17 Rozložení mediálního obrazu prevence (podklad ke grafu č. 11)

Typ útoku	Prevence je popsána	Prevence není popsána	
DDoS	7%	93%	100%
hacking	66%	33%	100%
malware	56%	44%	100%
phishing a pharming	86%	14%	100%

Tabulka 18 Zobrazení prevence podle typu útoku (podklad ke grafu č. 12)

Typ útoku	Počet zobrazení	Počet zobrazení (v procentech)
Phishing a pharming	36	74%
Malware	10	20%
hacking	2	4%
DDoS	1	2%
	49	100%