MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC

Ústav informatiky

Jan Bivoj Kolář

Bezpečnostní aspekty internetového bankovnictví

Security aspects of Internet banking

Bakalářská práce

Vedoucí práce: Mgr. Květoslav Bártek

Olomouc 2009

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a použil jen uvedené informační zdroje.

Olomouc 19.3.2009

Na tomto místě bych rád poděkoval Mgr. Květoslavu Bártkovi za odborné vedení a vstřícný přístup v průběhu psaní této bakalářské práce. Mé díky patří také mé rodině a přítelkyni, za jejich nikdy nekončící podporu a lásku.

OBSAH

ÚVOD

Internet se stal běžnou součástí života mnoha z nás. Vyhledáváme informace, komunikujeme s přáteli, nakupujeme zboží a využíváme mnoha dalších služeb, které nám Internet nabízí. Při této činnosti si však málokdy uvědomíme, jaká bezpečnostní rizika nám hrozí.

Touto prací bych čtenáři rád poskytl komplexní pohled na bezpečnostní aspekty internetového bankovnictví. Mým cílem je koncipovat práci tak, aby předkládaná fakta byla snadno srozumitelná i pro člověka, který má jen minimální zkušenosti z oblasti počítačů. Běžný uživatel, ale i manager, tak získá všechny potřebné informace, aby byl schopen zvážit výhody a nevýhody internetového bankovnictví z bezpečnostního hlediska.

První kapitola bude věnována vymezení internetového bankovnictví z širší skupiny elektronického bankovnictví. Pokusím se zde nastínit historii i souvislosti vzniku internetového bankovnictví.

Jakým způsobem je uživatel chráněn při práci s internetovým bankovnictvím? Na tuto otázku by měla odpovědět druhá kapitola. Čtenáři v ní předložím souhrn všech bezpečnostních prvků, které jsou dnes v této oblasti využívány.

Ve třetí kapitole se budu věnovat bezpečnostním rizikům, která mohou uživateli hrozit. Každé riziko se pokusím podrobně popsat a navrhnout, jakým způsobem je možné uvedené riziko minimalizovat.

Navazující čtvrtá kapitola bude zaměřena na pokročilejší typy útoků, které často zneužívají některé z rizik, se kterými jsme se seznámili v předchozí kapitole. Hodlám se zaměřit nejen na starší (ale stále nebezpečné) útoky, ale také na nejnovější hrozby. Podobně jako u bezpečnostních rizik, předložím i zde návrhy na ochranu před daným útokem.

V závěrečné kapitole nalezne čtenář přehled aktuální nabídky internetového bankovnictví v ČR s důrazem na bezpečnostní aspekty. Součástí této kapitoly bude i srovnání nákladů za příplatkové služby v této oblasti. Díky tomu bude moci budoucí, ale i stávající uživatel internetového bankovnictví posoudit, zda se mu ekonomické náklady na vyšší zabezpečení jeho účtu vyplatí.

1 VÝVOJ ELEKTRONICKÉHO BANKOVNICTVÍ

V této kapitole objasníme vývoj elektronického bankovnictví, pojmy homebanking a internetové bankovnictví. Pokusíme se nastínit, proč internetové bankovnictví vzniklo, jeho historii a také jeho výhody oproti jiným druhům bankovnictví, ať už se jedná o bankovnictví klasické či bankovnictví elektronické.

1.1 Historie

Bankovnictví v klasickém pojetí má tisíciletou tradici. Již staří Řekové a Egypťané využívali principy, které si dnes spojíme s moderním bankovním ústavem. Jednalo se například o úschovu a směnu mincí, poskytování půjček a možnost vybrání peněz v jiném městě, než ve kterodně uloženy.[1]

Na rozdíl od klasického bankovnictví je elektronické bankovnictví relativně nový pojem. Vzniká s rozvojem osobních počítačů v osmdesátých letech minulého století. Zásadními milníky v elektronickém bankovnictví jsou homebanking a internetové bankovnictví. Oba pojmy spolu velmi úzce souvisí a dalo by se říci, že internetové bankovnictví v mnoha ohledech vychází z principu fungování homebankingu.[2]

1.2 Homebanking

Pojem homebanking je úzce spjat s rozvojem osobních počítačů ve firmách. Jednou z oblastí, která k nasazení počítačové techniky přímo vybízela, bylo vedení účetnictví. V té době však neexistoval jednotný ucelený systém, který by umožňoval předávání vložených údajů ostatním institucím, jako jsou obchodní partneři nebo

[1] Srov. *History of banking* [on-line], <http://en.wikipedia.org/wiki/History_of_banking>.

[2] V závislosti na způsobu rozdělení elektronického bankovnictví (dle komunikace, dle stáří, atd.) některá literatura uvádí pojem internetové bankovnictví na stejné úrovni jako pojem homebanking.

banky. Z tohoto důvodu bylo často nutné údaje několikrát ručně přepisovat, což bylo velmi zdlouhavé a vedlo k častějšímu výskytu chyb.

Banky se proto spolu se softwarovými společnostmi začaly zabývat myšlenkou propojení účetních systémů jednotlivých firem přímo se systémem banky. Mnoho bank začalo posléze tuto službu poskytovat pod názvem homebanking (nebo také PC bankovnictví).[3]

Aby mohl klient využívat služeb homebankingu, musí mít na svém PC nainstalován specializovaný software. Ten při komunikaci s bankou zajistí správný formát předávaných souborů, šifrování a autentizaci. Softwarové firmy nabízející účetní software často poskytují podporu pro homebanking přímo ve svých produktech. Tím odpadá nutnost přepisu údajů či potřeba ruční konverze dat z formátu účetního programu do formátu používaného bankou.

Výhodou, kterou homebanking přinesl, nebyla pouze možnost předávání již zadaných dat. Propojení s účetním systémem přineslo navíc možnost automatizace procesů. Moderní účetní systémy jsou díky údajům poskytnutými bankou schopny kontrolovat, zda došlo včas k zaplacení vystavených faktur. Dokáží také automaticky generovat platební příkazy na základě údajů vložených do systému.

Homebanking můžeme rozdělit dle několika kritérií:[4]

- **Způsob předávání dat**
  - **Pevná média** – zpočátku se pro předávání dat mezi systémy používala pevná média, obvykle diskety. Nevýhoda tohoto způsobu předávání dat je zjevná – člověk musel pravidelně navštěvovat pobočku banky, aby zde předal disketu s příkazy k platbám a vyzvedl si disketu s údaji o stavu účtu.
  - **BBS** – s rozvojem komunikačních technologií začínají banky nabízet možnost odeslání a příjmu dat pomocí BBS (Bulletin Board System). Klient musel kromě PC vlastnit také modem a telefonní přípojku. Spojení probíhalo tak, že se klient pomocí modemu připojil k serveru banky. Zde poté mohl získat soubory s informacemi o stavu svého účtu, nebo nahrát soubory s příkazy pro banku.

[3] Srov. PŘÁKA, M., a KALA, J., *Elektronické bankovnictví*, s. 61.

[4] Srov. tamtéž, s. 62-64.

- **Internet** – Internet přinesl zcela nové možnosti předávání dat. Tím hlavním je možnost získávání dat on-line (viz rozdělení dle Způsobu komunikace). Aplikace na PC připojeném k internetu může sama získávat aktualizovaná data, bez nutnosti zásahu člověka. Data jsou získávána přímo ze serveru banky po ověření identity klienta.

- **Způsob komunikace**
  - **Off-line režim** – data získaná od banky udávají stav našeho účtu s několikadenním zpožděním. To je způsobeno způsobem transportu dat, proto o tomto režimu hovoříme především v souvislosti s použitím pevných médií (disket) a BBS. Banka potřebovala nějaký čas na zpracování údajů a jejich přípravu k transportu (tvorba souborů, nahrávání na disketu), takže klient obvykle obdržel stav účtu z předchozího dne.
  - **Semi on-line režim** – data jsou aktualizována několikrát denně, např. každou hodinu. Tento režim se používá u některých homebankingových systémů při připojení pomocí BBS nebo Internetu. Klient tedy získá od banky data účtu k určitému času.
  - **On-line režim** – data jsou aktuální. Tento režim využívají jak některé homebankingové aplikace, tak internetové bankovnictví. Klient při dotazu obdrží aktuální stav svého účtu.

Je zjevné, že s postupným vývojem technologií se také měnily možnosti a způsoby užívání homebankingu. Moderní homebankingové aplikace jsou již úzce spjaty se sítí Internet a využívají všech předností on-line komunikace. Podobně je na tom i internetové bankovnictví.

1.3 Internetové bankovnictví

Jak je patrno z názvu, internetové bankovnictví by nikdy nemohlo vzniknout nebýt prudkého rozvoje Internetu koncem minulého století. Podobně jako je tomu u moderních homebankingových systémů, využívá i internetové bankovnictví

k přenosu dat on-line režim a jako přenosové médium síť Internet.[5] Jaký je tedy hlavní rozdíl mezi internetovým bankovnictvím a homebankingem?

Podstatou homebankingu je specializovaná aplikace (ať už účetní systém nebo speciální software od banky), kterou je nutné mít nainstalovanou na PC. Můžeme tedy říci, že homebanking je vázán na konkrétní počítač a jedná se tedy o neplnohodnotné internetové bankovnictví.

Naproti tomu je internetové bankovnictví realizováno pomocí webových technologií a je možné k němu přistupovat z kteréhokoliv počítače na světě. Stačí k tomu pouze, aby počítač byl připojen k Internetu a měl nainstalován webový prohlížeč. Internetové bankovnictví je tedy nezávislé na konkrétním počítači a jedná se o plnohodnotné internetové bankovnictví.[6]

Kromě výše uvedených rozdílů je také každá aplikace určena pro jinou část klientů banky. Homebanking je výrazně orientován na firemní klienty, jelikož poskytuje mnohem více možností pro spojení s účetními systémy. U firem může být navíc žádoucí vázanost homebankingu na jeden počítač (nebo několik málo počítačů). Naproti tomu je internetové bankovnictví spíše určeno pro drobné klienty, kteří nevyžadují propojení bankovnictví s účetnictvím. Webové rozhraní bývá obvykle jednodušší, umožňuje však plnohodnotnou správu bankovního účtu. Pro tyto klienty je pak nevázanost na konkrétní počítač nesporně výhodou, jelikož mohou ke svému účtu přistupovat odkudkoliv.

Velmi zajímavým řešením, obzvláště pro firemní klienty, je pak kombinace výše uvedených principů. Asistentka ve firmě zadá pomocí homebankingového (nebo účetního) programu příkazy k převodu peněz bankou. Ty však nejsou ihned vykonány, ale čekají na potvrzení finančního ředitele, který je může potvrdit pomocí internetového bankovnictví odkudkoliv na světě, například ze služební cesty.[7]

Za hlavní výhody internetového bankovnictví lze považovat tyto:

- **Dostupnost** – můžeme s účtem pracovat odkudkoliv na světě, 24 hodin, 7 dní v týdnu.

---

5 Srov. POLOUČEK, S., a kol., *Bankovnictví*, s. 178.

6 Srov. PŘÁKA, M., a KALA, J., *Elektronické bankovnictví*, s. 74.

7 Srov. tamtéž, s. 71.

- **Rychlost** – velmi snadno a rychle můžeme zadávat příkazy k převodům peněz i kontrolovat zůstatkový stav účtu.
- **Kontrola** – můžeme kontrolovat toky na našem účtu a okamžitě upozorňovat na nesrovnalosti. Zrakový vjem je navíc pro člověka lépe pochopitelný než vjem sluchový (např. z telefonického bankovnictví).
- **Úspora času** – většinu bankovních operací je možno vykonávat bez nutnosti navštívit pobočku banky.

1.4 Ostatní druhy elektronického bankovnictví

Různé druhy elektronického bankovnictví jsou spolu úzce spjaty a klient obvykle využívá služeb několika z nich. Velmi často také samotná banka kombinuje různé druhy elektronického bankovnictví do balíčků, které pak klientovi nabízí.

Nejčastěji bývá internetové bankovnictví kombinováno s bankovnictvím přes mobilní telefon (GSM Banking). Zde se využívá čtyř základních přístupů. Prvním z nich je ovládání pomocí krátkých textových zpráv (SMS), druhým specializovaná aplikace v SIM kartě telefonu (GSM Sim Toolkit), třetím přístup přes mobilní Internet (WAP) a čtvrtým je forma klasického hlasového hovoru (operátor banky, hlasový informační systém).[8]

Dalším druhem elektronického bankovnictví je použití klasické telefonní linky či faxu. Pomocí faxu můžeme např. posílat pokyny bance. V případě telefonu se obvykle jedná o komunikaci s živým operátorem banky a nebo ovládání účtu pomocí hlasového informačního systému.

Jako poslední druh elektronického bankovnictví můžeme uvést internetové stránky banky a e-mail. Klient sice přes tyto kanály nemůže přímo ovládat svůj účet, může je ale využít při získávání informací o cenách, službách, při vyřizování reklamací či komunikaci s bankou.

[8] Srov. MÁČE, M., *Platební styk: klasický a elektronický*, s. 171.

2 BEZPEČNOSTNÍ PRVKY

V této kapitole popíšeme jednotlivé bezpečnostní prvky, které jsou využívány v oblasti internetového bankovnictví. Tyto prvky rozdělíme dle oblasti jejich použití, zmíníme principy fungování a také slabé a silné stránky jejich nasazení. Znalost využívaných bezpečnostních prvků nám pomůže lépe pochopit hrozby související s internetovým bankovnictvím, které jsou předmětem další kapitoly.

2.1 Autentizace uživatele

Obecně lze autentizaci popsat jako proces, ve kterém systém ověřuje identitu uživatele.[9] K autentizaci nejčastěji dochází při přihlašování do systému internetového bankovnictví. Uživatel zadá určitý údaj, kterým se identifikuje (obvykle se jedná o uživatelské jméno) a údaj, kterým se ověřuje (obvykle se jedná o heslo). Systém dle zadaného identifikátoru nalezne uživatele ve své databázi. Po nalezení uživatele dojde k porovnání autentizačního údaje zadaného uživatelem a toho, který má systém uložen ve své databázi. Pokud se oba údaje shodují, je uživatel ověřen a může přistoupit ke svému účtu. Pokud se údaje neshodují, je uživatel požádán, aby data zadal znovu. Počet pokusů bývá omezen a po jeho překročení je účet dočasně zablokován.

2.1.1 Metody autentizace

Existuje několik přístupů k autentizaci, přičemž každý pro své fungování využívá jinou vlastnost uživatele. Za základní lze považovat tři přístupy založené na:[10]

- **něčem, co daný uživatel zná** – jedná se o nějakou tajnou informaci (heslo, PIN, přístupovou frázi). Výhodou tohoto přístupu je, že se dá informace snadno přenášet, jednoduše používat a nepotřebuje údržbu. Nevýhodou pak je, že lidská paměť si velmi špatně pamatuje složitá hesla – náhodný soubor

[9] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 11.

[10] Srov. tamtéž, s. 12.

znaků a číslic. Navíc lze informaci jednoduše zcizit (odposlech, záznam stisknutých kláves) a to bez vědomí uživatele.

- **něčem, co daný uživatel má** – jedná se o nějaký předmět (čipová karta, autentizační kalkulátor). Výhodou tohoto přístupu je bezpečnost, jelikož čipová karta může obsahovat digitální certifikáty nebo hesla mnohem složitější, než by si byl člověk schopen zapamatovat. Zařízení není možné jednoduchým způsobem okopírovat a také jeho ztrátu uživatel odhalí poměrně snadno. Nevýhodou pak je technická náročnost použití (např. k čipové kartě potřebujeme čtečku, tam, kde není, se nepřipojíme), potřeba údržby a možnost poruchy. Často se navíc jedná o proprietární zařízení, která nebývají navzájem kompatibilní.
- **něčem, co daný uživatel je** – jedná se o vlastnost (otisk prstu, oční sítnice). Všechny tyto vlastnosti, které umožňují identifikaci člověka, se souhrnně nazývají biometrické údaje. Hlavní výhodou je, že se zde nedá nic zapomenout ani ztratit. Také možnost krádeže je v tomto případě omezena. Nevýhodou je míra chybovosti, jelikož většina vlastností není absolutně stálá (hlas závisí na náladě, otisk prstu na způsobu položení na čtečku) a přístroje nejsou schopny měřit s absolutní přesností. Tím se zvyšuje počet chybně zamítnutých přístupů u oprávněných uživatelů (uživatel nerozpoznán) a počet chybně povolených přístupů u neoprávněných uživatelů (uživatel rozpoznán jako někdo jiný). Přístroje také zatím nejsou schopny rozeznat živou tkáň od neživé, tudíž je možné se po určitou dobu falešně identifikovat již mrtvou částí těla (např. amputovaný prst).

Posledně jmenovaný přístup se zatím v praxi internetového bankovnictví příliš nepoužívá. Hlavní doménou zůstává jeho nasazení uvnitř firem a institucí. S rozvojem moderní vědy však lze očekávat růst významu tohoto přístupu i v oblasti internetového bankovnictví.

Existují další dva přístupy, které kombinují výše uvedené metody. Jedná se o:

- **dvoufaktorovou autentizaci** – kombinuje dva přístupy, např. uživatel musí k ověření použít čipovou kartu (přístup „co daný uživatel má“) a poté je systémem požádán o přístupové heslo (přístup „co daný uživatel zná“).
- **třífaktorovou autentizaci –** kombinuje všechny tři výše uvedené přístupy.

2.1.2 Typy autentizačních údajů

Jak jsme již uvedli, existuje několik přístupů k autentizaci uživatelů a každý z nich využívá jiných autentizačních údajů pro ověření uživatelské identity. Každý typ má své silné i slabé stránky, které se nyní pokusíme popsat. Nejprve popíšeme typy, které se využívají při přístupu „něco, co daný uživatel zná“:[11]

- **Hesla –** jedná se o nejjednodušší a v současnosti nejvíce využívaný způsob autentizace. Typické heslo bývá řetězec dlouhý 6 – 10 znaků. Ideální heslo by mělo být netriviální, tzn. mělo by obsahovat různé druhy znaků (velká a malá písmena, číslice, pomlčku, mínus a další tisknutelné znaky), aby odolalo útokům hrubou silou a slovníkovým útokům.[12] Také by mělo být pro uživatele snadno zapamatovatelné, což většinou bývá v protikladu se složitostí. Pokud si uživatel může své heslo zvolit, tak moderní systémy obvykle kontrolují jeho složitost a uživatele upozorní, pokud jím vybrané heslo není dostatečně bezpečné (např. obsahuje málo znaků, jedná se o běžně používané slovo, řadu čísel, apod.)
- **Jednorázová hesla –** uživatel dostane od banky seznam jednorázových hesel. Každé z těchto hesel je možné použít pouze jednou. Tím se zvyšuje bezpečnost, protože odposlechnutá hesla není možné znovu použít pro další transakci. Tímto je však omezen uživatelský komfort, jelikož si uživatel musí svůj seznam hesel pravidelně aktualizovat. Obvykle tak učiní návštěvou pobočky banky, kde obdrží nový seznam hesel.
- **Osobní identifikační čísla (PIN[13])** – jedná se o číslo dlouhé 4 – 8 číslic. Výhodou bývá snazší zapamatovatelnost a také možnost omezení počtu chybně zadaných pokusů. Pokud uživatel zadá několikrát po sobě špatně svůj PIN, je jeho účet zablokován do doby, než provede jeho odblokování. K odblokování účtu může být požadován nějaký složitější kód (PUK[14]), hovor do zákaznického centra nebo osobní návštěva pobočky banky.

---

[11] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 32.

[12] Podrobně se těmto útokům věnujeme v kapitole 4.1 Útok na heslo uživatele.

[13] PIN – z anglického **P**ersonal **I**dentification **N**umber (osobní identifikační číslo).

[14] PUK – z anglického **P**ersonal **U**nblocking **C**ode (kód pro odblokování).

- **SMS jednorázové heslo** – banka zašle klientovi jednorázové heslo pro přihlášení pomocí SMS. Jelikož se tento typ využívá převážně u autorizací plateb, věnujeme se mu podrobněji v kapitole 2.2 Autorizace bankovních operací.

Následující typy autentizačních údajů jsou využívány u přístupu „něco, co daný uživatel má“:[15]

- **Osobní certifikát** – jedná se o dvojici šifrovacích klíčů – veřejný klíč a k němu příslušný privátní klíč. Banka využije své certifikační autority[16] a klientovi vygeneruje certifikát (což je digitálně podepsaný veřejný klíč). Díky tomu, že certifikát generuje samotná banka, může ho automaticky považovat za důvěryhodný. Uživatel si uloží vygenerovaný certifikát na přenosné datové médium (USB flash disk, disketa). Poté jej v kombinaci se soukromým klíčem využívá k elektronickému podpisu.[17] Tento certifikát má omezenou platnost a po této době musí uživatel navštívit pobočku banky, aby získal certifikát nový. Banka také poskytuje možnost bezpečnějšího uložení certifikátu do čipové karty (viz níže).
- **Čipové karty –** jedná se o kartu vyrobenou z pevné plastické hmoty obvykle o standardním rozměru 85,5 x 54 mm. Čipové karty mohou obsahovat buď statickou paměť, nebo přímo celý počítač dle upravené koncepce von Neumannova počítače. Prvně zmíněný druh byl využíván v minulosti (např. telefonní karty), v dnešní době převládá použití druhého druhu karet. Výhodou čipových karet je, že ve své zabezpečené paměti obsahují digitální certifikáty, které jsou mnohem bezpečnější než použití obyčejných hesel. Díky přítomnosti procesoru a pamětí mohou samy vykonávat různé operace (např. šifrování) a tím nedochází k předání tajných informací do dalšího zařízení. Můžeme je tedy využít i v nedůvěryhodném prostředí jako je počítač kolegy nebo internetová kavárna. Mezi nevýhody použití čipových karet patří nutnost použití čtečky a instalace potřebných ovladačů na počítač, který chceme pro přístup použít. Díky vyšší pořizovací ceně kompletu karty

[15] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 43.

[16] Certifikační autorita generuje a spravuje certifikáty (veřejné klíče) a ručí za identitu jejich držitelů.

[17] Podrobně se principu elektronického podpisu věnujeme v kapitole 2.3 Ochrana komunikačních kanálů.

a čtečky nabízejí banky možnost použití tohoto autentizačního prostředku za poplatek.[18] Čipové karty můžeme rozdělit na:

  - **Kontaktní** – karta má viditelné kontakty a musí být vložena do čtečky, která poté s kartou komunikuje a zajišťuje napájení.
  - **Bezkontaktní** – karta nemá viditelné kontakty, ale vestavěnou anténu. Komunikace probíhá na dálku bez přímého kontaktu se čtečkou. Ta také pomocí magnetického pole zajišťuje napájení karty.
  - **Kombinované** – karta obsahuje jak vestavěnou anténu, tak kontakty.

- **Autentizační kalkulátory –** jedná se o specializované zařízení, které je podobné kalkulačce – obsahuje displej a číselnou klávesnici. Princip fungování autentizačního kalkulátoru může být založen buď na sdíleném tajemství nebo na synchronizovaných hodinách.[19] Princip sdíleného tajemství spočívá v tom, že bankovní systém i kalkulátor v sobě mají uložen tajný údaj a ke komunikaci využívají symetrického šifrování. V tomto případě bankovní systém vyšle uživateli výzvu, kterou zadá do autentizačního kalkulátoru. Ten pomocí sdíleného tajemství vypočítá odpověď, kterou zobrazí na displeji. Tu uživatel zašle zpět do bankovního systému a tím je ověřen. Princip synchronizovaných hodin je založen na časovém otisku. Kalkulátor uživateli vypočítá kód pro daný okamžik (s malým rozpětím), kdy se uživatel snaží ověřit svoji identitu. Bankovní systém po obdržení žádosti vypočítá stejným způsobem kód pro daný okamžik a porovná jej s tím, který zaslal uživatel. Pokud se oba shodují, tak je uživatel ověřen. Kalkulátor bývá proti zneužití chráněn PIN kódem, který uživatel musí před každou operací zadat. Výhodou použití autentizačního kalkulátoru je tvorba jednorázových hesel, takže zde opět odpadá hrozba odposlechu. Nevýhodou pak je nekompatibilita různých zařízení a nutnost vytvoření specializované bezpečnostní infrastruktury. Banka i klient se tak stávají závislými na jednom dodavateli.

Jelikož se přístup „něco, co daný uživatel je“ zatím v praxi internetového bankovnictví příliš nevyužívá, zmíníme využívané typy údajů jen okrajově. Jedná se o:

[18] Srovnáním nákladů se blíže zabýváme v kapitole 5.3 Cenové srovnání příplatkových služeb.

[19] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 37.

- **Měření fyziologických vlastností –** např. otisk prstu, geometrie ruky, vzorek oční duhovky
- **Chování člověka** – např. dynamika podpisu, vzorek hlasu

2.2 Autorizace bankovních operací

Po úspěšném provedení autentizace uživatel získá přístup ke svému účtu. Jeho možnosti jsou však omezeny pouze na tzv. pasivní operace. Může sledovat stav svého účtu, historii plateb nebo kontrolovat různá nastavení. Naproti tomu aktivní operace jsou ty, které přímo manipulují s finančními prostředky na klientském účtu. Jedná se například o příkaz k úhradě, povolení inkasa nebo zaslání platby do zahraničí. Při použití některé z aktivních operací bývá uživatel požádán o její autorizaci. Autorizace platby může probíhat několika způsoby a liší se nejen způsobem provedení, ale také tím, kdy bývá ten který způsob vyžadován:[20]

- **SMS jednorázové heslo** – po zadání všech potřebných údajů a odeslání platebního příkazu je uživatel vyzván k zadání hesla pro ověření platby. Toto heslo však uživatel zatím nemá. Bankovní systém jej vygeneruje při příjmu platebního příkazu a odešle uživateli na jeho mobilní telefon formou SMS ve stejný čas, kdy zobrazí požadavek na zadání hesla na monitoru uživatele. Jelikož není možné přesně určit, za jak dlouho (a zda vůbec) uživatel SMS zprávu obdrží, je jeho platnost nastavena na omezenou dobu. Tento časový interval slouží oběma stranám – bance zajišťuje dostatek času k doručení SMS zprávy (síť může být přetížena) a uživateli zase kontrolu, zda se heslo neztratilo (pokud v daném intervalu nedorazí, vyžádá si nové). Použité heslo je jednorázové a bývá náhodně generováno. Výhodou použití tohoto přístupu je nenáročnost a mobilita – nepotřebujeme žádné speciální zařízení připojené k počítači. Nevýhodou pak je nutnost vlastnit mobilní telefon, mít ho u sebe při zadávání transakcí a také možnost krádeže. Jelikož se však jedná až o sekundární ověření, musel by útočník navíc znát naše přístupy k internetovému bankovnictví.

[20] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 131.

- **Jednorázové heslo** – banka poskytne klientovi seznam jednorázových hesel, které bude používat pro ověřování plateb. Jednorázová hesla jsme podrobně popsali v kapitole 2.1.2 Typy autentizačních údajů.
- **Telefonické potvrzení –** v určitých případech může banka požadovat autorizaci platby pomocí telefonního hovoru. Obvykle se jedná o převody většího objemu finančních prostředků. V tomto případě musí uživatel zavolat do zákaznického centra banky, kde bude spojen s operátorem. Pro tuto komunikaci má uživatel speciální heslo. Operátor požádá uživatele pouze o některé znaky z hesla, není tedy možné celé heslo odposlechnout z jednoho telefonického hovoru. Po ověření operátor platbu autorizuje.
- **Osobní certifikát** – i platbu, stejně jako uživatele, je možno autorizovat osobním certifikátem. Podrobněji jsme se o osobním certifikátu zmínili v kapitole 2.1.2 Typy autentizačních údajů.

Existují další ochranné prvky bankovních operací, které přímo nesouvisí s autorizací platby, jsou však významnými bezpečnostními opatřeními. Jedná se například o limity objemu finančních transakcí za určité období. Obvykle jde o denní, týdenní a měsíční limit nebo také limit na jednu transakci. Tato opatření brání odčerpání celého zůstatku na účtu jediným převodem, pokud jsou údaje k řízení účtu kompromitovány. Pokud uživatel potřebuje převést větší částku peněz, musí obvykle navštívit pobočku banky nebo využít více druhů autorizace.

Dalším prvkem je možnost, aby si uživatel nechal posílat informace o provedených platbách. Banky umožňují jak zasílání informačních SMS, tak informačních e-mailů. Pokud uživatel obdrží informaci o platbě, kterou neautorizoval, může zahájit potřebné kroky k jejímu zablokování. Nejvhodnější je v tomto případě banku ihned telefonicky kontaktovat a zažádat o stornování této platby.

2.3 Ochrana komunikačních kanálů

V předchozích kapitolách jsme objasnili, jaké metody se používají při autentizaci uživatelů i při autorizaci platebních operací. Účinnost i těch nejlepších metod by však byla silně omezena, kdybychom nebyli schopni pro data proudící mezi klientem

a bankou vytvořit bezpečnou a důvěryhodnou cestu. Samotný Internet rozhodně takovou cestou není, jelikož nemůžeme přesně určit, kudy naše data budou proudit a kdo k nim získá přístup. Abychom mohli data bezpečně přenášet, musíme vytvořit bezpečný komunikační kanál mezi bankou a klientem, který bude data chránit nejen proti neoprávněnému přečtení, ale také proti pozdějším úpravám při přenosu. Zároveň musí také zajišťovat autentizaci komunikujících stran.

Tento kanál si lze představit jako tunel, uvnitř kterého probíhá zabezpečená (šifrovaná) komunikace mezi klientem a bankou. Nikdo z vnějšího prostředí, kdo nezná patřičné klíče, nemá k této komunikaci přístup.

Při ochraně komunikačních kanálů se využívá metod symetrického a asymetrického šifrování. Princip jejich fungování nyní popíšeme:[21]

- **Symetrické šifrování** – u tohoto typu šifer se používá jednoho společného klíče jak k šifrování, tak k dešifrování. Obě komunikující strany tedy musí ještě před začátkem komunikace disponovat stejným tajemstvím (klíčem). Samotná komunikace poté probíhá tak, že odesílatel pomocí předem dohodnuté matematické funkce a klíče data zašifruje a příjemce je pomocí shodného klíče dešifruje. Hlavní výhodou této metody je velmi nízká výpočetní náročnost. Nevýhodou pak je nutnost pro obě strany vlastnit stejný klíč.
- **Asymetrické šifrování** – zde se pro šifrování a dešifrování využívá dvou rozdílných klíčů – soukromého a veřejného. Princip fungování asymetrického šifrován můžeme přirovnat k poštovní schránce – jakmile odesílatel vloží dopis do schránky, ztrácí k němu přístup a jediný, kdo si jej může přečíst je příjemce (majitel klíče od poštovní schránky). Roli poštovní schránky zde hrají dva šifrovací klíče – veřejný, který je určen pro šifrování, a soukromý, který je určen pro dešifrování. Díky použití speciálních matematických funkcí není možné data šifrovaná veřejným klíčem pomocí tohoto klíče opět dešifrovat. Z toho vyplývá, že obě komunikující strany nemusí před začátkem komunikace znát společné tajemství. Postačuje, pokud odesílatel získá od příjemce jeho veřejný klíč. Poté pomocí veřejného klíče data zašifruje a odešle příjemci. V této chvíli není ani sám odesílatel schopen tato data dešifrovat. Příjemce pro dešifrování využije svůj soukromý klíč a získá původní

[21] Srov. PŘÁKA, M., a KALA, J., *Elektronické bankovnictví*, s. 79-80.

data. Výhodou je, že veřejný klíč se může předávat i přes nezabezpečený kanál, jelikož slouží pouze k šifrování. K ověření toho, že veřejný klíč patří skutečně námi požadovánému příjemci, slouží tzv. certifikační autority.[22] Ty vydávají certifikáty (digitálně podepsané veřejné klíče) a zároveň ručí za identitu vlastníka. Nevýhodou asymetrického šifrování je velká výpočetní náročnost, která může být až stotisíckrát pomalejší než šifrování symetrické.

Při komunikaci mezi bankou a klientem se úspěšně využívá kombinace obou výše zmíněných metod, čímž se daří minimalizovat jejich negativní stránky. Celý princip spočívá v tom, že si obě strany pomocí asymetrického šifrování vymění náhodný klíč. Ten bude poté použit pro symetrické šifrování celé komunikace. Po skončení komunikace se náhodný klíč zahodí, takže jej již nebude možno použít pro další komunikaci.

Tento přístup tvoří základ protokolu SSL, který pracuje mezi vrstvou TCP/IP[23] a aplikační vrstvou. Pomocí zabezpečeného protokolu HTTPS[24] zprostředkovává šifrovanou komunikaci mezi webovým prohlížečem klienta a serverem internetového bankovnictví. Princip sestavení bezpečného komunikačního kanálu pomocí protokolu SSL:[25]

1. Klient zašle požadavek na zabezpečené spojení bance.
2. Banka zašle klientovi odpověď spolu se svým certifikátem, který obsahuje veřejný klíč.
3. Klient si ověří identitu držitele certifikátu pomocí certifikační autority, která certifikát podepsala.
4. Po ověření vygeneruje klient náhodný základ šifrovacího klíče. Tento klíč poté zašifruje pomocí veřejného klíče banky a odešle jej.
5. Banka pomocí soukromého klíče zprávu dešifruje a získá tak základ šifrovacího klíče. Ze základu vygeneruje jak banka, tak klient finální šifrovací klíč pro budoucí komunikaci.
6. Tímto je sestaven bezpečný komunikační kanál a veškerá komunikace je nyní šifrována symetricky pomocí dohodnutého klíče.

[22] Srov. *Autentizace uživatelů a autorizace elektronických transakcí*, s. 43.

[23] Více informací o protokolu TCP/IP je možno naleznout na http://cs.wikipedia.org/wiki/TCP/IP.

[24] Více informací o protokolu HTTPS je možno naleznout na http://cs.wikipedia.org/wiki/HTTPS.

[25] Srov. PŘÁKA, M., a KALA, J., *Elektronické bankovnictví*, s. 80.

Po sestavení komunikačního kanálu mohou již obě strany bezpečně komunikovat, aniž by hrozila kompromitace zasílaných údajů. Po skončení komunikace je bezpečný komunikační kanál rozbit a vygenerovaný šifrovací klíč zahozen.

Šifrování se využívá také při elektronickém podpisu.[26] Tímto podpisem potvrzuje odesílatel autentičnost odeslané zprávy. Zde se navíc do procesu šifrování přidávají tzv. hashovací funkce[27]. Tyto matematické funkce dokáží z obsahu sdělení vypočítat jedinečný kód, který se rapidně mění i při sebemenší změně v obsahu zprávy. Pomocí hashovacích funkcí lze tedy zaručit, že se zprávou nebylo manipulováno, aniž by musela být nutně šifrována (a tudíž nečitelná pro ostatní). Princip tvorby elektronicky podepsané zprávy je následující:[28]

1. Klient vytvoří zprávu a aplikuje na ni hashovací funkci.
2. Klient zašifruje výstup hashovací funkce pomocí svého soukromého klíče, čímž vznikne digitální podpis. Ten poté připojí ke zprávě a odešle do banky.
3. Banka přijme zprávu a dešifruje podpis pomocí veřejného klíče klienta. Tímto získá výsledek hashovací funkce, kterou jí klient zaslal.
4. Banka aplikuje hashovací funkci na původní zprávu (bez podpisu) a porovná výsledek s tím, který získala od klienta. Pokud se shodují, tak se zprávou nebylo manipulováno.

V tomto případě zná soukromý klíč pouze klient a tudíž on jediný mohl výstup hashovací funkce takto zašifrovat. Tím je zaručena autentizace odesílatele. Ze stejného důvodu nemohl nikdo jiný zašifrovaný výstup hashovací funkce změnit a tím je zaručena autentičnost zprávy.

---

[26] Elektronický podpis se může využívat pro autentizaci uživatele nebo autorizaci platby. Podrobněji jsme se tomuto využití věnovali v kapitolách 2.1.2 Typy autentizačních údajů a 2.2 Autorizace bankovních operací.

[27] Více informací o hashovacích funkcích je možno naleznout na http://cs.wikipedia.org/wiki/Hashovací_funkce.

[28] Srov. PŘÁKA, M., a KALA, J., *Elektronické bankovnictví*, s. 81.

3 BEZPEČNOSTNÍ RIZIKA

V předchozí kapitole jsme podrobně popsali bezpečnostní prvky, které se využívají v oboru internetového bankovnictví. Nyní tedy máme potřebný teoretický základ, který využijeme při hledání bezpečnostních rizik a možných způsobů obrany.

Jako první zmíníme základní bezpečnostní rizika, která mohou sloužit jako základ pro vedení sofistikovanějších typů útoků. Tyto pokročilé techniky popíšeme v následující kapitole. U každého bezpečnostního rizika se pokusíme navrhnout vhodná opatření, abychom šance na jeho zneužití minimalizovali.

3.1 Malware

Pojem „malware“ pochází ze spojení dvou anglických slov – „malicious“ (nebezpečný, škodlivý) a „software“ (programové vybavení počítače). Jedná se o společné označení pro škodlivé počítačové programy, jejichž účelem je průnik a případné poškození počítače bez vědomí jeho majitele.[29] Jelikož tento pojem zastřešuje mnoho různých druhů škodlivého software, tak pro účely této práce vymezíme pouze některé z nich:

- **Viry –** jsou malé počítačové programy, které mají za úkol ovlivnit chování počítače. Jejich základní vlastností je to, že se umí sami šířit a sami spouštět. Obojímu však musí předcházet prvotní akce uživatele – spuštění infikovaného souboru. Šíření obvykle probíhá tím, že virus napadne soubory jiných spustitelných programů v počítači. Pokud dojde ke spuštění takto infikovaného programu, tak se zároveň spustí i virus, který pokračuje ve svém šíření a ovlivňování chování počítače. Hlavní nebezpečí virů v oblasti internetového bankovnictví je, že po napadení počítače mohou potají nainstalovat další nebezpečný software – trojské koně nebo tzv. „keylogery“ (viz níže).
- **Červi –** jedná se o malé počítačové programy, podobné virům. Hlavním rozdílem mezi červem a virem je ve způsobu šíření. Viry ke svému šíření

[29] Srov. HARRIS, S., aj., *Manuál hackera*, s. 47-48.

potřebují soubory dalších spustitelných aplikací, které mohou infikovat. Červ naproti tomu ke svému šíření žádný infikovaný soubor nepotřebuje. Dokáže se automaticky replikovat a šířit na další počítače v síti (např. posílá sám sebe v příloze emailu na všechny adresy v adresáři). Červi také často pro své šíření využívají bezpečnostních chyb počítačových programů a operačních systémů. V tomto případě dochází k napadení počítače bez jakékoliv interakce uživatele. Stejně jako u virů, spočívá hlavní nebezpečí pro uživatele internetového bankovnictví především ve faktu, že po napadení počítače může červ nainstalovat další nebezpečný software ve formě trojského koně nebo „keylogeru“.

- **Rootkity –** jsou počítačové programy, které mají za úkol skrýt další nebezpečný software před zrakem uživatele a znemožnit (nebo co nejvíce ztížit) jeho odstranění z napadeného počítače.[30] Uživatel si tedy nemusí být vůbec vědom, že je jeho počítač napaden. Rootkity obvykle pracují pod administrátorským účtem a využívají mnoho různých technik k maskování. Dokáží skrýt své soubory i běžící procesy nebo se vydávat za legitimní součásti operačního systému. Obvykle také obsahují různé kontroly, zda rootkit a jím chráněná aplikace běží. Pokud se je uživatel pokusí ukončit, rootkit se postará o okamžité opětovné spuštění. Rootkity jsou využívány především trojskými koňmi, kde je žádoucí, aby uživatel nezpozoroval napadení svého počítače.
- **Trojské koně –** stejně jako trojský kůň v řecké mytologii, je i počítačový trojský kůň nástroj, který útočníkovi umožní nepozorovaně „obsadit“ počítač oběti. Napadený počítač poté může být útočníkem zcela ovládán. Útočník může pracovat se soubory a programy stejně, jako by fyzicky seděl u napadeného počítače. Navíc může sledovat veškerou činnost uživatele – ať už přímým sledováním pracovní plochy nebo ukládáním záznamů o stisknutých klávesách a spuštěných programech. Trojské koně se sami nešíří, ani nenapadají jiné počítačové programy. Jejich šíření obvykle zajišťují červy a viry, které po napadení počítače trojského koně stáhnou z předem zadané adresy a nainstalují. Útočníkovi pak už jen stačí se k trojskému koni vzdáleně

[30] Srov. *Rootkit.cz - Úvod* [online], <http://www.rootkit.cz/>.

připojit. Aby uživatel nezpozoroval napadení, využívají trojské koně rootkitů pro své maskování.

- **Keyloggery –** jedná se o specializované aplikace určené k záznamu stisknutých kláves. Slovo vzniklo spojením anglických výrazů „key“ (klávesa) a „logging“ (zaznamenávat). Záznamy se pak můžou ukládat lokálně na napadeném počítači nebo posílat na vzdálené úložiště – ať už na e-mailovou adresu nebo FTP[31] server. Útočník ze záznamů může posléze získat hesla, PINy, čísla kreditních karet a jiné citlivé údaje. Stejně jako trojské koně, ani keyloggery se samy nešíří a nenapadají jiné programy.

3.1.1 Ochrana před malware

První linií ochrany před malware je vždy prevence. Je potřeba si uvědomit nebezpečnost internetového obsahu, zvlášť pokud nepochází z nám dobře známých zdrojů. Malware se navíc nevyhýbá nikomu, takže nástrahy mohou čekat i v e-mailové zprávě od našeho přítele či na renomovaných internetových stránkách známého vydavatele. Je proto dobré sledovat souvislosti a k předkládaným faktům být nedůvěřivý. V případě e-mailové zprávy se může jednat o způsob formulací, zmínění přílohy v těle emailu, logická struktura a smysl celé zprávy. Viry totiž velmi často používají předem připravený text, který nemusí mít souvislost s předchozí komunikací. Na internetových stránkách, kde je nabízen obsah ke stažení, je dobré sledovat diskuze pod vystaveným souborem. Někdo před námi mohl již hrozbu objevit a v diskuzi na ni upozornit.

Často však ani naše obezřetnost nemusí vést k odhalení škodlivého software. Proto existují aplikace, které mohou pomoci nebezpečný software odhalit a ochránit tak náš počítač před nebezpečím. V boji proti malware se jedná převážně o:

- **Antiviry –** jsou bezpečnostní aplikace zaměřené na boj proti virům. Při své práci využívají několik metod na odhalení virové hrozby. Tou první je virová databáze, která obsahuje identifikátory již známých virů. Do této databáze jsou obvykle několikrát denně přidávány nově nalezené hrozby. Antivirový

[31] FTP je zkratka anglického File Transfer Protocol (protokol pro posílání souborů). FTP server poskytuje prostor, kam je možné vzdáleně umístit soubory a poté k nim přistupovat odkudkoliv z Internetu.

program si svoji databázi aktualizuje pomocí Internetu,[32] proto je důležité se alespoň jednou za určitý čas připojit a nechat antivirus provést aktualizaci této databáze. Druhou metodou určenou na odhalování zatím neznámých hrozeb je heuristická analýza. Ta aktivně prověřuje spustitelný soubor a kontroluje, zda neobsahuje podezřelé instrukce. Může tak pomoci nalézt zcela nový virus, který ve virové databázi zatím chybí. Použití heuristické analýzy však má i stinnou stránku, kdy může být za virus označena i legitimní aplikace. Antiviry také obsahují tzv. rezidentní ochranu. Ta pomocí obou výše zmíněných metod kontroluje soubory, se kterými uživatel (nebo operační systém) aktuálně pracuje, zda neobsahují virovou nákazu. Pokud dojde k nalezení virové hrozby, nabídne antivirus možné řešení – může se jednat o léčbu souboru, jeho uložení do karantény[33] či úplné smazání. Moderní antivirové programy dokáží odhalit kromě virů také ostatní nebezpečný software, jako jsou červi a trojské koně. Je třeba zdůraznit, že žádný antivirový software není stoprocentně úspěšný,[34] přesto jeho instalací získáme znatelně vyšší úroveň zabezpečení.

- **Firewally –** na rozdíl od antivirů nejsou firewally určeny pro ochranu souborů, ale ochraňují náš počítač před nechtěnou síťovou komunikací. Existují různá firewallová řešení – může se jednat o fyzické zařízení nebo specializovaný operační systém, v domácnostech se však nejčastěji setkáme s firewally personálními.[35] Ty se dají popsat jako aplikace, které se po instalaci usadí mezi ovladač síťové karty a ostatní programy. Díky tomu mohou aktivně monitorovat a pomocí různých pravidel také filtrovat veškerou komunikaci, která na síťové kartě probíhá. Základní firewall obsahují dnes téměř všechny operační systémy, ať se jedná o Windows XP po instalaci Service Pack 2, Windows Vista nebo moderní Linuxové distribuce. Tato řešení však poskytují pouze základní ochranu, a proto je vhodné je nahradit

[32] Srov. *Viry.cz – Prevence* [online], <http://www.viry.cz/go.php?p=viry&t=clanek&id=1>.

[33] Antivirová karanténa slouží k uložení infikovaného souboru mimo běžný souborový systém pro pozdější použití. To může být vhodné například tehdy, pokud zatím nejsou známy způsoby, jak soubor vyléčit.

[34] Úspěšnost antivirových programů lze porovnat například podle testů AV-Test – http://www.virusbtn.com/news/2008/09_02.

[35] Srov. *Viry.cz – Prevence* [online], <http://www.viry.cz/go.php?p=viry&t=clanek&id=1>.

plnohodnotným personálním firewallem. Ten poskytuje mnohem širší možnosti při řízení komunikace v obou směrech (z a do počítače) a také mnohem více informací o právě probíhající komunikaci. To nám může například pomoci odhalit napadení počítače červem, který se snaží rozesílat své kopie po síti – posíláním totiž vytváří podezřele velký síťový provoz z našeho počítače ven. Moderní firewally umožňují nejen provádění kontroly komunikace na portech[36] síťového rozhraní, ale také kontrolu jednotlivých aplikací, které k síťovému rozhraní přistupují. To usnadňuje orientaci pro začínající uživatele, kteří mohou jednoduše zakázat nebo omezit komunikaci aplikací, které neznají. Mnoho firewallů dnes také obsahuje seznam důvěryhodných programů (obvykle součástí operačního systému, atd.), u kterých uživateli doporučí, aby jejich komunikaci povolil.

- **Anti-malware aplikace –** jsou aplikace speciálně určené na boj proti malware. Fungují podobně jako antiviry na principu pravidelně aktualizovaných databází, pomocí nichž se snaží na počítači vyhledat podezřelé soubory a záznamy v registru.[37] Na rozdíl od antivirů se však soustřeďují i na méně nebezpečný malware jako jsou programy na zobrazování reklamních oken, programy shromažďující statistiku webových stránek navštívených uživatelem, programy na cílenou reklamu, atd. Při nalezení nebezpečného software jsou pak schopny zajistit jeho odstranění nebo poskytnout návod, jakým způsobem toto provést. Některé anti-malware aplikace obsahují také rezidentní ochranu, která sleduje a hlásí případné změny v registru či v důležitých systémových souborech. Uživatel pak může tyto změny potvrdit (např. instaluje nový program a ten registr upravuje), nebo zamítnout (pokud se změny dělají „z ničeho nic“).

[36] Síťové rozhraní obsahuje celkem 65535 portů, které mohou využívat jednotlivé aplikace pro svou komunikaci. Firewall pak zabezpečuje monitorování a filtraci komunikace na jednotlivých portech. Více informací o portech lze nalézt na adrese http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers [EN].

[37] Registr se využívá v systémech Windows a dá se zjednodušeně označit za databázi všech nastavení operačního systému. Také většina aplikací si své nastavení ukládá do registru. Přímá práce s registrem je určena pouze pro zkušené uživatele systému.

3.2 Chyby operačních systémů a aplikací

V dnešní době nenajdeme téměř žádnou aplikaci, u které by nebyla vydána alespoň jedna aktualizace z důvodu opravy chyby. Aktualizace jsou vydávány formou záplat[38] nebo vydáním novější verze programu. Kromě aplikací bývají pomocí záplat aktualizovány také operační systémy.

Chyby můžeme rozdělit do několika kategorií – např. chyby funkčnosti, chyby způsobující nestabilitu aplikace, atd. Pro uživatele internetového bankovnictví jsou však nejzásadnější chyby bezpečnostní. Díky nim může být počítač napaden červem či na něj může být nainstalován trojský kůň a to zcela bez vědomí a interakce uživatele. V některých případech může nastat až úplné převzetí kontroly útočníkem nad postiženým počítačem.

Bezpečnostní chyby se dnes týkají mnoha aplikací, pro uživatele internetového bankovnictví však mezi nejdůležitější patří **operační systém** a **webový prohlížeč**. Pro nejčastější zástupce obou skupin uvedeme v tab. 1 několik bezpečnostních statistik[39] za rok 2008. Tyto statistiky zveřejnila Secunia,[40] světově uznávaná společnost zabývající se bezpečnostními riziky aplikací.

Tab. 1: Statistika bezpečnostních článků společnosti Secunia za rok 2008

Operační systém	**Bezpečnostních článků**	**Zatím neopravených problémů**
Windows XP	33	9,00%
Windows Vista	20	19,00%
Ubuntu Linux 8.10	28	0,00%
Webový prohlížeč	**Bezpečnostních článků**	**Zatím neopravených problémů**
Internet Explorer 6	13	15,00%
Internet Explorer 7	11	18,00%
Firefox 3.x	8	0,00%
Opera 9.x	10	0,00%

Je třeba zdůraznit, že pomocí uvedených statistik nelze přímo porovnávat bezpečnost jednotlivých prohlížečů nebo operačních systémů. U webových prohlížečů

[38] Záplata (anglicky patch) je kus programového kódu, který je určen k opravě chyby v aplikaci.

[39] Jedná se o statistiky bezpečnostních oznámení, které byly zveřejněny na stránkách společnosti Secunia. Statistiky pro jednotlivé aplikace lze nalézt v databázi společnosti dle názvu aplikace – http://secunia.com/advisories/product/ [EN].

[40] Srov. *History of Secunia* [online], <http://secunia.com/corporate/information/>.

hraje například roli rozšířenost mezi uživateli nebo přístup ke zdrojovým kódům programu.[41] U operačních systémů může pak hrát roli stáří. S časem totiž ubývá počet bezpečnostních děr a rizik, proto jsou prověřené systémy obvykle bezpečnější než novinky na trhu. Kompletní validace tak rozsáhlého systému ještě před vydáním je totiž neproveditelná.

Z hlediska bezpečnosti nehraje počet nalezených bezpečnostních chyb v programu velkou roli. Nejdůležitější je totiž čas mezi nalezením bezpečnostní chyby a vydáním její opravy – tzn. jak dlouho je uživatel vystaven bezpečnostní hrozbě. Širší přehled je možné získat z dalších statistik na serveru www.secunia.com.

3.2.1 Ochrana před chybami operačních systémů a aplikací

Největší riziko u chyb toho druhu je, že jim uživatel nemůže nijak předcházet. Po nalezení bezpečnostní chyby navíc nemůže sám zjednat nápravu – je zcela závislý na tom, kdy a zda vůbec tvůrce aplikace vydá patřičnou aktualizaci. Naštěstí jsou si tvůrci aplikací problému vědomi, a tak se snaží uživateli co nejvíce usnadnit přístup k vydávaným záplatám a novým verzím programu. Většina moderních aplikací má proto vestavěnu funkci na kontrolu existence nové aktualizace a uživatele na tuto skutečnost upozorní.

O aktualizaci operačních systémů a webových prohlížečů uvedených v předchozí kapitole se starají tyto komponenty:

- **Windows update –** tato aplikace je integrována v operačních systémech Windows a slouží pro distribuci záplat operačních systémů a aplikací firmy Microsoft. Uživatel si může nastavit zcela automatickou správu aktualizací nebo může ručně zvolit, které aktualizace nainstalovat. Nastavení aktualizací v systému Windows XP se podrobně věnujeme v příloze 1. Příloha 2 pak poskytne rady pro uživatele systému Windows Vista.
- **Správce aktualizací –** je integrován do systému Ubuntu Linux a slouží ke stahování a instalaci bezpečnostních záplat nejen samotného systému, ale

[41] Jedná se o zápis počítačového programu v programovacím jazyku, díky kterému lze pochopit principy fungování aplikace. Tím je také snazší nalézt chyby v uvedeném programu. Více informací na adrese http://cs.wikipedia.org/wiki/Zdrojový_kód.

také nainstalovaných aplikací. Jedinou podmínkou je, že aplikace musí být instalovány z tzv. repozitáře.[42] Po instalaci je systém automaticky nastaven na každodenní kontrolu nových aktualizací, uživatel ale může tuto hodnotu změnit. Nastavení Správce aktualizací je popsáno v příloze 3.

- **Firefox a Opera –** mají zabudovanou vlastní kontrolu nových verzí programu. Pokud je nová verze nalezena, je uživateli nabídnuto automatické stažení a instalace aktualizace.

Situace je zde podobná jako u antivirů – i zde je vhodné se jednou za určitý čas připojit k Internetu a provést kontrolu, zda neexistují nové aktualizace aplikací nebo operačního systému. Aktualizace aplikací nemusí obsahovat pouze opravy, ale mohou přinést také zcela nové funkce. Uživatel, který pravidelně aktualizuje své aplikace, tak získá nejen bezpečnější systém, ale také přidanou hodnotu ve formě zvýšeného uživatelského komfortu.

3.3 JavaScript

JavaScript představuje jednu ze základních webových technologií, která poskytuje moderním webovým stránkám interaktivitu. Tvůrci webových stránek využívají JavaScriptu k tvorbě dynamických nabídek (menu), různých náhledů obrázků, při ověřování formulářů, apod.

Základním znakem JavaScriptu je jeho spouštění na straně uživatele. JavaScript je do webových stránek integrován pomocí tzv. skriptů. Skript je kousek programového kódu, který obsahuje instrukce pro jednotlivé akce. Ke spuštění skriptu dochází až po úplném stažení a zobrazení webové stránky. Poté již má JavaScript přístup ke všem prvkům stránky a může je aktivně měnit – to je případ již zmíněného menu. Pokud najedeme myší na objekt představující „rozbalovací“ menu, JavaScript změní obsah stránky tak, aby se nám zobrazila celá nabídka. Pokud z objektu sjedeme, JavaScript opět upraví obsah stránky a nabídka zmizí.[43]

[42] Více informací o způsobu instalace aplikací a jejich aktualizací pod systémem Ubuntu Linux je možné získat na této adrese http://wiki.ubuntu.cz/Instalace programů.

[43] Srov. LANCE, J., *Phishing bez záhad*, s. 114.

JavaScript může také aktivně odesílat různé informace. Toho se například využívá u formulářů, kde dochází k odeslání dat, aniž by se musela celá stránka znovu načíst ze serveru.

JavaScript však nemusí být využíván jen k dobrým účelům. O těch špatných se zmíníme u jednotlivých útoků popsaných v následující kapitole.

3.3.1 Ochrana před JavaScriptem

U JavaScriptu je věc obrany obtížnější z toho důvodu, že útočník zde nevyužívá chyby, ale vlastnosti tohoto programovacího jazyka. Jedinou možností obrany je tedy buď použití JavaScriptu zcela zakázat (což však povede k obrovskému snížení komfortu při prohlížení stránek), nebo jeho možnosti omezit. K tomu mohou dopomoci různé doplňky do webových prohlížečů. Podrobněji se o těchto doplňcích zmiňujeme v kapitolách 4.4.1 Ochrana před Cross-site Scripting (XSS), 4.5.1 Ochrana před Cross-site Request Forgery (CSRF) a 4.6.1 Ochrana před ClickJacking.

4 BEZPEČNOSTNÍ ÚTOKY

V této kapitole popíšeme několik sofistikovaných typů útoků, které mohou uživateli internetového bankovnictví hrozit. U každého útoku vyhodnotíme způsob provedení a navrhneme vhodná opatření, abychom šance útočníka snížili na minimum.

4.1 Útok na heslo uživatele

Tento typ útoku se používá nejen k získání přístupu do internetového bankovnictví, ale také na různé webové stránky s placeným obsahem. Princip útoku spočívá v tom, že se útočník snaží „uhodnout“ heslo, které uživatel používá ke své identifikaci. Směr útoku probíhá od útočníka přímo na webové stránky, takže uživatel ani jeho počítač není tímto útokem nijak zasažen.[44] Ke zjištění hesla může útočník použít dva rozdílné způsoby:

- **Útok hrubou silou** – útočník testuje postupně všechny možné varianty hesla – např. u třímístného hesla složeného z písmen útočník začíná testovat řetězcem „aaa“, poté „aab“, poté „aac“ až k „zzz“. V závislosti na délce hesla a volbě znaků, které heslo obsahuje, také závisí doba potřebná ke zjištění hesla. Logicky tento způsob útoku vede vždy ke zjištění hesla, může to však trvat i několik tisíc let.
- **Slovníkový útok** – útočník postupně testuje slova z předem připraveného seznamu (slovníku) na shodu s neznámým heslem. Jako zdroje slov zde můžou sloužit výkladové slovníky, technické slovníky, slovník spisovné češtiny, atd. Moderní aplikace navíc dokáží slova ze slovníků různě kombinovat a spojovat, čímž slovní zásobu ještě více rozšíří. Tento typ útoku využívá faktu, že lidé jako svoje hesla často volí již existující slova. Je mnohem rychlejší než útok hrubou silou, nemusí však nutně vést ke zjištění hesla.

[44] Srov. *Password Recorvery Methods* [online], <http://www.lastbit.com/password-recovery-methods.asp>.

Útok na heslo uživatele nemusí sloužit pouze k získání hesla. Je možné ho použít také jako tzv. DoS[45] útok. Využívá principu, že uživateli se po několika zadáních špatného hesla zablokuje přístup k jeho internetovému bankovnictví. Zmíněné využití však nebývá v praxi příliš časté, jelikož banky mohou omezit přístup pouze z útočníkovy IP[46] adresy a tím účel útoku zmařit.

4.1.1 Ochrana před útokem na heslo uživatele

V tomto případě není v uživatelově moci jakkoli útočníkovi ve vykonání útoku zabránit. Může však pomocí silného hesla úspěch útoku znemožnit. Silným heslem v této souvislosti rozumíme heslo, které by se mělo skládat minimálně z osmi znaků, mezi znaky by se měly vyskytovat velká a malá písmena, číslice, pomlčky či jiné tisknutelné znaky. Dále by se nemělo jednat o běžně používané slovo (ani pokud takové slovo doplníme číslicí). Sílu hesla si můžeme otestovat na Internetu, např. na http://www.microsoft.com/cze/athome/security/privacy/password_checker.mspx.[47]

4.2 Sociální inženýrství

Výraz sociální inženýrství neboli sociotechnika poprvé použil známý hacker Kevin Mitnick ve své knize s názvem Umění klamu. Pojem sociotechnika objasňuje v knize takto:[48] „Sociotechnika je ovlivňování a přesvědčovaní lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.“ Sociální inženýrství tedy využívá převážně poznatky z psychologie

[45] Denial of Service (nedostupnost služby) – snaží se pomocí různých technik zamezit legitimnímu uživateli přístup k požadované službě. Nejčastěji používanou technikou je přetížení služby obrovským množstvím dotazů.

[46] IP adresa udává jedinečnou adresu počítače v síti.

[47] Pro opravdu komplexní otestování hesla je možno použít The Password Meter, který využívá propracovanější algoritmus pro testování hesla – http://www.passwordmeter.com/ [EN].

[48] MITNICK, K., *Umění klamu*, s. 1.

a sociologie – obecnou důvěru lidí, snahu pomoci druhým, strach z možných problémů, atd. Technické znalosti jsou zde až druhořadé a slouží spíše k dotvoření obrazu předstírané osoby.

Základní myšlenkou sociotechniky je, že je zbytečné získávat heslo technickou cestou, když můžeme jednoduše přimět toho, kdo heslo zná, aby nám je řekl. Uvedeme si názorný příklad: Sociotechnik zavolá obchodníkovi nadnárodní společnosti a představí se jako pracovník IT oddělení. Pod záminkou kontroly od něj získá jeho uživatelské jméno, které mu obchodník rád sdělí, protože je přece chráněno heslem a to zná pouze on. Sociotechnik poté zavolá na IT oddělení dané společnosti, představí se jako zástupce obchodního oddělení a požádá o reset hesla u svého účtu. Jelikož pracovníkovi IT oddělení sdělí své (před chvílí zjištěné) uživatelské jméno, tak je mu reset hesla proveden a sděleno heslo nové. Pracovník IT oddělení totiž předpokládá, že uživatelské jméno zná pouze pracovník, kterému bylo přiděleno.

Při získávání informací využívá sociotechnik moderní komunikační technologie jako je telefon nebo e-mail, jelikož tyto odhalení podvodu ještě více znesnadňují. Pokud sociotechnikovi na informacích skutečně záleží, tak věnuje jistý čas budování vztahu důvěry s obětí (např. několik dní s obětí chatuje[49] na internetu). Ta je mu poté ochotna sdělit více informací, jelikož to již není „cizí člověk“.

Sociotechnik navíc nemusí požadovat pouze informace, může se také snažit nás přimět ke spuštění nebezpečného souboru či k jiné činnosti (např. vypnutí firewallu), která povede k získání kontroly nad naším počítačem. Jednoduchou záminkou může být například to, že nám posílá fotky z dovolené zabalené v samorozbalovacím archivu.[50] Tento archiv však může kromě fotek obsahovat také trojského koně, který se při dekomprimaci „tiše“ nainstaluje, aniž by to uživatel zpozoroval.

4.2.1 Ochrana před sociálním inženýrstvím

Jelikož sociální inženýrství není technickým rizikem, není nám v této oblasti schopna pomoci žádná aplikace. Podobně, jako jsme zmínili u ochrany před malware,

[49] Textová diskuze na internetu odehrávající se v reálném čase.

[50] Samorozbalovací archiv je spustitelný soubor, který v sobě obsahuje komprimovaná data a malý program, který je dokáže dekomprimovat. Na cílovém PC tedy nemusí být dekomprimační nástroj nainstalován.

je důležité sledovat souvislosti a být nedůvěřivý vůči předkládaným faktům. U výše uvedeného příkladu můžeme ověřit identitu volajícího tím, že zavoláme zpět – obchodník by v tomto případě nesměl sdělit uživatelské jméno, ale musel by zavolat zpět na číslo IT oddělení z interního telefonního seznamu společnosti. Tam by se posléze dozvěděl, že jeho uživatelské jméno nikdo nepožadoval a útok by byl zmařen.

Ve firemním prostředí je také možné využít interních firemních směrnic, kde je přesně uvedeno, jaké informace má kdo komu poskytovat, jakou cestou a za jakých okolností.

V domácím prostředí je pak vhodné být obezřetný na sdělování osobních údajů, příjem souborů, apod. Nikdy si totiž nemůžeme být jisti, kdo sedí na druhé straně a zda nehodlá získané informace zneužít proti nám.

4.3 Phishing

Výraz „phishing“ vychází z anglického slova „fishing“ (rybaření), jelikož technika útoku připomíná lov ryb. Předpona „ph“ pak značí anglické slovo „sophisticated“, jelikož útočníci využívají k lovení svých obětí velmi sofistikované metody.[51] Do češtiny bývá tento výraz překládán také jako „rhybaření“.

Pojem phishing se neustále vyvíjí stejně tak, jako se vyvíjí techniky tohoto útoku. Zjednodušeně by se dal princip útoku popsat takto – uživateli je zaslán podvodný e-mail vydávající se za legitimní organizaci, který ho pod nějakou záminkou žádá k vyzrazení citlivých informací. Ty má uživatel obvykle zadat na webových stránkách, jejichž odkaz je umístěn v e-mailu. Tyto falešné stránky pak perfektně kopírují design organizace, aby v uživateli vyvolaly ještě větší pocit důvěry.

Útočník ke zvýšení pravděpodobnosti „úlovku“ využívá mnoha triků – podvodné e-maily jsou rozesílány hromadně, v obsahu e-mailu jsou logické důvody pro zadání informací, falešné odkazy vzbuzují dojem pravých odkazů, atd. Útočník také často využívá poznatků ze sociálního inženýrství.

[51] Srov. LANCE, J., *Phishing bez záhad*, s. 22.

4.3.1 Ochrana před phishingem

Jak jsme již několikrát v této práci zmínili, nejdůležitější je prevence. Webové prohlížeče a e-mailoví klienti se sice snaží uživateli pomoci při odhalování phishingového útoku, jejich účinnost je však omezena. Ochrany totiž fungují na principu aktualizovaného seznamu nebezpečných adres. Aby tedy ochrana fungovala, musel adresu před námi již někdo navštívit a nahlásit ji jako nebezpečnou.

Znovu tedy zdůrazněme, že důležitá je nedůvěřivost k předkládaným faktům a snaha si tato fakta ověřit. Je vhodné se informovat na pobočce své banky, jaké informace mohou její pracovníci po klientovi požadovat. Většina bankovních ústavů totiž nikdy nevyžaduje citlivé údaje a zvláště ne přes nezabezpečené komunikační kanály jako je telefon nebo e-mail. Bohužel však existují i takové bankovní ústavy, které svým klientům rozesílají zprávy podobné těm phishingovým, a tím snižují jejich ostražitost vůči pravým útokům.

4.4 Cross-site scripting (XSS)

Základ útoku spočívá ve zneužití existující webové stránky, která není proti XSS dostatečně zabezpečena. Útočník do takovéto stránky propašuje svůj vlastní klientský skript (např. v jazyce JavaScript), který mu umožní získat důvěrná data uživatelů navštěvujících napadenou stránku. Existují tři typy útoku:[52]

1. **Typ 0** (založený na DOM[53]) – tento typ využívá chyby v samotném klientském skriptu. Ta vzniká, pokud si skript bere parametry přímo z URL adresy a tyto parametry nejsou před použitím ošetřeny. Útočník tak může skriptu předat upravený parametr, který mu umožní manipulaci se zobrazovanou stránkou.
2. **Typ 1** (netrvalý) – jedná se o nejčastější typ. Využívá chyby webové stránky, kdy jsou parametry zadané uživatelem bez ošetření použity pro vytvoření

[52] Srov. *Najpopulárnejšie útoky XSS a CSRF na výslní* [online], <http://blog.synopsi.com/2007-12-12/najpopularnejsie-utoky-xss-a-csrf-na-vyslni>.

[53] Document Object Model – objektový model, který představuje webovou stránku.

nové webové stránky. Například se může jednat o funkci vyhledávání, kterou webová stránka obsahuje. Stejně jako v předchozím příkladě předá útočník stránce upravený parametr (v tomto případě hledaný výraz), a tím ovlivní stránku s výsledky vyhledávání. Může tak do ní např. přidat vlastní skript či HTML kód. Hlavním znakem tohoto typu je, že musí být spuštěn z počítače oběti – tzn. oběť musí do vyhledávání zadat upravený parametr. Toho útočník obvykle dosahuje pomocí sociálního inženýrství.

3. **Typ 2** (trvalý) – tento typ umožňuje nejrozsáhlejší útoky. Opět využívá chyby webové stránky, kdy nejsou ošetřeny vstupy zadané uživatelem. Oproti předchozímu útoku jsou však tyto vstupy použity pro vytvoření trvalého obsahu stránky – např. diskuzní fóra, návštěvní knihy, apod. Útočník tedy pomocí upraveného parametru změní obsah stránky trvale, dokud jej ručně neodstraní majitel nebo správce napadené stránky. Ohrožený je tak každý návštěvník takto upravené stránky.

Tento typ útoku je hojně využíván v kombinaci s výše zmíněným phishingem. Útočník v tomto případě rozešle odkaz na existující, jím upravené stránky, a tím ztíží možnost rozpoznání podvodu. Navíc při útoku nemusí jít pouze o získání důvěrných informací. Upravená stránka může sloužit také k instalaci malware.

4.4.1 Ochrana před Cross-site Scripting (XSS)

Výše zmíněný útok spoléhá na spuštění nebezpečného skriptu na straně uživatele. Vhodnou obranou je tedy omezit spouštění uživatelských skriptů ve webovém prohlížeči. Uživatelé prohlížeče Firefox mohou využít doplňku NoScript,[54] který jim usnadní vypínání a zapínání jednotlivých skriptů na navštívených stránkách. Doplněk je stále aktivně vyvíjen dle aktuálních trendů, aby uživateli poskytl nejvyšší možnou úroveň ochrany. Instalací doplňku NoScript se zabýváme v příloze 4. Podobnou funkci poskytuje také doplněk do prohlížeče Opera s názvem BlockIt.[55]

[54] Více informací na http://noscript.net/.

[55] Více informací na http://my.opera.com/community/forums/topic.dml? Id=241208.

4.5 Cross-site Request Forgery (XSRF)

Tento útok zneužívá principu tzv. sezení (sessions). Pokud se uživatel přihlásí na webovou stránku, vytvoří se sezení, které si uloží jeho přihlašovací údaje do malého souboru na disku jeho počítače (do tzv. cookie). Tento soubor je poté využíván k ověřování identity uživatele po celou dobu sezení. Uživatel se tedy nemusí stále dokola přihlašovat při zobrazení každé jednotlivé stránky. Sezení má obvykle omezenou platnost, jejíž délka se může lišit – od několika minut až po týdny.

Útok probíhá následujícím způsobem – útočník si nejprve vytvoří svoji webovou stránku, do které zakomponuje odkaz na škodlivý skript (např. v jazyce JavaScript). Tento skript se po spuštění v uživatelově počítači pokusí zaslat požadavek (např. na bankovní převod, na změnu hesla) na jinou legitimní stránku. Při tomto pokusu využije skript výše zmíněných přihlašovacích údajů uložených v cookie.[56] Tento postup však může fungovat pouze za předem určených podmínek:

- Uživatel před navštívením útočníkovy stránky navštívil také legitimní stránku.
- Uživatel má na legitimní stránce aktivní sezení (tzn. má uloženy údaje v cookie).
- Útočník musí předem znát veškeré vstupy, které legitimní stránka požaduje pro vykonání požadavku.
- Útočník musí předem znát hodnoty vstupů. Pokud stránka pro provedení požadavku požaduje např. heslo, tak je útok neproveditelný.

Útočník tento útok provádí v podstatě „naslepo“. Nemůže si být jist, zda uživatel výše zmíněné body splňuje, ani nemůže vidět, jakou odpověď legitimní stránka uživateli poslala. Tyto pro útočníka nevýhodné aspekty však lze potlačit kombinací tohoto útoku s útokem Cross-site scripting.

[56] Srov. LANCE, J., *Phishing bez záhad*, s. 201.

4.5.1 Ochrana před Cross-site Request Forgery (CSRF)

Uživatel může pro svoji obranu, podobně jako u útoku XSS, omezit spouštění klientských scritpů ve webovém prohlížeči. K tomu mohou opět dopomoci zmíněné doplňky NoScript pro webový prohlížeč Firefox a BlockIt pro webový prohlížeč Opera.

Jelikož tento útok počítá s aktivním sezením uživatele k legitimní stránce, je dobré při práci se zabezpečenými webovými stránkami dodržovat několik pravidel:

- Přihlašovat se pouze na dobu nezbytně nutnou k vykonání potřebných operací. Poté se ihned odhlásit.
- V průběhu práce na zabezpečené stránce neprohlížet jiné stránky na Internetu.
- Po odhlášení zcela zavřít okno webového prohlížeče, a tím zajistit smazání cookie.

4.6 ClickJacking

Jedná se o poměrně novou formu útoku, kterou v září 2008 poprvé představili pánové Jeremiah Grossman a Robert Hansen.[57] Název útoku by se dal přeložit jako „ukradené kliknutí“, což přesně vystihuje princip, jakým je útok prováděn. Vše je založeno na překrytí určitého prvku (např. tlačítka) jiným prvkem. Uživatel tedy na tento nový prvek klikne, jelikož od něj očekává akci původního tlačítka.

Překrytí může být vytvořeno pomocí několika oken prohlížeče, nebo vložením průhledného rámu do stávajícího okna. Tento rám poté může zobrazovat pouze ten prvek, který má být nahrazen. Uživatel tedy vůbec nezpozoruje, že kliká na jiné tlačítko.

Tento útok postihuje veškeré webové prohlížeče i značnou část webových aplikací. Jako praktická ukázka útoku sloužil při jeho představování příklad, kdy

[57] Srov. *SecTheory – Clickjacking* [online], <http://www.sectheory.com/clickjacking.htm>.

uživatel klikáním na tlačítka webové stránky nevědomky povolil přístup ke své webové kameře a mikrofonu v aplikaci Flash 9.[58]

4.6.1 Ochrana před ClickJacking

Jelikož se jedná o poměrně novou bezpečnostní hrozbu, neexistuje zatím jednoznačná obrana proti tomuto útoku. K dispozici je několik nástrojů, které mohou pomoci majitelům webových stránek tomuto útoku zabránit. Tvůrci aplikací postupně vydávají aktualizace, které brání zneužití tímto útokem (např. v době psaní je již k dispozici Flash 10).

Obranu na uživatelské úrovni zajišťuje již zmíněný doplňek NoScript (od verze 1.8.2). Ten obsahuje funkci ClearClick, která uživatele chrání před tímto typem útoku, a to dokonce i tehdy, pokud uživatel nepoužívá doplněk k řízení klientských scriptů. Tato funkce pracuje na jednoduchém principu – pokud uživatel klikne na objekt nebo rám, je pořízen „obrázek“ aktuální stránky, přičemž jsou všechny objekty a rámy zbaveny průhlednosti. Tento obrázek je poté porovnán s původní stránkou a pokud je nalezen rozdíl, zobrazí se varovné hlášení. Uživateli je pak zobrazena stránka zbavená průhlednosti, aby mohl posoudit, zda skutečně chtěl kliknout na daný objekt.

Uživatelé ostatních prohlížečů mohou útoku zabránit pouze vypnutím určitých prvků stránek, což však omezuje uživatelský komfort při jejich prohlížení. Zlepšení situace by měla přinést osmá verze prohlížeče Internet Explorer.

4.7 Sniffing, Spoofing, Man-in-the-middle

Všechny tři zmíněné útoky jsou zaměřeny na komunikaci uživatele a to je také důvod, proč jsme je spojili do jedné skupiny. Od předchozích útoků se liší také cíleností. Dříve zmíněné útoky jsou spíše necílené – snaží se útočit na velké množství uživatelů a počítají s tím, „že se někdo chytí“. Tento přístup však u útoků jako je

[58] Názorné video útoku je možné shlédnout na adrese http://vimeo.com/3462600.

sniffing nebo spoofing neplatí, jelikož si útočník musí svoji oběť předem vybrat. Základní principy zmíněných útoků jsou tyto:[59]

- **Sniffing** – by se dal přirovnat k odposlechu. Útočník odposlouchává komunikaci uživatele při cestě po komunikačním kanálu. Získává tak informace zcela bez interakce s počítačem oběti.
- **Spoofing** – útočník vytváří falešnou komunikaci, a tím se vydává za svoji oběť. Snaží se tak přesvědčit protější komunikační stranu, že komunikuje s původním uživatelem.
- **Man-in-the-middle –** útočník využívá obou výše zmíněných útoků. Odposlouchává komunikaci mezi dvěma komunikujícími stranami. Části této komunikace posléze blokuje a nahrazuje komunikací vlastní. Obě strany tak mají pocit, že komunikují pouze mezi sebou, přestože obě dostávají podvržená data od útočníka.

4.7.1 Ochrana před Sniffing, Spoofing a Man-in-the-middle

Základní ochranou proti těmto útokům je zajištění bezpečného komunikačního kanálu. Toho lze docílit pomocí nástrojů, které jsme zmínili v kapitole 2.3 Ochrana komunikačních kanálů. Důležité tedy je přistupovat na stránky internetového bankovnictví pomocí zabezpečeného protokolu HTTPS a také si vždy ověřit předkládaný certifikát stránky.

Spoofing mohou také odhalit moderní firewally. Ty kontrolují tok komunikace a pokud zaznamenají nějaké změny v adrese odesílatele, tak na ně okamžitě upozorní. Obdobným způsobem chrání firewall také před útokem typu man-in-the-middle.

[59] Srov. *Man-in-the-middle attack* [online], <http://en.wikipedia.org/wiki/Man-in-the-middle_attack>.

5 NABÍDKA INTERNETOVÉHO BANKOVNICTVÍ V ČR

V této kapitole popíšeme aktuální nabídku v oblasti internetového bankovnictví pěti největších bankovních ústavů v ČR. Uvedeme základní charakteristiky jednotlivých produktů a provedeme srovnání přístupů k autentizaci uživatele a autorizaci plateb.

V další části této kapitoly se zaměříme na možnosti zvýšení bezpečnosti internetového bankovnictví využitím příplatkových služeb. Porovnáme aktuální nabídku jednotlivých bank a to včetně srovnání finančních nákladů.

5.1 Přehled služeb

Služby internetového bankovnictví jsou v ČR poskytovány na vysoké úrovni a z tohoto důvodu najdeme velkou část funkcí ve všech nabízených produktech. Jedná se např. o kontroly stavu účtu, výpisy transakcí, podávání příkazů k úhradě (jednorázových, trvalých, hromadných), dobíjení předplacených karet mobilních operátorů, správa SIPO (zřízení, změna, zrušení), atd. Proto v následujícím přehledu uvedeme pouze vlastnosti, které jsou pro jednotlivé služby charakteristické:

- **SERVIS 24 Internetbanking (Česká spořitelna)**[60]
  - možnost nastavení změn Osobního účtu České spořitelny
  - možnost sjednání předschváleného spotřebitelském úvěru nebo kontokorentního úvěru
  - e-faktury – možnost aktivovat a přijímat elektronické faktury
- **InternetBanking 24 (ČSOB)**[61]
  - možnost změny adresních údajů ke službě

[60] Srov. *Česká spořitelna - Servis 24 Internetbanking* [online], <http://www.csas.cz/banka/content/inet/cs/PRODUCT_DESCRIPTION_CS_PI01_005000.XML?category=57>.

[61] Srov. *ČSOB – ČSOB InternetBanking 24*, [online], <http://www.csob.cz/bankcz/cz/Lide/Elektronicke-bankovnictvi/CSOB-InternetBanking-24.htm>.

- možnost vlastního pojmenování účtů
- vytváření přehledu bankovních spojení partnerů platebního styku

- **Max Internetbanking PS (Poštovní spořitelna)**[62]
  - možnost změny adresních údajů ke službě
  - možnost vlastního pojmenování účtů
  - vytváření přehledu bankovních spojení partnerů platebního styku
- **Mojebanka (Komerční banka)**[63]
  - elektronické výpisy k účtům a platebním kartám
  - on-line investice do podílových fondů
  - on-line objednávka dalších služeb
  - služba je dostupná rovněž v anglickém jazyce
- **Internet Banka (GE Money Bank)**[64]
  - možnost zakládat spořící a revolvingové účty, bez nutnosti navštívit pobočku
  - služba GE Money Manager – je soubor několika nástrojů, které umožní sledovat příjmy a výdaje roztříděné dle kategorií a také plánování budoucích úspor

5.2 Srovnání možností autorizace a autentizace

Nyní již známe hlavní charakteristiky jednotlivých produktů a můžeme se zaměřit na jejich srovnání z pohledu bezpečnosti. Každá z bank využívá při autorizaci a autentizaci jiného z přístupů, které jsme uvedli v kapitolách 2.1 Autentizace uživatele a 2.2 Autorizace bankovních operací. Některé banky dávají dokonce uživateli na výběr z několika způsobů autorizace a autentizace. Ten si tak může zvolit ty nejvhodnější. Možnosti jednotlivých produktů jsme porovnali v tab. 2. na str. 43.

[62] Srov. *Poštovní spořitelna – Max Internetbanking PS* [online], <http://www.postovnisporitelna.cz/Obcane/ucty-a-platby/elektronicke-bankovnictvi/Stranky/max-internetbanking-ps.aspx>.

[63] Srov. *Komerční banka – Mojebanka* [online], <http://www.kb.cz/cs/seg/seg1/products/mojebanka.shtml>.

[64] Srov. *GE Money CZ – Přímé bankovnictví – Internet Banka* [online], <http://www.gemoney.cz/ge/cz/1/ucty/internet-banka>.

Tab. 2: Srovnání autorizace uživatele a autentizace platby

Název produktu	Autentizace uživatele	Autorizace platby	Šifrování SSL
SERVIS 24 Internetbanking	klientské číslo a heslo; autentizační kalkulátor; klientský certifikát	SMS kód	128 bit
InternetBanking 24	identifikační číslo a PIN; identifikační číslo, PIN a SMS klíč; certifikát k elektronickému podpisu (na čipové kartě)	elektronický podpis; SMS klíč	128 bit
Max Internetbanking PS	identifikační číslo a PIN; identifikační číslo, PIN a autorizační kód; identifikační číslo a autorizační kód	SMS klíč	128 bit
Mojebanka	osobní certifikát a heslo	autorizační SMS kód a heslo	128 bit
Internet Banka	identifikační číslo a heslo; identifikační číslo a mobilní klíč; identifikační číslo, heslo a digitální certifikát	mobilní klíč; digitální podpis	128 bit

5.3 Cenové srovnání příplatkových služeb

Banky nabízejí některé ze zmíněných metod autorizace či autentizace pouze jako příplatkovou službu. Tento přístup však může vést k tomu, že uživatelé budou méně využívat pokročilejších způsobů zabezpečení. Nevýhodou uživatele v tomto případě je, že dle většiny smluvních ujednání ručí za škody způsobené kompromitací údajů k internetovému bankovnictví právě on.

V tab. 3 najdeme přehled příplatkových nákladů při použití autorizace (autentizace) pomocí osobního certifikátu. Jedinou bankou, která tento způsob ověřování pro své internetové bankovnictví neposkytuje, je Poštovní spořitelna.

Tab. 3: Srovnání příplatkových služeb k 22.03.2009.

Název banky	Čtečka čipových karet	Čipová karta	Vygenerování osobního certifikátu	Obnova osobního certifikátu (ročně)
Česká spořitelna	350 Kč	320 Kč	320 Kč	320 Kč / 420 Kč[1]
ČSOB	500 Kč / 2000 Kč[2]	neuvedeno	300 Kč	300 Kč / 100 Kč / 300 Kč[3]
Poštovní spořitelna	---	---	---	---
Komerční banka	298,00 Kč	390,00 Kč	zdarma	zdarma
GE Money Bank	neuvedeno	neuvedeno	neuvedeno	neuvedeno

1) v termínu / po termínu; 2) USB / PCMCIA verze ; 3) na pobočce / pomocí internetového bankovnictví / mimořádná obnova

ZÁVĚR

Cílem této práce bylo čtenáři ozřejmit bezpečnostní aspekty internetového bankovnictví. Na úvod této problematiky jsme se seznámili s historií a zařazením internetového bankovnictví v rodině elektronického bankovnictví. Poté jsme se již plně věnovali bezpečnostním aspektům internetového bankovnictví, ať už se jednalo o používané bezpečnostní prvky či aktuální bezpečnostní hrozby.

Z hrozeb jsme nejdříve popsali bezpečnostní rizika, které mohou uživateli internetového bankovnictví hrozit. Na ně jsme navázali bezpečnostními útoky, které velmi často zmíněná rizika zneužívají. U každé nalezené hrozby jsme uvedli možný způsob ochrany. Na závěr této bakalářské práce jsme uvedli přehled aktuálně nabízených služeb internetového bankovnictví na českém trhu, přičemž jsme se zaměřili hlavně na způsob jejich zabezpečení.

V této bakalářské práci jsem se snažil uvést a utřídit všechna podstatná fakta tak, aby byl čtenář schopen kvalifikovaně porovnat jednotlivé nabízené služby. Běžný uživatel, stejně tak jako vedoucí manager společnosti, mohou jasně zvolit to nejvhodnější internetové bankovnictví spolu s bezpečnostními prvky, které vyhovují právě jim.

Tato práce také přináší čtenáři bezpečnostní informace a principy, díky kterým je schopen využívat své internetové bankovnictví zodpovědně a bezpečně. V podnikové sféře může navíc tato práce sloužit jako podklad pro vznik interních směrnic, které jasně udávají způsob práce s internetovým bankovnictvím v podniku.

Domnívám se, že jsem touto bakalářskou prací připravil prostor i pro další studenty, kteří ji mohou v budoucnu využít pro srovnání aktuálně využívaných bezpečnostních prvků a také pro sledování vývoje bezpečnostních hrozeb v oblasti internetového bankovnictví.

ANOTACE

Příjmení a jméno autora:	Jan Bivoj Kolář
Instituce:	Moravská vysoká škola Olomouc, o.p.s.
Název práce v českém jazyce:	Bezpečnostní aspekty internetového bankovnictví
Název práce v anglickém jazyce:	Security aspects of Internet banking
Vedoucí práce:	Mgr. Květoslav Bártek
Počet stran:	59
Počet příloh:	4
Rok obhajoby:	2009

Klíčová slova v českém jazyce: bezpečnost, internetové bankovnictví, elektronické bankovnictví, bezpečnostní hrozby, ochrana

Klíčová slova v anglickém jazyce: security, internetbanking, electronic banking, security threats, protection

Cílem této bakalářské práce je poskytnout běžným uživatelům i managerům komplexní přehled o bezpečnostních aspektech internetového bankovnictví na českém trhu. Práce se na počátku věnuje objasnění pojmu internetového bankovnictví a jeho historii. Poté je čtenář seznámen s aktuálně využívanými bezpečnostními prvky. Hlavní část práce je věnována bezpečnostním hrozbám a návrhům protiopatření, která může uživatel na své straně podniknout. Poslední část práce přináší přehled aktuální nabídky internetového bankovnictví v ČR se zaměřením na bezpečnost.

The objective of the present thesis is to provide regular users and managers with a complex overview of security-related aspects of the internet banking available in the Czech market. In its opening section, the thesis clarifies the concept of internet banking and its history. Subsequently, it presents to the reader a list of currently used security tools. The core of the thesis is devoted to the threats and possible preventive and

protective measures that the user may adopt. The final part gives an overview of the currently offered internet banking services within the Czech Republic, with special focus on safety and security.

LITERATURA A PRAMENY

Autentizace uživatelů a autorizace elektronických transakcí. Praha: Tate international, 2007. 318 s. ISBN 978-80-86813-14-1.

Česká spořitelna – Servis 24 Internetbanking [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.csas.cz/banka/content/inet/cs/PRODUCT_ DESCRIPTION_CS_PI01_005000.XML?category=57>.

ČSOB – ČSOB InternetBanking 24 [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.csob.cz/bankcz/cz/Lide/Elektronicke-bankovnictvi/ CSOB-InternetBanking-24.htm>.

GE Money CZ – Přímé bankovnictví – Internet Banka [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.gemoney.cz/ge/cz/1/ucty/internet-banka>.

HARRIS, Shon, aj. *Manuál hackera.* 1. vyd. Praha: Grada, 2008. 399 s. ISBN 978-80-247-1346-5.

History of banking [online]. [cit. 16. března 2009]. Dostupné na WWW: <*http://en.wikipedia.org/wiki/History_of_banking*>.

History of Secunia [online]. [cit. 25. března 2009]. Dostupné na WWW: <http://secunia.com/corporate/information/>.

Komerční banka – Mojebanka [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.kb.cz/cs/seg/seg1/products/mojebanka.shtml>.

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

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

Man-in-the-middle attack [online]. [cit. 7. dubna 2009]. Dostupné na WWW: <*http://en.wikipedia.org/wiki/Man-in-the-middle_attack*>.

MITNICK, Kevin. *Umění klamu.* 1.vyd. Gliwice: HELION, 2003. 348 s. ISBN 83-7361-210-6.

Najpopulárnejšie útoky XSS a CSRF na výslní [online]. [cit. 22. března 2009]. Dostupné na WWW: <http://blog.synopsi.com/2007-12-12/najpopularnejsie-utoky-xss-a-csrf-na-vyslni>.

Password Recorvery Methods [online]. [cit. 21. března 2009]. Dostupné na WWW: <http://www.lastbit.com/password-recovery-methods.asp>.

POLOUČEK, Stanislav, a kol. *Bankovnictví.* 1. vyd. Praha: C. H. Beck, 2006. 716 s. ISBN 80-7179-462-7.

Poštovní spořitelna – Max Internetbanking PS [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.postovnisporitelna.cz/Obcane/ucty-a-platby/elektronicke-bankovnictvi/Stranky/max-internetbanking-ps.aspx>.

PŘÁKA, Michal, a KALA, Jan. *Elektronické bankovnictví.* 1. vyd. Praha: Computer press, 2000. 166 s. ISBN 80-7226-328-5.

Rootkit.cz – Úvod [online]. [cit. 24. března 2009]. Dostupné na WWW: <http://www.rootkit.cz/>.

SecTheory – Clickjacking [online]. [cit. 18. března 2009]. Dostupné na WWW: <http://www.sectheory.com/clickjacking.htm>.

Viry.cz – Prevence [online]. [cit. 17. března 2009]. Dostupné na WWW: <http://www.viry.cz/go.php?p=viry&t=clanek&id=1>.

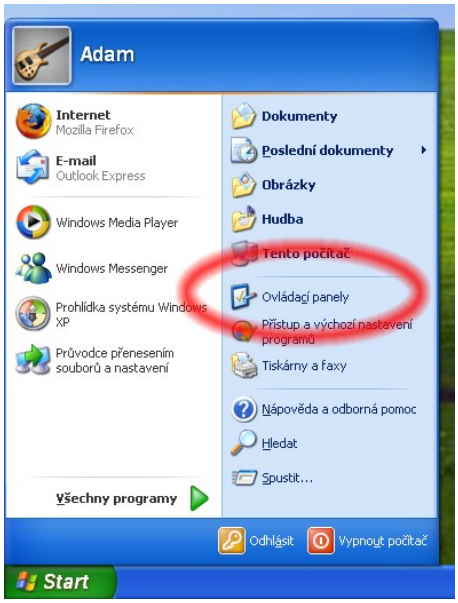
SEZNAM TABULEK

SEZNAM PŘÍLOH

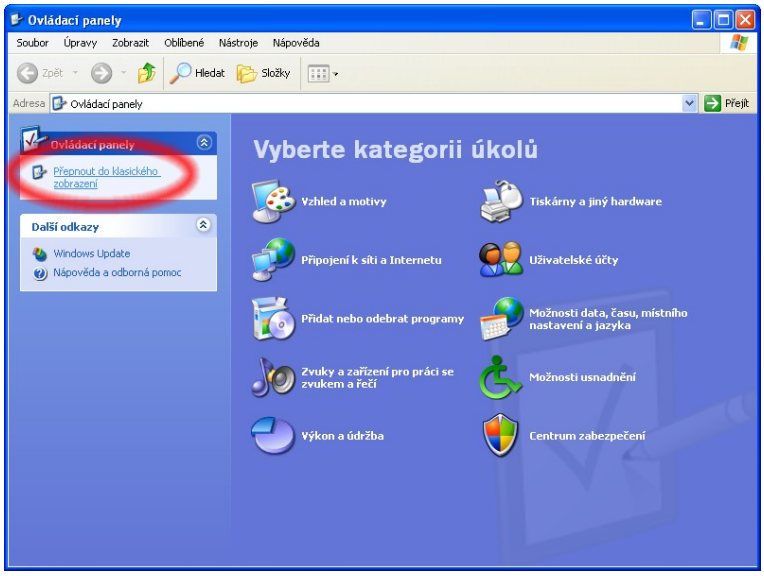
PŘÍLOHA 1: NASTAVENÍ WINDOWS UPDATE VE WINDOWS XP

V systému Windows XP můžeme volit čas automatických aktualizací, jejich činnost (zda aktualizace instalovat, stahovat nebo o nich pouze informovat), nebo je můžeme zcela vypnout. Ke zmíněným nastavením se dostaneme takto:

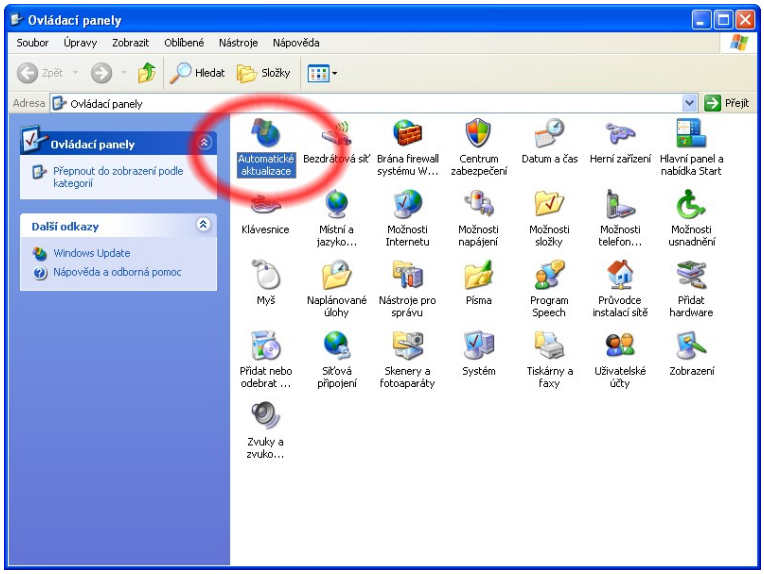
V nabídce **Start** vybereme položku **Ovládací panely**.



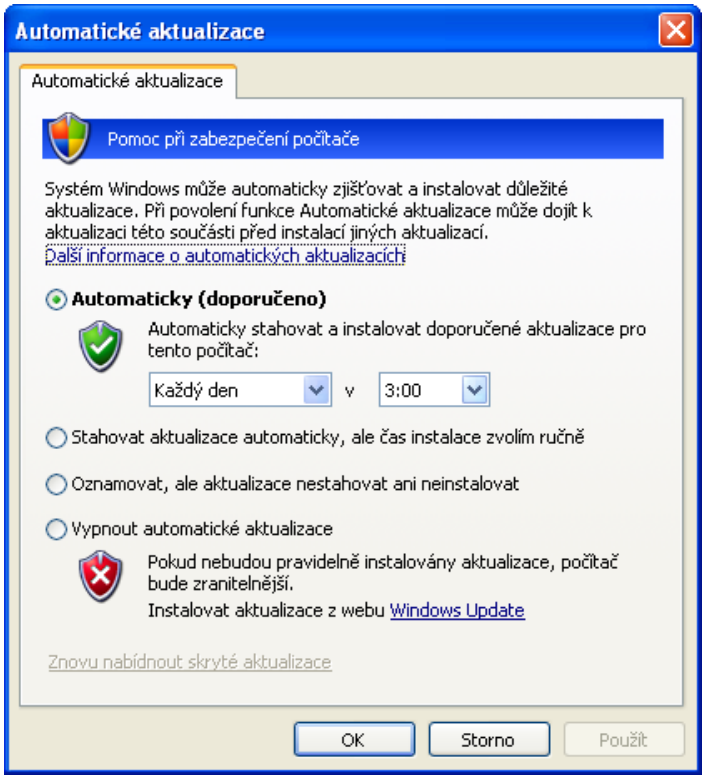
V levém horním menu **Ovládací panely** vybereme volbu **Přepnout do klasického zobrazení**.



Po přepnutí zobrazení vybereme ikonu **Automatické aktualizace**.



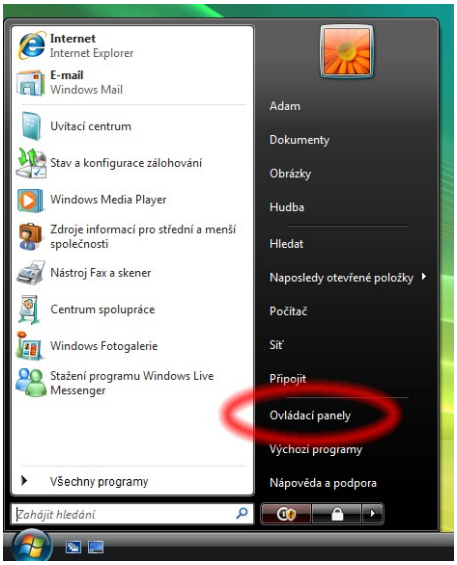
Nyní se nacházíme v nastavení automatických aktualizací Windows Update. Po provedení požadovaných změn nastavení uložíme kliknutím na tlačítko **OK**.



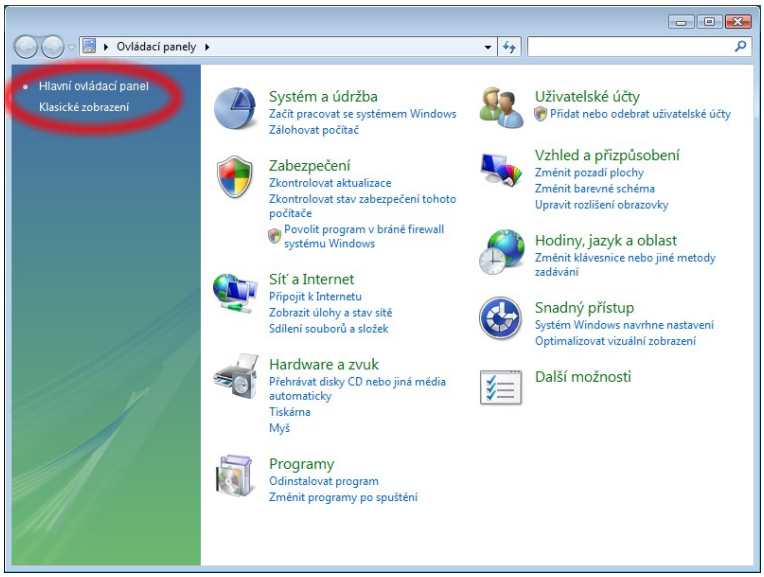
PŘÍLOHA 2: NASTAVENÍ WINDOWS UPDATE VE WINDOWS VISTA

Podobně jako v systému Windows XP můžeme i v systému Windows Vista volit čas automatických aktualizací, jejich činnost, nebo je můžeme zcela vypnout. K nastavením automatických aktualizací se dostaneme takto:

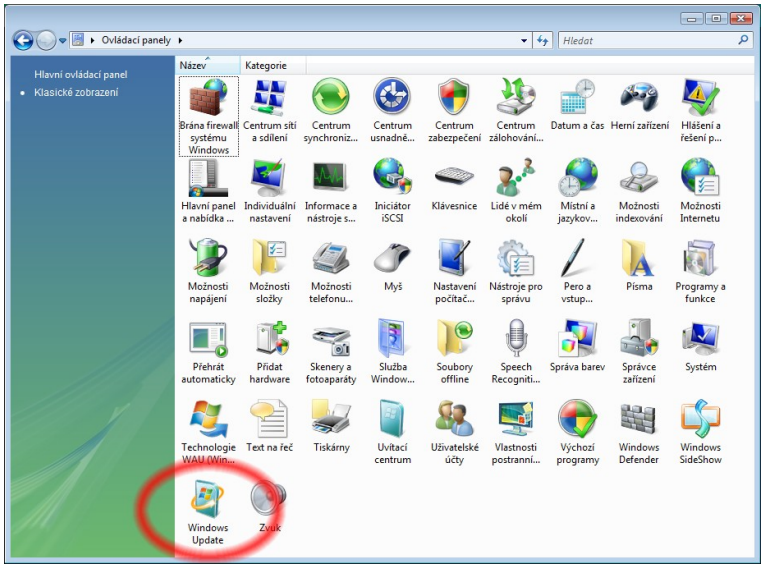
V nabídce **Start** vybereme položku **Ovládací panely**.



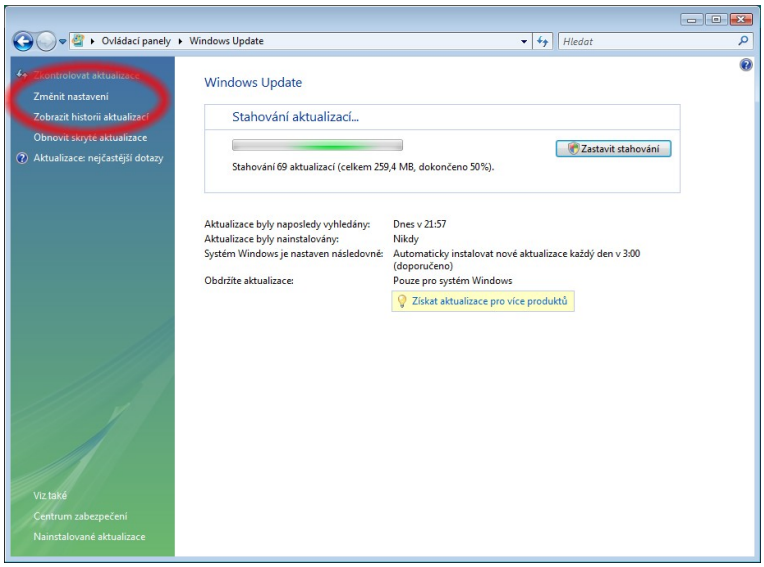
V levém horním menu **Hlavní ovládací panely** vybereme volbu **Přepnout do klasického zobrazení**.



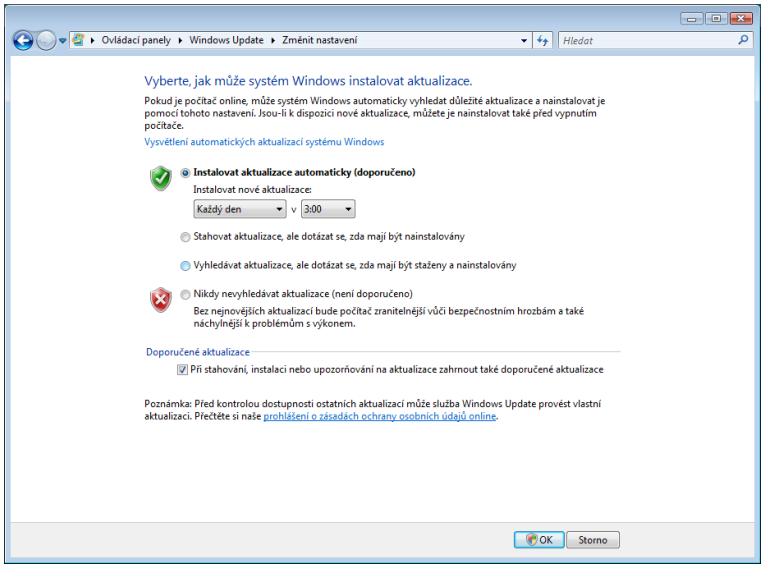
Po přepnutí zobrazení vybereme ikonu **Windows Update**.



Po otevření okna **Windows Update** vidíme informace o aktuálním stavu aktualizací. V horní části je právě prováděná činnost (instalace), ve spodní části jsou uvedeny statistické informace (čas posledního vyhledávání nebo instalace aktualizací). Pro změnu nastavení zvolíme z levého horního menu **Změnit nastavení**.



Nyní se nacházíme v nastavení automatických aktualizací Windows Update. Po provedení požadovaných změn nastavení uložíme kliknutím na tlačítko **OK**. Tato akce vyžaduje v systému Windows Vista administrátorské oprávnění.

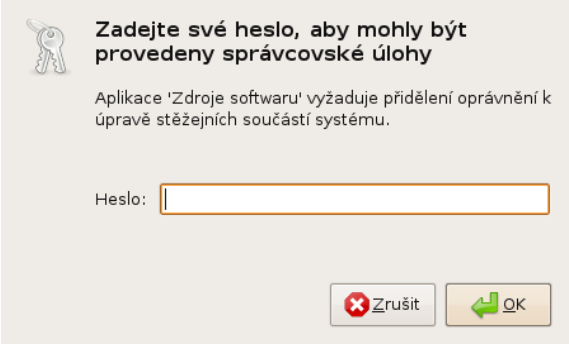


PŘÍLOHA 3: NASTAVENÍ SPRÁVCE AKTUALIZACÍ V UBUNTU LINUX

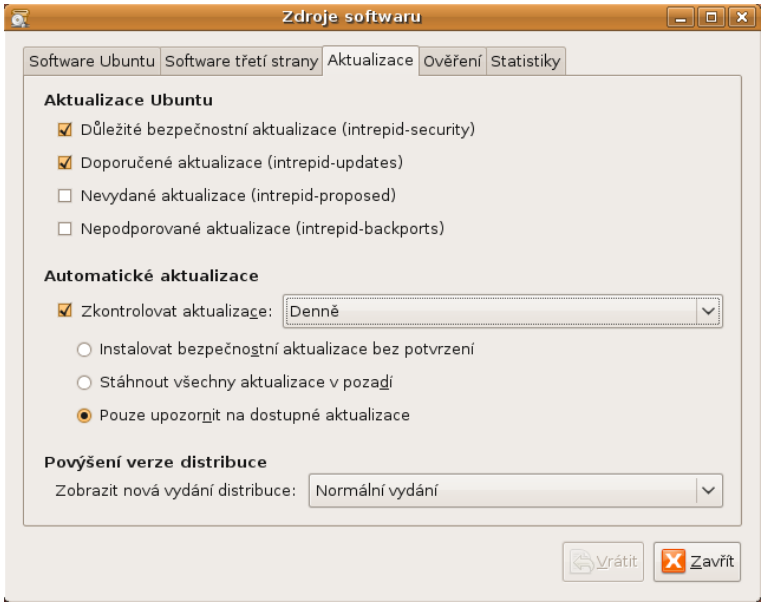
V systému Ubuntu Linux slouží pro aktualizace systému a nainstalovaných aplikací Správce aktualizací. Podobě jako v systémech Windows i zde můžeme specifikovat čas spouštění a činnost správce aktualizací. K nastavení se dostaneme následujícím způsobem:

Z hlavního systémového menu v levém horním rohu vybereme **Systém**, poté zvolíme **Správa** a zde vybereme položku **Zdroje softwaru**.

Pro spuštění **Zdroje softwaru** jsou potřeba administrátorská práva, proto nás systém požádá o heslo. Po jeho zadání stiskneme tlačítko **OK**.



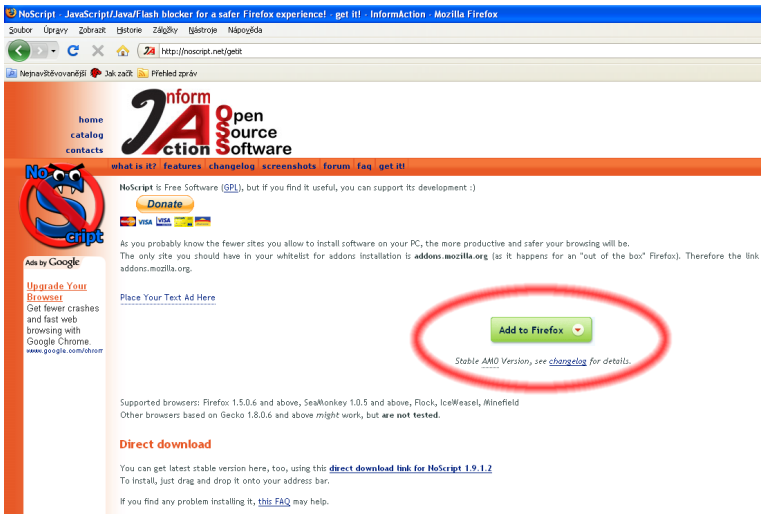
Po otevření okna přepneme na záložku **Aktualizace**. Zde můžeme nastavit nejen čas a činnost automatické aktualizace, ale můžeme také zvolit zdroje aktualizací. Můžeme tak například získat velmi čerstvé aktualizace, které však neprošly testováním a mohou být nestabilní. Po provedení požadovaných změn uložíme změny kliknutím na tlačítko **Zavřít**.



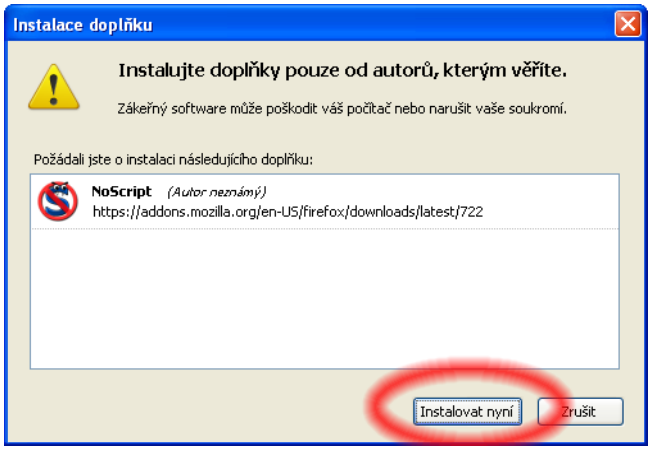
PŘÍLOHA 4: INSTALACE ROZŠÍŘENÍ NOSCRIPT

Instalací rozšíření NoScript získáme výrazné zvýšení bezpečnosti při prohlížení webových stránek v prohlížeči Firefox. Rozšíření automaticky blokuje skripty v jazyce JavaScript, jelikož bývají zneužívány k rozličným typům útoků. Pomocí rozšíření pak můžeme jednoduše povolit individuální skripty, kterým důvěřujeme. Instalaci NoScript do prohlížeče provedeme následujícím způsobem:

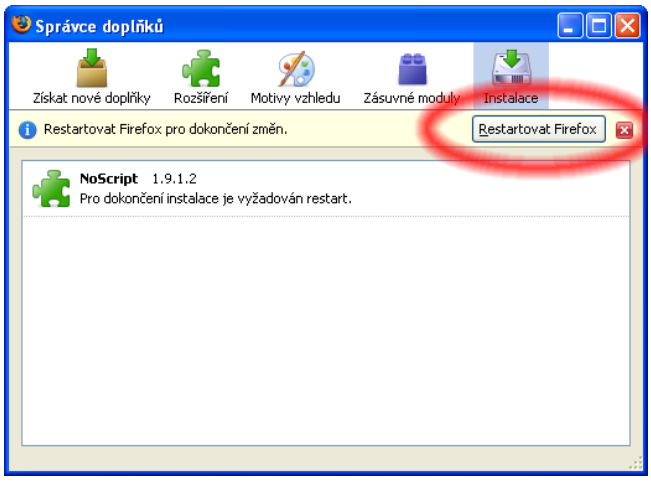
Spustíme **Firefox** (např. ikonou na ploše) a přejdeme na stránku **http://noscript.net/getit** (bez www). Uprostřed stránky klikneme na tlačítko **Add to Firefox**.



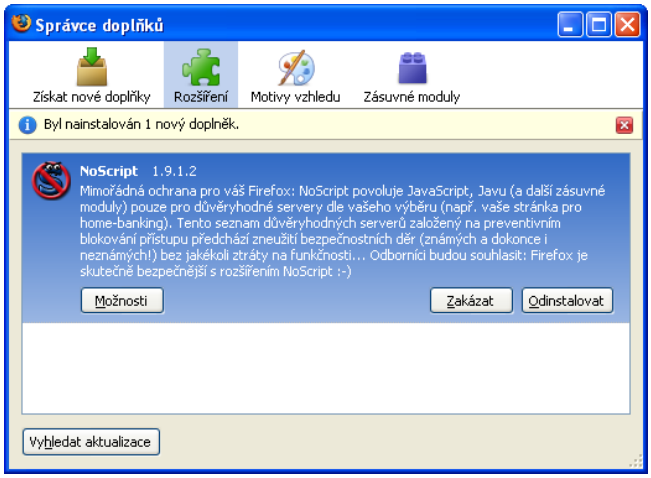
Po kliknutí na tlačítko se otevře okno **Instalace doplňku**. Instalaci potvrdíme kliknutím na tlačítko **Instalovat nyní**.



Abychom mohli rozšíření začít ihned používat, musíme prohlížeč Firefox restartovat. Proto klikneme na tlačítko **Restartovat Firefox**.



Po restartu nás o úspěšném dokončení instalace informuje okno **Správce doplňků**.



Nainstalované rozšíření přidalo svoji ikonu do pravého dolního rohu hlavního okna prohlížeče. Odtud jej můžeme snadno vyvolat a upravit jeho nastavení. Rozšíření nás navíc na každé blokování skriptu upozorní informační lištou ve spodní části prohlížeče. Kliknutím na lištu můžeme požadované skripty dočasně (nebo i trvale) povolit.