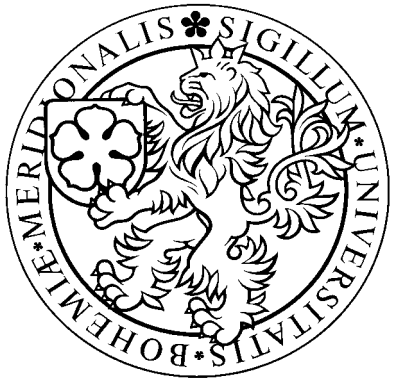
JIHOČESKÁ UNIVERZITA
PEDAGOGICKÁ FAKULTA
KATEDRA INFORMATIKY



OFICIÁLNÍ WWW PREZENTACE OBCE JÍLOVICE
BEZPEČNOSTNÍ ASPEKTY INTERNETU

BAKALÁŘSKÁ PRÁCE

RADEK FILIP

ČESKÉ BUDĚJOVICE 2003

Anotace:

Tato práce se zabývá problematikou bezpečnosti internetu a jeho hlavních služeb, jako jsou WWW a elektronická pošta. Jsou zde popsána rizika, která uživatelům internetu hrozí z různých stran. Důležité jsou možnosti obrany a ochrany, které jsou zde rovněž popsány.

Práce může posloužit pro získání přehledu o možných ohroženích, která s sebou rozvoj internetu přináší a bez kterých si jeho využívání již nelze představit.

Praktickou částí této práce je oficiální WWW prezentace obce Jílovice v okrese České Budějovice.

Poděkování:

Děkuji tímto PaedDr. Petru Pexovi za poskytnutí užitečných rad a za vedení při psaní této bakalářské práce.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a použil pramenů, které jsou uvedeny v seznamu literatury.

V Českých Budějovicích, 5. prosince 2003

Obsah

1 Úvod

Internet je rozlehlá počítačová síť, která vznikla a vzniká postupným propojováním lokálních sítí do větších celků a jež používá jednotný komunikační protokol - IP (Internet Protocol). Internet tvoří jednak vlastní počítače, jednak komunikační infrastruktura - kabely lokálních sítí, optická vlákna, telefonní linky, mikrovlnná nebo laserová pojítka, satelitní linky a podobně - a hlavně propojovací prvky (opakovače, mosty, směrovače, brány, routery). Propojovací prvky jsou vlastní duší internetu, neboť ony zajišťují schopnost přenášet informace od odesílatele k příjemci.

Z této definice je vidět, že internet je pouhý technický prostředek zajišťující libovolným strojům k němu připojeným (potažmo jejich uživatelům) možnost vzájemné komunikace. To, co dělá internet tak přitažlivým, jsou jednotlivé služby, které nabízí, zejména služba WWW. Z technického hlediska jsou tyto služby jednoduše distribuované aplikace využívající internet pro přenos svých vlastních dat (distribuované proto, že jednotlivé části těchto služeb – servery a klienti - jsou rozmístěny na různých počítačích v síti). Každá taková aplikace používá vlastní protokol, kterým se spolu domlouvají její jednotlivé části (v případě WWW je tímto protokolem HTTP - Hyper-Text Transfer Protocol).

Internet je velice významným prostředkem komunikace mezi lidmi a také významným prostředkem obchodu. Připojení na internet je nutností nejenom pro počítačové firmy, ale i pro organizace, které se přímo počítači nezabývají, ale využívají je ke své činnosti. Jednou z hlavních, a patrně nejčastěji využívaných, služeb je komunikace pomocí elektronické pošty. Velký význam má také prezentace firmy na internetu a v neposlední řadě též využití internetových technologií pro interní práci, tzv. intranet.

V souvislosti s využíváním komunikace prostřednictvím internetu a rozvojem elektronického podnikání, se zvyšují bezpečnostní rizika s tím spojená. Napojením systému na okolí pomocí internetu se zvyšuje zranitelnost připojených sítí a počítačů a roste nebezpečí zneužití či ztráty informací, například prostřednictvím počítačových virů nebo externími útoky. Následky zcizení nebo ztráty dat jsou potom jen těžko vyčíslitelné.

Internet byl a je nezabezpečeným přenosovým kanálem. Nesnaží se totiž jakkoli zabezpečovat data, která jsou mu svěřena k přenosu. Tato data nijak nekóduje (nešifruje), ani příliš nezkoumá, zda každá z komunikujících stran je skutečně tím za koho se vydává. Naštěstí ale takovýto nezabezpečený charakter internetu není nepřekonatelnou překážkou, neboť nebrání tomu aby se vše potřebné zajistilo již na aplikační úrovni. Tedy aby se přenášená data zabezpečila proti eventuelnímu odposlechu vhodným zašifrováním ještě před jejich odesláním.

Při vzájemné komunikaci (nejen na internetu) je někdy důležité mít hodnověrný důkaz o identitě svého partnera. To se týká nejen využívání síťových služeb, ale například i komunikace uživatele s počítačem. Bývá zvykem, že uživatel zahajuje svoji práci s počítačem vložením svého jména a hesla - počítač tak má možnost ověřit si totožnost obsluhy. Důkaz totožnosti bývá založen na existenci informace, kterou může (nebo alespoň by měla) disponovat pouze dotyčná osoba, a způsobu, jakým ověřit pravost této informace.

Ne všechny služby a informace v počítačovém systému mohou být přístupné všem uživatelům. Proto se používá řízení přístupu (autorizace), což je proces, při kterém se rozhoduje, má-li uživatel právo vykonat akci, o kterou žádá. Tato služba nezbytně potřebuje možnost ověření totožnosti (tato vzájemná provázanost jednotlivých složek bezpečného systému je naprosto obvyklá a ve skutečnosti nevyhnutelná).

Jsou-li v počítači uloženy informace, které jsou důvěrné, je zapotřebí systém, který důvěrnost informací zajišťuje. Tato vlastnost znamená, že nikdo cizí si nemůže přečíst určitá data bez patřičného oprávnění. Je také potřebné, aby systém garantoval, že data nemůže nikdo neoprávněně měnit, nebo alespoň zajišťoval, že změna dat je snadno detekovatelná.

Internet jako takový žádnou z výše uvedených funkcí neposkytuje. Při komunikaci s jiným počítačem není jistá jeho identita, řízení přístupu je jakousi formou implementováno ve firewallech, důvěrnost a nedotknutelnost informací je téměř nulová (odposlouchávat data je snadné zejména na lokálních sítích). Neznamená to však, že je internet nebezpečný. Pouze je třeba bezpečnostní mechanismy budovat na vyšších úrovních, tedy u jednotlivých aplikací.

2 Elektronická pošta

Elektronická pošta představuje jednu z nejvyužívanějších funkcí, které uživatelům internet nabízí. Je to velice efektivní, rychlý a pohodlný způsob komunikace, bez kterého si už mnoho lidí nedokáže představit život. Na lidi, kteří elektronickou poštu využívají však mohou také číhat mnohá nebezpečí. Často lidem neškodí tak, že by páchaly nějakou destrukční činnost, ale například je okrádají o čas nebo v nich chtějí vzbudit zbytečný strach. Stejně tak ale v souvislosti s elektronickou komunikací mohou vzniknout konkrétní škody napáchané například nějakým destruktivním virem.

Základními prvky sítě pro přenos elektronické pošty jsou poštovní servery. Jedná se o počítače trvale připojené na internet, na kterých běží specializovaný software. Poštovní server obsahuje e-mailové schránky svých uživatelů, do kterých ukládá došlou poštu. Aby si uživatelé mohli poštu přečíst, komunikují s poštovním serverem pomocí jimi ovládaného programu, který se nazývá poštovní klient. Tímto klientem nemusí být nutně program běžící na jejich počítači, ale může jím být například webové rozhraní, známé z mnoha freemailových služeb. Způsob komunikace se řídí oficiálně stanovenými protokoly:

- **SMTP** (Simple Mail Transfer Protocol) - protokol používaný pro odesílání pošty
- **POP3** (Post Office Protocol 3) - protokol pro přijímání (stahování) e-mailů
- **IMAP** (Internet Message Access Protocol) - protokol pro vzdálený přístup ke schránce a pokročilejší práci s jejím obsahem

Pomocí SMTP protokolu je tedy e-mail odeslán na příslušný SMTP server, který jej přijme. Pokud je e-mail určen lokálním adresátům, umístí jej rovnou do jejich schránky. Není-li tomu tak, dále jej zpracuje. Snaží se jej doručit na cílový poštovní server, ze kterého si ho adresát stahuje pomocí protokolu POP3.

Zajímavostí je, že u protokolu SMTP se nepoužívá žádná autentizace. To znamená, že SMTP umožňuje odeslat e-mail cizím jménem, případně z neexistující adresy. Ochrana proti tomu musí být implementována na odesílacím serveru vhodnými nastaveními. Při stahování pomocí protokolu POP3 je situace jiná, neboť po identifikaci serveru následuje autentizace pomocí uživatelského jména a hesla.

V běžné praxi většinou není pro doručení e-mailu využíván pouze jeden poštovní server, ale zpráva cestuje mezi více servery. Podrobnosti o e-mailu lze zjistit z hlavičky, která je součástí každé zprávy a která obsahuje informace o příjemci, odesílateli, předmětu a dalších podobných údajích potřebných pro doručení zprávy. Součástí hlavičky je také široká škála služebních informací, včetně údajů o směrování mezi servery.

První položkou je *Return-Path*, jejímž obsahem je zpáteční adresa, která se použije při odpovědi na e-mail. Následuje první položka *Received*. Takto označený záznam přidá do hlavičky každý poštovní server, který zpracovává zprávu. Pokud tedy chceme zjistit cestu zprávy mezi servery, musíme sledovat záznamy *Received* v textu hlavičky směrem zdola nahoru. Odesílatel je označen jako *From*, předmět jako *Subject*, použitý poštovní klient jako *X-Mailer* apod.

Informací získaných z hlavičky lze tedy velmi vhodně využít v případě, kdy dostaneme nějakým způsobem nebezpečný nebo podezřelý e-mail. Podrobné údaje o cestě zprávy přes poštovní servery mohou často vést k jednoznačné identifikaci jejího původce. Přesto však není pravdivost údajů v hlavičce vždy stoprocentní.

Pro mnoho uživatelů je odesílatel e-mailu uvedený v políčku *From* věrohodným údajem, kterému naprosto důvěřují. Bohužel právě tento údaj lze velmi jednoduše zfalšovat a pak se kdokoliv může vydávat za někoho úplně jiného, než kým ve skutečnosti je.

E-mailový klient většinou umožňuje velice jednoduše nastavit jakékoliv jméno a uživatelskou adresu. Místo skutečného jména lze tedy jednoduše nastavit například jméno *Bill Gates*, adresu *billg@microsoft.com* a začít posílat e-maily pod tímto jménem. Taková je skutečnost, kterou si bohužel mnoho uživatelů internetu neuvědomuje a bere údaj o odesílateli za směrodatný. Bohužel není ani problém odeslat e-mail přes SMTP server,

který používá osoba, za níž se podvodník vydává. Většinou se jedná o server providera (poskytovatele připojení k internetu), u kterého je dotyčná osoba připojena. Vše bude tedy vypadat zcela věrohodně i po této stránce.

Proto nelze nikdy důvěřovat jen údaji v políčku *From:*. V případě sebemenších pochybností o původu e-mailu je potřeba si ověřit, zda daný člověk tento e-mail opravdu napsal a odeslal. E-maily je proto vhodné podepisovat digitálními podpisy (viz. Kapitola 6.2). Odesílatel pak e-mail podepíše a příjemce pouze zkontroluje za pomoci veřejného klíče odesílatele, zda podpis souhlasí (tedy, zda e-mail napsala skutečně uvedená osoba). U takto podepsaného e-mailu lze rovněž snadno zjistit, zda nebyl jeho obsah cestou neoprávněnou osobou změněn.

Při psaní e-mailu se vyplatí dodržovat pravidlo, které říká, že elektronickou poštou by si měl uživatel dovolit poslat zhruba to, co si dovolí napsat na obyčejnou papírovou pohlednici či korespondenční lístek.

2.1 Viry přenášené elektronickou poštou (wormy)

Velké nebezpečí při práci s elektronickou poštu spočívá v možnosti infiltrace počítače virem. Virové problematice je věnována samostatná kapitola. Zde se budu zabývat typem viru, který se označuje jako *červ (worm)*. Červ způsobuje takový typ infiltrace, která se do počítače dostane elektronickou poštou. Na počítači se vyskytuje nejčastěji pouze v jednom exempláři – souboru, který v sobě neobsahuje nic jiného, než jmenovaného červa.

Infikovaný e-mail obsahuje většinou přílohu se souborem. Pokud tento soubor obsahující worm uživatel spustí, dojde k jeho aktivaci. Nejčastěji se pak uloží v počítači a ve vhodném okamžiku odešle další takto infikované e-maily na e-mailové adresy dalších uživatelů (obvykle těch, které si uživatel eviduje ve svém adresáři kontaktů).

K tomu, aby přiložený soubor s červem příjemce pošty spustil, je motivován většinou lákavými názvy přílohy nebo jejím popisem v těle e-mailu. Autoři wormů spoléhají na to, že pro mnoho lidí je lákavý například soubor s názvem „Anna Kurnikovová“ či „Pamela Anderson“, který je navíc v těle zprávy podpořen textem „Podívejte se do přílohy na nahou Pamelu

Anderson, nebudete litovat!“. Běžný uživatel by se mohl těšit na obrázek, ale ve skutečnosti může jít o červa, který jen čeká na to, až ho uživatel spustí.

Příloha e-mailu bývá tvořena souborem s tzv. dvojitou příponou. Někteří červi se k e-mailu připojí v souboru, jehož celý název vypadá následovně: „nazev.pripona1.pripona2“. Při nesprávném nastavení Windows může uživatel vidět jen „nazev.pripona1“. V praxi se tak může soubor „PamelaAnderson.jpg.exe“ jevit jako „PamelaAnderson.jpg“, což vypadá pro zvědavého uživatele velmi lákavě. Náprava je jednoduchá, stačí pouze upravit registry Windows (např. pomocí programu *regedit*) a z vhodných klíčů ve větvi HKEY_CLASSES_ROOT odstranit položky s názvem NeverShowExt.

Existuje však také možnost, že červ je přímo součástí zprávy a není potřeba žádného souboru v příloze. Nutnou podmínkou pro úspěšné šíření těchto červů je existence poštovních klientů, které dokážou poštu přijímat v HTML formátu. S příchodem HTML do poštovních klientů jsou sice zprávy mnohdy vizuálně přívětivější (obrázky na pozadí, barevné písmo atd.), ale zároveň tím byly otevřeny dveře červům. Příkladem může být JS/Kakworm, který vkládá svoje tělo přímo do HTML kódu zprávy ve formě JavaScriptu. Červ se v tomto případě aktivuje pouhým otevřením infikované zprávy.

2.1.1 Wormy nezávislé na použitém poštovním klientu

Tuto skupinu zastupuje například červ I-Worm/Haiku, který kromě skládání veršů hledá emailové adresy dalších obětí v některých souborech po celém disku. Na získané emailové adresy pak hromadně, za podpory SMTP serveru někde ve světě, odesílá svoje kopie (tj. soubor haiku.exe, který tvoří přílohu emailové zprávy). Červ I-Worm/Happy99 (alias Ska) pro změnu modifikuje soubor WSOCK32.DLL tak, aby se při volání služeb Connect a Send aktivoval kód červa, který připojí svoje tělo k odesílanému emailu.

2.1.2 Wormy závislé na použitém poštovním klientu

Mezi tyto červy patří především všechny typy makrovirů, které jsou založeny na principech makroviru W97M/Melissa. Některé antiviry přidávají na konec takových makrovirů označení @mm. Patří sem i VBS/LoveLetter,

VBS/AnnaKurnikova apod. Tyto wormy jsou závislé především na klientu MS Outlook, který je součástí kancelářského balíku MS Office 97/2000.

2.1.3 Wormy ve Windows

Červi se nacházejí v souboru samostatně a nepotřebují žádného hostitele (až na výjimky). Antivirové programy tak ve většině případů mažou všechny soubory, které si červ pro svůj chod v systému vytvořil. Nevracejí však do původního stavu registry Windows, popřípadě soubory, které červ zmodifikoval tak, aby si zajistil včasnou aktivaci po každém startu operačního systému Windows. Většina červů si zajistí automatické spuštění nejčastěji pomocí modifikace registrů, pomocí modifikace souboru WIN.INI nebo SYSTEM.INI (v adresáři s instalací Windows).

V registrech Windows využívají červi často klíč HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\\Run. V něm vytvářejí nové položky s údaji obsahující cestu k souboru, který se pak při každém startu Windows aktivuje. Využíván bývá také klíč HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open. Jeho modifikací si některé wormy zajistí to, že se aktivují přesně v okamžiku, kdy uživatel spustí nějaký EXE soubor. Při léčení je nutné nejprve vrátit jmenovaný klíč do původního stavu "%1" %* a až potom odstranit soubory patřící červu. V opačném případě nebude možné spustit žádný EXE soubor (Windows se budou odkazovat na neexistující soubor červa). Problém je v tom, že i program na úpravu registrů je s příponou EXE (regedit.exe). Lze však využít změny přípony na COM a červa tak oklamat. Příkladem z praxe může být červ I-Worm/PrettyPark, který původní hodnotu "%1" %* jmenovaného klíče upraví na FILES32.VXD "%1" %*.

V souboru WIN.INI je občas pod útokem červa řádek RUN= v sekci [WINDOWS]. Podobně na tom může být i sekce [BOOT] s řádkem SHELL= v souboru SYSTEM.INI. Za sekvencí znaků RUN= se zpravidla nic nenachází. Pokud ano, může to být známka toho, že na počítači je nebo byl červ. Nemusí se však vždy jednat o červa, občas tyto možnosti využívají i některé užitečné programy. Za řádkem SHELL= se pak běžně vyskytuje pouze příkaz EXPLORER.EXE.

2.2 Hoax

Anglické slovo *hoax* v překladu znamená falešná zpráva, mystifikace, poplašná zpráva. V počítačovém světě slovem hoax nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem a většinou je rozesílána prostřednictvím elektronické pošty.

Text poplašné zprávy obsahuje většinou tyto body:

- Popis nebezpečí (viru) – Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděn i způsob šíření.
- Ničivé účinky viru – Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem běžné, např. zformátování disku, nebo už méně důvěryhodné - roztočení HDD opačným směrem apod.
- Varování důvěryhodných zdrojů – Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že původní varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" apod.)
- Výzva k dalšímu rozeslání – Tento bod hoax vždy obsahuje. Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechne. Díky tomu se tyto nesmysly lavinovitě šíří. V praxi lze použít pravidlo, které říká, že pokud zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností hoax.

Nejčastějším typem hoaxů jsou poplašné e-maily varující před viry a různými útoky na počítač. Výjimkou však nejsou ani zprávy varující před nebezpečím mimo oblast výpočetní techniky. Velmi časté jsou falešné prosby o pomoc (obvykle finanční), které útočí na základní lidské city. S rozvojem mobilních telefonů se začaly vyskytovat také fámy obsahující vymyšlené, zkreslené nebo neúplné informace o mobilních telefonech.

Zajímavým druhem hoaxů jsou různé petice a výzvy. Může se jednat buď o smyšlenou petici jako žert nebo o nedomyšlenou snahu boje za určitou věc. Petice šířená e-mailem často neobsahuje potřebné údaje podepisujících se (pokud je lze takto označit), aby mohla být platná. Na druhou stranu, jestliže jsou ke jménu připojeny další osobní údaje, jsou pak k dispozici

komukoliv, kdo e-mail dostane. Zpráva s osobními údaji se šíří pyramidovitě v mnoha různých variantách na další adresy.

Podvodné e-maily tvoří další skupinu hoaxů. Podvodníci rozesílají e-maily s lákavými nabídkami na velkou sumu peněz. Údajnými odesílateli jsou například vdovy po bohatém podnikateli, které žádají o pomoc při převodu peněz ze země. Jako odměna za pomoc je slíbeno až několik miliónů dolarů. Hlavní trik podvodu je v tom, že nachytaná oběť je nucena postupně platit několikatisícové poplatky na údajné výdaje spojené s převodem peněz, který je stále pod různými záminkami odkládán.

Dalšími hoaxy mohou být různé obdoby pyramidových her. Podle českých zákonů jsou pyramidové hry zakázány, proto se je organizátoři snaží maskovat jako prodej různých produktů. Tyto nabídky mají stejný základ: koupím produkt od zapojeného účastníka(ů), tím již zapojené členy posunu o pozici výš a snažím se přesvědčit jiné, aby produkt koupili a moji pozici tím také vylepšili. Pokud je trh nasycen - a to díky pyramidovému způsobu je poměrně rychle - poslední mají minimální šanci, že někdo další se připojí a jsou to pouze jejich peníze, které pomohly alespoň částečně vrátit náklady zapojeným předchůdcům. Hoaxy, které jsou známé většinou i ve své „papírové“ variantě, jsou řetězové dopisy štěstí šířené z pověrčivosti nebo z neznalosti.

Mnohým se může zdát, že šíření hoaxů nemůže být škodlivé. Při bližším pohledu na věc zjistíme opak. Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemný, zejména v době epidemie, kdy se v jejich e-mailových schránkách objevuje stejná zpráva několikrát denně.

Odesláním hoaxu obchodním partnerům nikdo svou prestiž určitě nezvýší. Šíření poplašných zpráv státními úředníky není dobrou vizitkou úřadu a vrcholem je rozeslání falešného varování před virem zaměstnancem firmy, která se zabývá výpočetní technikou nebo programováním.

Přestože výkonnost serverů a rychlost vzájemného propojení se zvyšuje, je nutné si uvědomit, že zatížení sítí také narůstá. Vyšší nároky na sítě jsou dány nejen narůstajícím počtem uživatelů, ale také stále větším počtem šířících se wormů - červů. Velké množství hoaxů rozesílají uživatelé pomocí funkce přeposílání (Forward) a na všechny adresy. Tím dochází k postupnému přidávání adres k textu zprávy a samozřejmě narůstá velikost zprávy,

často až do velikosti přesahující 100 kB. Pro porovnání běžný e-mail mívá velikost 2-6 kB, e-mail s přiloženým dvoustránkovým dokumentem, vytvořeným v programu Microsoft Word přibližně 65 kB.

Jestliže se hoax přeposílá výše uvedeným způsobem, dává se k dispozici obrovský seznam e-mailových adres náhodným příjemcům. Díky lavinovitému šíření zprávy nelze dopředu vědět, komu v dalších úrovních bude e-mail doručen. Seznam adres je rájem pro spammery, kteří pak mohou na získané adresy posílat nevyžádané e-maily. Někteří uživatelé se pak mohou divit, jak mohl spammer získat jejich adresu, kterou svěřili pouze několika známým. Další nepříjemná situace by mohla nastat, kdyby se seznam adres klientů a obchodních partnerů dostal ke konkurenci.

2.3 Spam

Spam je nevyžádaná zpráva doručená elektronickou poštou, většinou s komerčním reklamním obsahem. Spamming je vlastní činnost rozesílání spamových zpráv. Pokud má odesílatel souhlas adresáta se zasíláním určitého druhu informací, může tak činit po dobu, po kterou tento souhlas bude platit. Adresát totiž může svůj souhlas kdykoliv odvolat. Pokud odesílatel souhlas nemá, je situace složitější. Zákon o ochraně osobních údajů umožňuje, aby správce nebo zpracovatel použil jméno, příjmení a adresu subjektu údajů pro zpracování těchto údajů za účelem nabízení obchodů nebo služeb. Ovšem v případě, že s takovým zpracováváním subjekt údajů vyslovil nesouhlas, nelze uvedené údaje dále zpracovávat. Otázkou je, zda je či není adresa elektronické pošty takovým údajem.

Správce, který zpracovává údaje za účelem nabízení obchodu nebo služeb, může tyto údaje předat jinému správci, při splnění následujících podmínek:

- údaje subjektu byly získány v souvislosti s činností správce nebo se jedná o zveřejněné osobní údaje
- údaje budou využívány pouze za účelem nabízení obchodu nebo služeb
- subjekt údajů byl o tomto postupu správce předem informován a nevyjádřil s ním nesouhlas

Z toho plyne, že spamming je legální aktivitou, ale jen do doby, kdy subjekt údajů odvolá dříve poskytnutý souhlas nebo vyjádří nesouhlas s takovou činností. Zákon o regulaci reklamy zakazuje šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje. Pokud tedy bude text spamu reklamou, a adresát je jí obtěžován nebo mu způsobuje výdaje, bude taková aktivita protiprávní.

Zatímco papírové letáky a jejich distribuce jsou pro autora poměrně nákladnou záležitostí, u spamu jsou náklady pro odesílatele téměř nulové a nese je zejména příjemce nevyžádaných e-mailů ve formě poplatků za připojení k internetu.

Studie společnosti Ferris Research odhaduje dobu strávenou mazáním každého spamu na 4,5 vteřiny. Na celkovém objemu příchozí firemní elektronické pošty se spam podílí 15–20%. Roční dopad spamu na evropské firmy je odhadován na 2,5 mld. USD, z toho 60% tvoří náklady spojené s přenosovou kapacitou a službami technické podpory.

Filosofie spamu je jednoduchá – rozeslat obchodní nabídku na co nejvíce adres s očekáváním, že alespoň mizivá část nechtěných příjemců zareaguje a inzerovaný výrobek nebo službu si koupí, což původci pomůže k zisku.

Definovat úplně přesně, co je spam, je obtížné. Jde o hromadné zasílání nevyžádaných e-mailů. Hromadné z toho důvodu, že velkému množství uživatelů (resp. do mnoha e-mailových schránek) je najednou zaslána zpráva. O tuto zprávu žádný z uživatelů (nebo alespoň jejich část) neprojevil zájem a nedal souhlas k tomu, aby mu odesílatel zasílal e-maily. Spam je samozřejmě také stav, kdy identická zpráva je zaslána sice jednomu příjemci, avšak mnohokrát za sebou na různé e-mailové adresy. Hranice mezi zasláním běžného a nevyžádaného e-mailu není někdy zcela zřejmá. Mnoho lidí zasílá spam záměrně, jindy může jít pouze o neznalost nebo nezkušenost.

O spam v žádném případě nejde například v těchto případech:

- když je e-mail poslán jednomu příjemci, a to i tehdy, pokud o odesílateli příjemce nikdy neslyšel a nemohl předem projevit souhlas se zasláním e-mailu
- zaslání dotazu nebo nabídky spolupráce potenciálnímu obchodnímu partnerovi, pokud se jedná jen o jednoho adresáta

- když se například s obchodními partnery odesílatel dohodne na pravidelném zasílání nových ceníků prostřednictvím elektronické pošty

Podstatou problému je v případě spammingu fakt, že jde o aktivity, které iniciuje jedna strana (rozesílatel, tj. spammer) a které sledují pouze jednostranné cíle, ale do spoluúčasti na těchto aktivitách jsou proti své vůli nuceny i další strany - příjemci spamů. Ti se musí spolupodílet na takových aktivitách, které sami neiniciovali, sami k nim nedali žádný podnět, a mnohdy s nimi dokonce aktivně nesouhlasí a bojují proti nim. Musí vykonávat takové činnosti, které by jinak nevykonávali (např. rozpoznávat a mazat nevyžádané e-maily) a platit za něco, co vůbec nechtějí (podílet se na nákladech na přenos nevyžádaných zásilek). Přitom jsou omezováni na svých právech (nemohou využívat své prostředky k účelům, ke kterým si je pořídili v takové míře, jaká by jinak byla obvyklá), a kvůli tomu jim následně mohou vznikat i dosti významné nepřímé škody. Například kvůli přeplnění poštovní schránky příjemce neobdrží důležitou zprávu, vedoucí k uzavření velkého kontraktu.

Velký rozvoj spammingu v současné době je motivován zejména jeho jednostrannou ekonomickou výhodností pro spamující subjekty (na úkor postižených), a nejvíce spamming "bují" v oblasti pořádání celých marketingových kampaní po internetu.

Nebude-li růst spammingu zastaven, hrozí, že jeho eskalace nabude takové míry, že znemožní řádné používání elektronických mechanismů komunikace - uživatelé například již nebudou chtít používat elektronickou poštu, protože mezi záplavami nevyžádaných zásilek nebudou schopni a ochotni složitě vyhledávat skutečně důležité zprávy (nebo se k nim tyto zprávy vůbec nedostanou).

Možnosti boje proti spammingu spočívají zejména v legislativních opatřeních, technických opatřeních a osvětě. Pro legislativní způsob boje proti spammingu připadají v úvahu tři cesty:

- Využití zákonné ochrany osobních údajů (protože při spammingu či v souvislosti s ním dochází ke zneužití osobních údajů). Praktickou aplikaci zde ale ztěžuje

skutečnost, že neexistuje jednotný právní konsensus o tom, zda emailové adresy jsou či nejsou osobními údaji.

- Využití obecné odpovědnosti za způsobené škody. Tento princip je zakotven snad ve všech právních systémech. Problémem zde ale je skutečnost, že škody způsobované jednotlivým postiženým jsou příliš malé na to, aby byly brány "dostatečně vážně". Významnější výše by škoda dosáhla v případě koordinovaného postupu více poškozených, ale to je zase značný organizační problém.
- Aplikování specifických zákonů a opatření, zaměřených konkrétně na danou problematiku. Takovéto zákonné normy ale zatím buď vůbec neexistují, nebo jsou teprve ve stádiu úvah či návrhů.

V případě ochrany proti spammingu pomocí technických opatření připadá v úvahu především filtrování a následná eliminace zpráv představujících spamy. V zásadě toto řešení ale neodstraňuje příčinu a pouze snižuje dopad přesunu nákladů na příjemce spamů - protože náklady na filtraci nese buď přímo koncový uživatel nebo poskytovatel připojení (který ale přenáší své náklady na zákazníka, neboli opět na koncového uživatele). Praktickým problémem je také rozpoznávání zpráv, představujících spamy. Rozpoznávání na základě interpretace obsahu je velmi složité a nespolehlivé (je úkolem pro tzv. umělou inteligenci). Jednodušší je rozpoznávání podle adresy, ze které zpráva přichází (např. ze stejné adresy, ze které spammer již dříve podniknul nějaký útok). Takovéto adresy je ale velmi snadné měnit, lze využívat například různých demo kont, které v rámci svých reklamních kampaní nabízí poskytovatelé internetu.

Boj proti spammingu cestou osvěty je zaměřen na vytvoření takové společenské atmosféry, která by potenciálním i aktuálním spammerům vzala jejich motivaci. Veřejné pranýřování konkrétních případů spammingu a firem, které ho využívají, vytváří negativní publicitu, která pro některé firmy může být mnohem důležitější a významnější, než přínos, který pro ně spamming může mít. Další součástí osvěty je i zlepšování veřejného povědomí o podstatě problému, o možnostech technické a legislativní obrany proti němu.

Běžnému uživateli lze doporučit následující rady, jak se bránit nevyžádané elektronické poště:

- je-li ve zprávě uvedeno, jak lze vyjmout adresu ze seznamu adres, na které jsou zprávy zasílány, vyjmout se tímto způsobem ze seznamu
- zkusit odpovědět se žádostí o ukončení zasílání podobných informací
- pomocí filtrů v poštovním klientovi je obvykle možné nastavit blokování příjmu pošty z určité adresy nebo rovnou domény.

3 Obchodování na internetu

Z pohledu účastníků obchodování existují tři hlavní typy obchodů: *Business to Business*, *Business to Customer* a *Business to Administrative*. Jak názvy samy říkají, týkají se obchodů mezi firmami navzájem, mezi obchodníky a koncovými zákazníky a úřady.

Business to Business jsou určeny pro relativně omezený a konečný počet obchodních partnerů na jedné straně a jediného partnera na straně druhé. Používají se především pro systém velkého výrobce a jeho subdodavatelů nebo pro distributora a jeho dealery.

Business to Customer jsou systémy s otevřeným prostředím, kde cílový zákazník není předem znám. Vždy se obchoduje s konečným výrobkem, který je dodáván koncovému zákazníkovi. Tyto systémy jsou podstatně náročnější na provoz, ale zejména na zabezpečení. Elektronické obchodování se tak týká (resp. může týkat) každého člověka jakožto koncového zákazníka.

Zatím poměrně málo rozšířené jsou systémy Business to Administrative. Týkají se oblastí elektronického placení poplatků a daní, poplatků spojených s udělováním licencí a poplatků za služby poskytované úřady a vládními organizacemi.

Ačkoliv oblast Business to Customer se může zdát méně významná z hlediska obratu než Business to Business, zažívá bouřlivější rozvoj a následující text bude věnován právě jí.

Nakupování na internetu je velice pohodlné, ale ne všechny servery provozující elektronické obchodování používají k přenosu finančních a osobních údajů bezpečné transakce. Je třeba ověřit si na každém serveru jeho bezpečnostní zásady, metody sledování objednávek a zásady pro vracení peněz a ochrany soukromí. Vyplatí se opatrnost při žádosti o poskytnutí osobních informací, například o bankovním účtu.

Některé servery provozující elektronický obchod požadují vytvoření uživatelského účtu s heslem. Nikdy by se nemělo používat stejné heslo jako pro jiné účty.

3.1 Internetový obchod

Elektronický obchod na internetu je stále mnohem méně bezpečný než ostatní formy obchodování a bankovních služeb a důvěřuje mu poměrně málo zákazníků. Nebezpečnost elektronického obchodu v současné době potvrzuje informace od Visa International, týkající se platebních karet. Ta říká, že 50% sporů v oblasti platebních karet, které vede tato organizace se zákazníky má původ v transakcích přes internet, které ovšem tvoří pouhá 2% z objemu všech transakcí.

Obchodník musí mít záruku, že získané peníze (v jakékoliv podobě) bude schopen proměnit ve vklad na vlastním účtu. Zákazník by měl mít jistotu, že cena za zboží je přesně taková, jakou obchodník zveřejňuje. Nezanedbatelným aspektem je i jistota získání zaplaceného zboží. Banka musí mít zase jistotu, že nepřijde o své peníze.

Systém pro elektronický obchod lze rozdělit na tři části. Tou první je informační báze, která obsahuje nabízené produkty. Druhou částí je vyhledávací systém, což je prostředek pro vyhledávání v informační bázi. Poslední částí je elektronický platební systém, který slouží k provádění obchodních transakcí.

Současný stav elektronického obchodování na internetu je značně nepřehledný. Postupně vzniklo velké množství virtuálních obchodních domů, kdy o většině se běžně ani uživatel nedozví. Obrovské rozdíly mezi seriozními obchody a těmi ostatními se projevují i v nakládání s osobními údaji zákazníků a jejich ochraně. V drtivé většině českých obchodů není přenos osobních údajů přes internet žádným způsobem chráněný, zákazník proto může jen doufat, že nikdo po cestě „neodposlouchává".

Podívejme se nejdříve, jakým způsobem může proběhnout platba v internetových obchodech:

- **Kreditní kartou** – Zákazník si vybere zboží, zadá číslo kreditní karty a odešle objednávku. Obchodník kontaktuje zákazníka elektronickou poštou nebo telefonem a ověří si zájem o nákup a číslo kreditní karty, kontaktuje banku a požádá o převod peněz od zákazníka a expeduje objednané zboží. Tento způsob platby vyžaduje pro přenos údajů některý z bezpečnostních protokolů,

které zaručí, že informace zadané do formuláře si přečte jedině obchodník a nikdo jiný.

- **Jinou variantou platby** – Například další druhy karet, šeky, v České republice často složenky. Postup se většinou shoduje s výše uvedenou kreditní kartou.
- **Dobírkou** – Zákazník si vybere zboží a odešle objednávku, obchodník kontaktuje zákazníka e-mailem nebo telefonem a ověří si zájem o nákup, obchodník expeduje objednané zboží na dobírku a zákazník při převzetí zboží zaplatí. Poměrně bezpečný způsob platby, ale pouze pro zákazníka. Obchodník si totiž nemůže být několik dní vůbec jist, zda zákazník skutečně existuje a zda dobírku převezme a zaplatí. Navíc do procesu vstupují nejisté služby České pošty – některým obchodům se vrací až třetina objednávek s vysvětlením "adresát nezastižen". Část sice připadá na neseriozní zákazníky, většinu však tvoří zásilky nedoručitelné pouze údajně.
- **On-line platbou přes internet** – S rozvojem internetových obchodů vzniklo velké množství firem, které se specializují na on-line platební transakce na internetu. Vyvinuly několik variant digitálních nebo elektronických peněz, elektronických šeků a platebních protokolů. Ve většině se však jedná o speciální proprietární řešení, která nejsou kompatibilní s ostatními (přestože jsou často technologicky velmi kvalitní). K těmto řešením můžeme přiřadit i eBanku – nejbezpečnější variantu platby přes internet v České republice. Zákazník i obchodník musí být však jejími klienty. Tyto společnosti prosazují vlastní produkty samy nebo v malých aliancích spolu s finančními institucemi.

Současné elektronické obchodování je pro svou rozdrobenost do několika nespolupracujících oblastí internetové jen z části. Většinou je přes internet realizováno pouze prohlížení a nákup zboží, placení a ostatní činnosti již většinou probíhají zcela mimo internet. Ztrácí se tím podstatná výhoda tohoto způsobu obchodování – počítačové propojení všech činností v procesu prodeje.

Placení po internetu může být bezpečné, ale musí být splněny jisté podmínky, mezi které patří i nezbytné šifrování osobních údajů. V současné době se pro bezpečný přenos dat zajištěný šifrováním používají protokoly, z nichž nejznámější je *SET*.

SET (Secure Electronic Transaction) je velmi dobrý protokol pro placení přes internet s využitím platebních karet. Stojí za ním obě nejvýznamnější kartové společnosti VISA a MasterCard, IBM a další velké firmy.

V roce 1996 založily kartové společnosti VISA a MasterCard společnost Secure Electronic Transaction LLC, která dohlíží spolu s ostatními organizacemi na vývoj platebního protokolu SET. Silným zázemím a podporou velkých světových firem z oblasti informačních technologií i bankovnictví se stal celosvětovým standardem pro on-line obchodování a placení na internetu.

3.2 Internetové bankovnictví

Možnost komunikace klientů s jejich bankou prostřednictvím internetu, v rámci služeb označovaných obecně jako internetbanking, je dnes již vcelku běžnou záležitostí a je součástí nabídek většiny bank. O úspěšnosti konkrétních služeb na bázi internetbankingu rozhodují především takové faktory, jako je cena, rozsah a kvalita poskytovaných služeb i celková reputace banky. Naopak relativně malou roli při rozhodování potenciálních klientů hrají otázky bezpečnosti internetových transakcí. Důvodem je skutečnost, že právě tato bezpečnost se stala určitou samozřejmostí, která musí být v každém případě a v dostatečné kvalitě zajištěna u každé služby charakteru internetbankingu. Jedno z nejčastějších řešení například umožňuje přistupovat k bankovním službám z kteréhokoli počítače v dosahu internetu, ale zase nutí uživatele, aby sebou stále nosil malé zařízení velikosti kapesní kalkulačky. Jiné oblíbené řešení zase nenutí zákazníka cokoli nosit sebou, ale na druhé straně jej váže k používání konkrétního počítače na kterém má nainstalováno to, co ke komunikaci s bankou potřebuje.

Požadavky na zajištění bezpečnosti internetbankingu nejsou principiálně odlišné od obecných požadavků kladených na bezpečnou komunikaci po

internetu. Určitou odlišností snad může být různý důraz na jednotlivé aspekty bezpečnosti a na míru, v jaké musí být zajištěny. Přenášená data musí zůstat důvěrná a nesmí se dostat se do nepovolaných rukou. Toho lze dosáhnout jejich zašifrováním, které způsobí, že pokud se tato data přece jen dostanou do rukou někoho nepovolaného, nebudou mít pro něj význam, protože je nebude schopen dešifrovat. Možnostem šifrování a také problematice autentizace je věnována celá kapitola 6.

Každá z komunikujících stran potřebuje mít jistotu že druhá strana nebude moci někdy později popřít svůj požadavek, který vznesla. Například když banka přijme elektronickou cestou nějaký požadavek svého klienta a provede jej, potřebuje mít jistotu že klient si později vše nerozmyslí, nezačne tvrdit že žádný požadavek nevznesl a nezačne se domáhat navrácení původního stavu před provedením transakce. Princip zajištění potřebné neodmítnutelnosti je vcelku jednoduchý - je nutné zajistit, aby příslušný požadavek byl v takovém tvaru, aby nebylo možné zpochybnit, že jej nevygeneroval nikdo jiný než příslušný klient.

Pro banku je velmi významný požadavek identifikace a autentizace, který spočívá v možnosti určení identity komunikující protistrany (identifikace), a dále v ověření, že druhá strana je skutečně tím, za koho se vydává (autentizace). Způsobů, jak zajistit identifikaci a autentizaci je celá řada a jsou vesměs založeny na něčem, co je pro oprávněného klienta charakteristické a unikátní - může jít například o znalost nějaké informace (heslo), vlastnictví nějakého předmětu (např. elektronického klíče) či o určitou fyziologickou charakteristiku (např. otisk prstů). Spolehlivé metody identifikace a autentizace naopak nemohou být založeny na odvozování identity klienta z komunikačního kanálu, prostřednictvím kterého s bankou komunikuje. Právě zde je totiž v konkrétním případě internetu největší prostor pro různé možnosti podvodu.

Banka se vždy potřebuje ujistit o tom, že všechny údaje specifikující požadovanou transakci jsou skutečně takové, jaké jejich klient požaduje. K tomu slouží certifikace, tj. potvrzení platnosti předávaných údajů, charakterizujících požadovanou finanční transakci. Jde například o číslo účtu klienta, číslo cílového účtu, převáděnou částku, variabilní symbol, specifický symbol atd.

V internetovém bankovnictví se pro účely autentizace a certifikace velmi často využívá hardwarové zařízení označované jako elektronický klíč. Je schopné generovat posloupnost jednorázových hesel, které mají jednu velmi důležitou vlastnost - i když by někdo znal posloupnost všech dosud vygenerovaných jednorázových hesel, nedokáže uhodnout (vypočítat) heslo následující. Takže i kdyby někdo na přenosové trase mezi klientem a bankou dokázal zachytávat všechna přenášená hesla a pak z nich chtěl předpovědět heslo příští, nepovede se mu to (a opakovaně použít jednou použité heslo také nemůže, kvůli jejich jednorázovému charakteru). Praktické použití pak nejčastěji vypadá tak, že každou významnější operaci, například samotné přihlášení do klientského systému banky či zadání nějakého platebního příkazu apod., klient stvrzuje zadáním nového jednorázového hesla, které mu vygeneruje jeho elektronický klíč.

Užitečným vylepšením právě popsaného systému jednorázově použitelných hesel je učinit je závislé na parametrech transakce, kterou jednorázové heslo stvrzuje. To sice nutí uživatele zadávat do elektronického klíče příslušná data, ale na druhé straně to výrazně zvyšuje celkovou bezpečnost komunikace klienta s bankou (zajišťuje to certifikaci požadavku). Pokud by se totiž někdo nepovolaný dokázal postavit mezi tyto dva komunikující klienty, zachytávat požadavky klienta, modifikovat je (například tak, aby převod peněz směroval na jeho účet) a teprve pak předávat bance, po změně parametrů by jednorázové heslo nebylo správné a banka by tuto skutečnost bezpečně poznala.

Při právě popsaném způsobu identifikace a autentizace klienta banka odvozuje "pravost" klienta od toho, že má ve svém držení určitý konkrétní předmět, v daném případě elektronický klíč. Pokud by klient předal klíč někomu jinému, či jej získal někdo neoprávněný (například jej ukradl) a dokázal jej správně používat, banka by tuto skutečnost nedokázala rozpoznat. Proto je používání elektronického klíče chráněno ještě osobním PINem, bez jehož zadání není klíč funkční (a po několika chybných pokusech o zadání PINu se zablokuje). Dalším stupněm ochrany pak bývá určité omezení na počet nesprávných pokusů o autentizaci či certifikaci, po jejichž překročení dojde k dočasnému zablokování účtu v bance.

Nutnost používat elektronický klíč je sice v praxi určitým handicapem (je nutné jej nosit všude tam, odkud chce klient komunikovat s bankou), ale na druhé straně má zase významné přednosti co do požadavků na používané počítače a zabezpečení komunikace. Vše co je důvěrné a nemělo by se dostat do nepovolaných rukou je totiž soustředěno v elektronickém klíči, jehož výstupem jsou pouze jednorázově použitelná hesla, která po svém použití ztrácejí jakoukoli hodnotu. Hesla vygenerovaná elektronickým klíčem (ještě k tomu závislá na parametrech požadované transakce) je díky tomu možné přenášet i po nezabezpečeném přenosovém kanálu. To pak v praxi znamená, že klient může využít jakýkoli počítač a jakýkoli prohlížeč, aniž by jej musel jakkoli upravovat a aniž by musel cokoli na daný počítač instalovat. S elektronickým klíčem v ruce je možné jít například do internetové kavárny a komunikovat s bankou odsud.

Průběh takovéto komunikace spočívá v postupném vyplňování formulářů na webových stránkách, které banka klientovi předkládá, a kde klient uvádí parametry požadované transakce (jako výši částky, číslo cílového účtu, variabilní symbol atd.). Do formuláře nakonec také vepíše jednorázové heslo vygenerované elektronickým klíčem. Obsah takto vyplněného formuláře je pak odesílán bance s využitím zabezpečeného protokolu SSL (Secure Sockets Layer), který z nezabezpečeného internetu činí zabezpečený přenosový kanál (a šifruje přenášená data, tj. zajišťuje i jejich důvěrnost).

Řešení s elektronickým klíčem v ČR poprvé zavedla Expandia banka (dnes přejmenovaná na eBanku), a to nejen pro potřeby svého internetbankingu, ale obecně pro všechny možnosti dálkové komunikace zákazníka s bankou (například pro komunikaci po telefonu). Stejné řešení s elektronickým klíčem dnes používají i další banky, i když se ani nemusí jednat o internetbanking (například Komerční banka používá elektronický klíč pro telefonický přístup v rámci své Expresní linky, ale pro svůj internetbanking zvolila jiné řešení, na bázi elektronických podpisů).

Elektronický klíč v podobě fyzického zařízení velikosti kalkulačky má mnohé přednosti - především tu, že nevyžaduje žádné instalace ani změny softwaru na počítači a neváže uživatele na použití žádného konkrétního počítače. Na druhé straně jeho nevýhodou jsou relativně vysoké náklady na samotný elektronický klíč v jeho materiální podobě, ale i nutnost servisu

těchto zařízení, jejich tzv. synchronizace a odblokování po neoprávněném nebo chybném zásahu, výměna baterií atd. Proto se v praxi lze setkat i s alternativami, které elektronický klíč v jeho materiální podobě nahrazují.

Jde o použití tzv. mobilního klíče, který si lze představit jako nemateriální elektronický klíč, který má navíc v držení banka a nikoli její klient. Klient prostřednictvím obvyklého formuláře vyplní údaje specifikující požadovanou transakci. Ovšem místo toho, aby klient následně zadal potřebné údaje do elektronického klíče a tento mu vypočítal potvrzující kód, vypočítá jej banka. Ta k tomu použije klientem již jednou zadané údaje o transakci, a sama provede potřebný výpočet jednorázového hesla. Banka vypočítaný certifikační kód pošle uživateli takovým kanálem, u kterého je oprávněna očekávat, že vede skutečně jen k osobě oprávněné nakládat s příslušným účtem. Klient, který toto jednorázové heslo přijme, jej pak musí přepsat do příslušného políčka formuláře, kterým zadává svůj požadavek, a vše pak odeslat bance. Teprve tím je transakce certifikována a banka ji začíná realizovat.

Přenosovým kanálem, kterým banka posílá vypočítaný certifikační kód oprávněnému klientovi, je jeho mobilní telefon. Banka mu příslušný kód pošle na takové číslo mobilního telefonu, které se svým klientem sjedná v rámci smlouvy o vedení účtu. Mobilní telefon pak vydá certifikační kód až po zadání osobního PINu, což je další ochranný prvek.

3.3 Zneužívání platebních karet

Zneužívání platebních karet, někdy označované jako *carding*, souvisí především s rozvojem internetového obchodování. Platební karta se právě v této oblasti stala často používaným platebním nástrojem a zabezpečení karetních transakcí je v mnoha případech zcela nedostatečné.

Zneužít platební kartu je možné několika způsoby, z nichž nejprimitivnějším je krádež čísla platební karty, případně krádež karty samotné. Zajímavostí je využívání tzv. generátorů, což jsou programy, které dokáží vygenerovat číslo kreditní karty na základě zřejmě odcizeného algoritmu. V souvislosti se zdokonalením platebních systémů, kde se dnes ověřuje již nejen číslo platební karty, ale on-line verifikací přímo v bance

i faktická existence dotyčného účtu, není již dnes použití tohoto způsobu v mnoha případech možné.

Pachatelé cardingu získávali osobní údaje majitelů účtů různými pokoutnými způsoby. Oblíbeným bylo například zavolat majiteli účtu, kterému se představili jako pracovníci banky, která kartu k účtu vydala, a předstírali, že nastaly nepředvídané problémy v počítačovém systému a že je nutné, aby jim dotyčná osoba nadiktovala své osobní údaje, číslo karty, datum vypršení její platnosti atd. Použití takovýchto metod nemůže samozřejmě fungovat donekonečna. Potenciální oběti jsou čím dál tím méně důvěřivé, a proto se vymýšlí stále nové metody. Časté je například probírání odpadků a hledání vyhozených výpisů z bankovních kont.

S tím, jak se platební karty začaly používat pro nakupování po internetu, začaly se vyvíjet další, někdy velmi sofistikované metody jejich zneužití. Zejména v první polovině 90. let, kdy úroveň zabezpečení elektronických transakcí nebyla valná, se rozšířily případy, kdy si nepoctivý obchodník „strhnul“ z účtu více peněz, než jaká byla cena. Není náhoda, že podobné případy se dějí velmi často při platbách za služby jako například přístup na pornografické stránky, hraní v internetových kasinech apod., kde existuje velká naděje, že se oběť cardingu nebude příliš domáhat svých práv.

Typický cardingový útok vypadá tak, že se na cílovém účtu začnou objevovat podezřelé pokusy o transakci, kdy jakoby někdo testoval, jaký je na učtu zůstatek, a kolik je ještě banka schopna vyplatit. Toto "testování" probíhá tak dlouho, až je příkaz k platbě proveden.

Bezpečnost kartových transakcí na internetu stále není optimální a nejlepší ochrana před cardingem spočívá v opatrnosti uživatelů, kteří by v žádném případě neměli sdělovat informace týkající se svých platebních karet nikomu mimo okruh zvláště důvěryhodných obchodníků. Ani tak nelze ovšem riziko zneužití karty vyloučit, dojde nicméně k jeho minimalizaci.

4 Hacking

Vznik pojmu *hacking* či *hacker* (tj. ten, kdo provádí hacking) sahá zhruba do 70. let dvacátého století. Programátoři, kteří pracovali na tehdejších počítačích si často potřebovali poradit s nepříliš dobře fungujícím programem. Zásahy do programů, které je měly přimět k tomu, aby fungovaly lépe a efektivněji, se označovaly anglickým termínem *hacks*. Toto slovo je obtížně přeložitelné, doslova znamená *záseky*. Je zřejmé, že úloha tehdejších hackerů byla pozitivní, neboť vylepšovali programy. Postupně se toto označení začalo používat pro počítačové nadšence, kteří analyzovali systémy, aby zjistili, jak fungují, případně se snažili odhalit a napravit chyby, které se v nich vyskytovaly, nebo na ně alespoň upozornit. Na významovém posunu pojmu hacker měla a má nemalý vliv medializace problému.

Hacking v dnešním pojetí znamená proniknutí do počítačového systému jinou než standardní cestou, tedy při obejití nebo prolomení jeho bezpečnostní ochrany. Osoba provádějící hacking se nazývá hacker. Motivace hackera k jeho činnosti může být různá. V prvopočátcích hackingu se většinou jednalo o snahu zjistit, jak systém funguje, případně odstranit jeho chyby. Často také docházelo k hackingu proto, aby si hacker vydobyl ve své komunitě slávu a image tím, do jakého systému se mu podařilo nabourat. Hackeři tohoto typu neměli v úmyslu cílový systém jakkoli poškodit, a také k tomu, až na výjimky, nedocházelo. Časem ale došlo k nástupu nového typu hackerů, jejichž pohnutky jsou výrazně materiální, kdy účelem jejich činnosti je především obohatit se. Tito programátoři raději hledají trhliny v počítačových (ale také jiných komunikačních) systémech než by je spravovali. Ačkoliv se většina hackerů pokouší proniknout do systémů pro osobní požitek, existuje mnoho těch, kteří se podílejí na průmyslových a špionážních sabotážích. Ať už pro osobní zadostiučinění nebo pro jakékoliv průmyslové záměry, představují hackeři neobyčejné nebezpečí pro počítačovou síť připojenou k internetu.

4.1 Druhy hackerských útoků

Existuje několik základních typů útoků, které hackeři mohou vést na sítě připojené k internetu:

- útoky na hesla
- útoky založené na slídění v síti a „čmuchání“ v paketech
- útoky založené na předstírání IP adresy
- útoky založené na společenském plánování
- útoky založené na únosu sezení
- útoky s úmyslem využít zranitelnost technologie
- útoky založené na uhodnutí pořadového čísla

Útoky na hesla jsou historicky jedním z nejoblíbenějších způsobů přístupu k on-line sítím. Na začátku se hackeři pokoušeli nabourat do síťových systémů vkládáním jednoho přístupového jména a jednoho hesla. Hacker zkoušel heslo po heslu, dokud nezačalo fungovat. Hackeři ale velmi brzy přišli na to, že by mohli napsat jednoduché programy, které by zkoušely hesla na za ně. Tyto programy zpravidla cyklují a zkoušejí a vyzkoušejí všechna slova ze slovníku, ve kterém jsou uvedena potenciální hesla. Tyto rychlé automatizované útoky se staly známými jako slovníkově orientované útoky (dictionary-based attacks).

Tzv. „čmuchání“ v paketech je snad nejobtížnějším typem nabourávání sítí. Každý paket přenášený po internetu může putovat přes obrovské množství počítačů před tím, než dorazí ke svému cíli. Použitím čmuchala paketů mohou hackeři zachytit pakety (včetně paketů s uživatelskými jmény a hesly, přenosy čísel kreditních karet, pakety e-mailů atd.) cestující mezi jednotlivými místy na internetu. Když hacker zachytí paket, může ho otevřít a ukrást jméno počítače, uživatelské jméno a heslo přidružené k paketu.

Předstírání IP adresy (IP spoofing) těží ze způsobu adresování paketů, který používá protokol TCP/IP při přenosu. Počítače při přenosu dat z jednoho na druhý s každým přenosem uvádí také identifikaci odesílajícího a přijímajícího počítače. Když hackeři používají IP spoofing k napadení sítě, znamená to, že poskytují chybné informace o svém počítači. Stručně řečeno, hacker tvrdí, že je hostitelem v rámci interní sítě nebo jinak chráněné sítě, tím, že okopíruje TCP/lP adresu hostitele. To umožní hackerovi získat

vnitřní (ne však vnější) přístup k systému a systémovým službám. Kdysi namáhavou, časově náročnou práci tohoto útoku jsou dnes schopny provést automatické nástroje během 20 sekund a tím se z předstírání IP adresy stala jednoduchá záležitost.

Útoky založené na společenském plánování (social engineering) jsou častější a nebezpečnější v souvislosti s rostoucím počtem uživatelů, kteří jsou připojeni k internetu a sítím. Obvyklým příkladem společenského plánováni je pro hackera poslání e-mailu, který naznačuje, že hackerem je systémový administrátor. Často e-mail uživatele nabádá, aby poskytli své heslo e-mailem "administrátorovi", aby mohl pracovat na systému. Útoky založené na společenském plánování závisí na tom, kolik toho uživatelé ví o počítačích a sítích. Nejlepší ochranou je v tomto případě (ale také v řadě jiných) proškolení a poučení uživatelů.

Únos sezení (session hijacking) je poměrně populární útok, částečně proto, že únos sezení dovoluje jak import, tak export dat ze systému. Při tomto způsobu napadnutí "holýma rukama" najde útočník existující spojení mezi dvěma počítači, obecně serverem a klientem. Po vniknutí bud' přes nechráněný směrovač nebo nevhodný firewall může útočník detekovat příslušná čísla TCP/lP adres během výměny mezi počítači. Jakmile útočník získá adresu legitimního uživatele, unese uživatelovo sezení tím, že simuluje čísla adresy uživatele. Poté, co útočník unese sezení, odpojí hostitelský počítač legitimního uživatele a získá volný přístup k souborům, ke kterým může přistupovat legitimní uživatel.

Útoky s úmyslem využít zranitelnost technologie zahrnují některé útoky na bezpečné přístupy a také mnoho dalších. Každý větší operační systém je zranitelný. Některé jsou přístupnější než jiné. Na druhé straně, pravděpodobnost, že nějaký hacker objeví místo zranitelnosti, je velmi malá.

Uhodnutí pořadového čísla představuje nejjednodušší hackerský útok. Každý počítač na síti má jedinečnou IP adresu. Každý síťový počítač připojí ke všem vysílaným paketům cílovou IP adresu a jedinečné číslo nazvané pořadové číslo (sequence number). V rámci spojení TCP akceptuje přijímající počítač na druhé straně pouze pakety se správnou IP adresou a správným pořadovým číslem. Některá bezpečnostní zařízení, včetně směrovačů, povolují vysílání v síti pouze počítačům s určitými IP adresami.

Útok uhodnutím sekvenčního čísla TCP/IP využívá pro získání přístupu do sítě způsoby, kterými se v síti adresují počítače a řadí výměny paketů. Hacker hádá pořadové číslo TCP/lP v podstatě ve dvou krocích. V prvním kroku se pokusí určit IP adresu serveru, obecně bud' pozorováním paketů na internetu, zkoušením čísel uzlů po řadě nebo připojením se k uzlu webovským prohlížečem a hledáním jeho IP adresy ve stavovém řádku.

Hacker ví, že u jiných počítačů dané sítě bude část adresy stejná jako adresa serveru, pokouší se proto hledat takovou IP adresu, která mu umožní průchod směrovačem a zajistí přístup do sítě jako internímu uživateli. Například, jestliže má systém IP adresu 192.0.0.15, hacker, který ví, že v síti může být připojeno maximálně 256 počítačů, zkouší hádat všechna čísla, které reprezentuje poslední bajt této série. IP adresa vypovídá mimo jiné o tom, kolik počítačů je do sítě připojeno. V tomto případě nastavení dvou nevýznamnějších bitů (128+6=192) v nejvyšším bajtu indikuje, že síť je třídy C. Hacker nejdříve monitoruje pořadová čísla paketů procházejících mezi počítači této sítě. Pak se pokusí uhodnout následující pořadové číslo, které server vygeneruje, a poté předstírá toto číslo, čímž se vloží mezi server a uživatele. Jelikož má také IP adresu serveru, může hacker skutečně generovat pakety se správnými pořadovými čísly a správnými IP adresami, což mu umožní zachytit vysílání s uživatelem.

Jakmile získá hacker interní přístup do systému uhodnutím pořadového čísla, získává i přístup k veškerým informacím vysílaným komunikačním systémem serveru včetně souborů hesel, přihlašovacích jmen, důvěrných dat i jakýchkoliv jiných informací procházejících sítí.

4.2 Falšování webu

Při tomto druhu útoku vytvoří hacker přesvědčivou, nicméně falešnou kopii celého webovského uzlu. Falešný web vypadá stejně jako skutečný. Jinými slovy, falešný uzel obsahuje stejné stránky a odkazy jako skutečný uzel. Celý však podléhá řízení hackera, takže veškerá komunikace mezi prohlížečem oběti a webem jde přes hackera. Tento útok umožňuje hackerovi pozorovat nebo modifikovat všechna data jdoucí od oběti na

webovský server a navíc i řídit zpáteční provoz od serveru k oběti. Hacker má tedy mnoho možností.

V průběhu útoku hacker zaznamenává obsah stránek, které oběť navštěvuje. Když oběť vyplní HTML formulář, prohlížeč odešle tato data serveru. Jenomže mezi server a klienta je vložený hacker, který tak zaznamená všechny údaje vyplněné klientem. Kromě toho může hacker zaznamenat i data, kterými server odpověděl klientovi. Vzhledem k tomu, že většina on-line obchodů používá formuláře, hacker má možnost získat čísla účtů, hesla i jiné důvěrné informace, které oběť vloží do falešného formuláře.

Hacker může pozorování uskutečnit dokonce i v případě, že oběť navázala zdánlivě bezpečné spojení. Ať již zdánlivě bezpečné spojení používá SSL nebo S-HTTP, hacker může spojení zfalšovat. Jinými slovy, přestože prohlížeč oběti zobrazuje bezpečnostní ikonu (obvykle obrázek zámku nebo klíče), může se stát, že oběť vysílá přes nezabezpečené spojení.

Hacker je rovněž schopen modifikovat jakákoliv data, procházející v obou směrech mezi obětí a serverem. Když si například oběť objedná 100 kusů nějakého zboží, hacker může změnit jak číslo produktu, tak jeho množství, nebo adresu dodávky a nechat si tak poslat například 200 kusů téhož zboží na účet oběti. Hacker může modifikovat také data, která server vrací.

Hacker nemusí uchovávat obsah celého webu. Všechno je totiž dostupné on-line, takže v případě potřeby si hacker příslušnou stránku stáhne ze skutečného webu a uživateli pak poskytne falešnou kopii. Požadavek na stránku prochází strojem hackera, hacker tedy může vyhledat každou novou stránku, o kterou oběť požádá. Falšující server ve skutečnosti potřebuje uchovávat stažené stránky pouze v průběhu páchání útoku.

Prvním krokem hackera je přepsat všechny lokátory URL na některé webovské stránce tak, aby ukazovaly na server hackera místo na skutečný server. Předpokládejme pro tuto chvíli, že hackerův server je na doméně *hacker.cz*. Hacker přepíše URL tak, že například vloží *http://www.hacker.cz/* před každou adresu. Potom se například z adresy *http://www.abc.cz* stane *http://www.hacker.cz/www.abc.cz/*. Při návštěvě přepsané webové stránky vypadají falešné URL normálně. Klepne-li návštěvník takového webu na

odkaz *http://www.abc.cz*, prohlížeč ve skutečnosti požádá o stránku *http://www.hacker.cz*, protože touto adresou URL začíná. Zbytek URL řekne serveru hackera, odkud má vzít požadovaný dokument.

Poté, co hacker vyhledá požadovaný skutečný dokument, přepíše všechny URL v dokumentu stejným způsobem jako předtím. Jinými slovy doplní http://www.hacker.cz před každé URL na vyžádané stránce. Nakonec hackerův server poskytne přepsanou stránku prohlížeči.

Vzhledem k tomu, že na přepsané stránce ukazují všechny URL zpátky na hackerův server, pokud zvolíme další odkaz z nové stránky, hackerův server požadavek opět zachytí. Takto zůstane uživatel uvězněn ve falešném webu hackera a může donekonečna cestovat po odkazech, aniž by falešný web opustil.

Pokud bude vyplněn formulář na stránce falešného webu, bude to vypadat, jako by byl zpracován správně pravý formulář. Falešné formuláře fungují zcela přirozeně, protože práce s formulářem je integrována v základních webovských protokolech. Prohlížeč zakóduje vyplněný formulář jako HTTP požadavek a webovský server odpoví použitím obyčejného HTML. Ze stejného důvodu mohou hackeři falšovat kterýkoliv URL a kterýkoliv formulář. Stejně jako jdou požadavky na stránky přes server hackera, jdou tudy i formuláře vyplněné obětí. Hacker má tedy možnost pozměnit informace před odesláním skutečnému serveru tak, jak si bude přát. Změnit může i odpověď skutečného serveru.

Obzvlášť zákeřnou stránkou předstírání webu je to, že útok funguje i v případě požadavku stránky přes bezpečné spojení. Jestliže se například uživatel pokusí navázat spojení s bezpečným webem (použitím protokolu S-HTTP) přes falešný web, bude okno prohlížeče vypadat jako obvykle. Hackerův server dodá stránku a prohlížeč zapne indikátor bezpečného spojení. Prohlížeč informuje, že je bezpečně připojen k serveru, protože bezpečné spojení má. Naneštěstí je to bezpečné spojení se serverem hackera a ne s požadovanou webovskou stránkou.

Zahájení útoku vyžaduje akci ze strany oběti. Aby mohl útok začít, hacker musí nějakým způsobem oběť do falešného webu vlákat. Jinými slovy musí hacker zajistit, aby obět klepla myší na falešný odkaz.

Hacker může zpřístupnit falešný odkaz velmi snadno, například následujícími metodami:

- Hacker vloží odkaz na falešný web do oblíbené webovské stránky.
- Pokud oběť používá e-mail s nastaveným prohlížečem, hacker může oběti zaslat odkaz na falešný web e-mailem.
- Alternativně může hacker e-mailem zaslat oběti obsah stránky falešného webu.
- Hacker může přelstít některý vyhledávácí stroj webu tak, aby do indexování zařadil i část falešného webu.

Oběti však musí zůstat v přesvědčení, že jsou pořád ve skutečném webu. Pokud není hacker dostatečně opatrný nebo pokud má prohlížeč některé funkce zablokované, mohou falešné stránky zobrazit ve stavovém řádku jisté prozrazující informace.

Údaje o stránce mohou poskytnout náznaky, aby si uživatel uvědomil, že vstupuje do falešného webu. Například pokud najede kurzorem myši nad odkaz, většina prohlížečů zobrazí ve stavovém okně absolutní adresu odkazu. Naneštěstí může zručný hacker využít jisté programovací techniky a eliminovat všechny ostatní příznaky útoku. Díky snadnosti uživatelského přizpůsobování prohlížečů je poměrně snadné důkazy útoku eliminovat. Schopnost stránky řídit chování prohlížeče je často žádoucí, ovšem pokud je stránka nepřátelská, může být řízení prohlížeče stránkou pro uživatele nebezpečné.

Útok může prozradit i řádek Location (Adresa), zobrazuje totiž URL právě prohlížené stránky. Zapsáním URL do tohoto řádku uživatel prohlížeči nařídí vyžádání zdroje s danou adresou. Většina uživatelů si přepsaného URL v informačním řádku nejspíš všimne. A pokud si ho všimne, uvědomí si pravděpodobně i probíhající útok. I v tomto řádku je možno ukrýt modifikovaný URL přidáním speciálního programu na server, který útok provádí. Program nahradí skutečný řádek falešným, který vypadá správně. Falešný řádek pak ukazuje informaci, kterou oběť očekává.

Většina rozšířených prohlížečů obsahuje možnost prohlížení zdrojového HTML textu zobrazené stránky. Nápaditější oběti tak při podezření na

uvíznutí ve falešném webu mohou prozkoumat zdrojový kód a vyhledat přepsané lokátory. Pokud se objeví, útok je odhalen. Avšak i proti tomu se může hacker bránit vloženým programem, který ukryje nabídkový řádek prohlížeče a nahradí ho řádkem, který vypadá naprosto shodně s původním. Ovšem při výběru "Zobrazit zdrojový kód" otevře hacker nové okno, ve kterém zobrazí původní (nepřepsaný) HTML zdroj.

Poslední stopou, kterou může oběť využít, je informace o dokumentu. V nabídce prohlížeče je položka View Document Information, která umožňuje prohlížet informace týkající se zobrazeného dokumentu. Tyto informace obsahují i URL dané stránky. Stejným způsobem jako u položky View Document Source může hacker nahradit informace o dokumentu použitím falešného nabídkového řádku. Pokud hacker vytvoří novou nabídku, zobrazí se pak příslušné dialogové okno se zmanipulovanou informací.

Stručně řečeno, hacker může potlačit všechny signály, které by oběti prozradily, že je připojená k falešnému webu. Jedinou obranou proti útoku je zablokování skriptových jazyků v prohlížeči.

Jediným odrazujícím prostředkem proti falšování webu je vystopování hackera a jeho potrestání. Pokud oběť útok detekuje, umístění serveru bude téměř určitě možné zjistit. Naneštěstí jsou tyto útoky prováděny z ukradených počítačů.

Falšování webu je nebezpečný a téměř nezjistitelný útok na bezpečnost. Naštěstí existují jistá preventivní opatření, která můžete podniknout pro svou ochranu nebo ochranu své sítě před tímto útokem. Nejlepší ochranou je uplatnit následující tříbodovou strategii:

1. Ve svém prohlížeči vypnout Javu, JavaScript a VBScript, aby hacker nemohl skrývat příznaky útoku.
2. Ujistěte se, že řádek s informací o umístění (Adresa, Location) je pořád viditelný.
3. Věnovat pozornost URL, který prohlížeč zobrazuje a ujistit se, že ukazuje na server, o kterém si uživatel myslí, že je k němu připojen.

Zatímco jsou krátkodobá řešení poměrně jednoduchá a mocná, vypracování uspokojivého dlouhodobého řešení je úkol mnohem obtížnější.

Řešení většiny problémů vyžaduje zásah ze strany výrobců prohlížečů. Například zajištění prohlížeče před externí modifikací - to znamená nedovolit hackerům vytvářet falešné stavové řádky, nabídky a podobně. K zajištění bezpečnosti by mohl přispět i zdokonalený indikátor bezpečného spojení. Místo toho, aby pouze indikoval bezpečné spojení, měl by jasně zobrazovat jméno serveru, se kterým bylo bezpečné spojení dokončeno. Informace o spojení by měla být vyjádřená jednoduchým jazykem způsobem, kterému rozumí i začátečníci.

5 Viry

Pro sítě připojené k internetu představují jedno z největších externích bezpečnostních rizik viry. Jejich množství stále narůstá a jejich tvůrci vymýšlejí stále nové metody a techniky.

Virus je program, který se od běžných programů liší především tím, že je schopen se sám množit a šířit, vykonává akce nezávisle a bez vědomí uživatele (ať už destruktivní nebo neškodné), není schopen samostatné existence – musí mít nositele (napadený soubor). Obecně platí, že přítomnost jakéhokoliv viru je v počítači nežádoucí a může vždy způsobit problémy.

5.1 Druhy virů

Existuje několik základních typů virů. Žádné členění však není vyčerpávající a přesné, protože mohou vznikat některé nové typy nebo jejich podskupiny. Nejdůležitější typy virů jsou:

- **Souborové** – Napadají zejména spustitelné soubory (.exe, .com, .vbs…).
- **Makroviry** – Napadají dokumenty MS Office (.xls, .doc, .mdb).
- **Boot viry** – Napadají boot sektor na disku (na tomto místě se nachází jádro operačního systému).
- **Rezidentní viry** – Sídlí v operační paměti a kontroluje diskové operace. Nejčastěji se zavedou do paměti při startu PC (boot viry).
- **Stealth** – Maskují se před antivirovým programem.
- **Polymorfní** – Mění svůj kód v závislosti na situaci. A velmi složitě se odhalují.
- **Červi** – Nová generace virů. Jedná se o viry, které se šíří internetem, téměř výhradně v přílohách e-mailu.

5.2 Projevy počítačových virů

Blokování místa – Tělo viru musí být někde uloženo. To lze považovat za první škodlivý projev viru. Obsazuje část volného místa na discích a v paměti, které by při jejich nepřítomnosti bylo prázdné. Při dnešních kapacitách disků a paměti tato vlastnost nepatří mezi nejvýznamnější.

Zpomalení systému – Každý virus při svém šíření, aktivaci apod. alokuje část zdrojů systému. Zatížení může být značné například tehdy, pokud virus začne automaticky rozesílat elektronickou poštou zprávy všem adresátům z adresáře nebo vyvíjet jinou automatickou činnost.

Vypsání textu, zvukové projevy viru – Viry mnohdy po své aktivaci vypisují hlášení o své přítomnosti nebo se snaží na sebe upozornit dalšími audiovizuálními efekty.

Nestabilita systému – Protože virus není nic jiného než program, mohou se vyskytnout situace, kdy se díky jeho nekompatibilitě s konkrétním prostředím (jiná verze operačního systému, nestandardní programy, speciální ovladače apod.) jeho přítomnost projeví i tím, že některé programy začnou být ne vlastní vinou méně stabilní. To se projevuje např. častým zhroucením konkrétní aplikace nebo služby, případně zablokováním celého systému. Z těchto projevů však obecně nelze vyvodit přítomnost viru.

Krádež dat – Pokud je počítač připojen k internetu, mohou viry odesílat soubory obsahující důvěrné informace prakticky komukoli na světě.

Šifrování dat – Protože virus má obecně pod kontrolou souborový systém infikovaného počítače, může například začít nenápadně šifrovat data na disku a při přístupu k nim je automaticky dešifrovat tak, aby nebylo nic poznat. V určité chvíli pak může virus data najednou znepřístupnit.

Zničení dat – Počítačový virus může jakkoli mazat či modifikovat data na disku. Jsou známy viry, které například začnou mazat systémové oblasti disku, FAT tabulky, celé oddíly disku nebo například programovatelný FlashBIOS.

5.3 Technologie pro detekci virů

Technologií pro odhalování virů je celá řada. Bohužel neexistuje ani jedna, která by byla 100% účinná na všechny existující viry. V následujících kapitolách jsou shrnuty a popsány základní druhy technologií používaných pro detekci virů.

5.3.1 Skenování na základě řetězců

Na této technologii je založena většina dnešních antivirových programů. Princip je jednoduchý. Antivirový program obsahuje vzorky známých virů uložených v databázi virových signatur, tedy sekvence charakteristické pro konkrétní viry. Antivirový program při skenování souborů speciálními rychlými algoritmy vyhledává tyto vzorky v kontrolovaných souborech. Protože tvůrci virů jsou velmi vynalézaví a tuto jednoduchou techniku hledání virů znají, snažili se detekci touto metodou znemožnit. Vymysleli tzv. polymorfní viry, které při svém šíření mají schopnost modifikovat sami sebe tak, aby každá jejich kopie byla jiná. Kód viru se jednoduše zakóduje pomocí tzv. polymorfní smyčky za použití náhodně vygenerovaného klíče. Antivirové programy se proto snaží odhalit tyto polymorfní smyčky a rozbalit je. Teprve po jejich dekódování je jejich obsah prozkoumáván skenováním na základě řetězců. Nevýhodou této metody je, že dokáže vyhledat pouze známé viry - tj. viry, jejichž vzorek je uložen v databázi virových signatur. Tato databáze musí být však často aktualizována. Dalším problémem je, že každá nová modifikace viru způsobí nový záznam v databázi virových signatur, čímž tato databáze velmi rychle roste a není jednoduché ji udržovat. Výhodou této techniky je však přesná identifikace, neboť prakticky neexistují falešná hlášení. Další velmi významnou vlastností antivirových programů založených na této technologii je, že po detekci určitého viru umožňují i jeho odstranění z počítače (to samozřejmě nemusí jít v každém případě).

5.3.2 Heuristická analýza

Je to analýza založená na kontrole programového kódu s ohledem na sekvence typické pro viry. Tato technika je velmi obtížná na naprogramování. Vyžaduje totiž naprogramování tzv. virtuálního stroje, tj.

softwarově simulovaného procesoru, který simuluje vykonávání instrukcí skenovaného programu. Tato technika byla používaná na 16-bitové programové viry. Pro 32-bitové souborové viry se však dodnes takovýto virtuální stroj nepodařilo sestrojit. Obrovskou, ale bohužel jedinou výhodou této metody je to, že heuristická analýza bez aktualizací detekuje i doposud neznámé nové viry. Největším problémem této metody je, že sekvence typické pro viry mohou obsahovat i běžné programy, například pro optimalizaci výkonu počítače. Po nasazení této metody proto dochází k tzv. falešným hlášením, tj. situacím, kdy heuristická analýza vyhodnotí běžný program jako podezřelý a vehementně tuto myšlenku vnucuje uživateli. Antivirové programy využívající heuristické analýzy proti falešným hlášením obvykle bojují seznamem výjimek, tedy databází běžných programů obsahujících tyto speciální sekvence, které nebudou programem hlášeny.

5.3.3 Kontrola integrity

Tvůrci této technologie uvažovali následujícím způsobem: protože každý virus při svém šíření modifikuje své hostitele, stačilo by přece detekovat změny v souborech. Programy tedy po své instalaci spočítají kontrolní součty pro jednotlivé soubory (čísla, která jsou jedinečná pro daný obsah souboru) a ty uloží do speciálních souborů. Antivirová kontrola poté spočívá v opětovném spočítání kontrolního součtu a jeho porovnání s původně zaznamenaným. Problémy této metody jsou jasné. Metoda je nepoužitelná pro vyhledávání makrovirů, protože práce s dokumenty vyžaduje jejich změnu. Ale problémy jsou i u spustitelných souborů, které si někdy přímo do svého těla zapisovaly například nastavování programů. Další nevýhodou je to, že tato metoda není schopna pojmenovat viry, ale jen zjistit, které soubory jsou modifikovány. Metoda kontroly integrity se obvykle používá jako doplňková spolu s jinými metodami - je zbytečné skenovat soubor např. časově náročnou heuristikou, pokud se jeho obsah nezměnil.

5.4 Antivirové programy

Všechny dnes prodávané antivirové programy se skládají ze dvou základních částí - *antivirového motoru (engine)* a *aplikační části*. Antivirový motor je jádro programu založené na některé z technologií popsaných výše. Jeho úkolem je po obdržení přístupu ke konkrétnímu souboru rozhodnout, jestli obsahuje virus, a pokud ano, tak jaký. Pokud je motor založen na vyhledávání na základě řetězců, pak k motoru patří také databáze virových signatur, kterou je nutné pravidelně aktualizovat. Aplikační část antivirového programu se stará o předkládání souborů ke skenování motoru (například také o rozbalování komprimovaných souborů). Obvykle bývá složena ze dvou základních částí:

On-demand skenování se může také nazývat skenování na požádání či off-line skenování. Spočívá v kontrole vybraných souborů na přímou výzvu uživatele. Většina antivirových programů umožňuje definici úkolů pro toto skenování - např. skenování všech lokálních pevných disků nebo skenování diskety. Po spuštění úkolu aplikační část prochází všechny soubory definované úkolem (například všechny soubory na lokálním pevném disku) jeden po druhém a předkládá je motoru. Ten rozhodne o tom, jestli obsahují virus nebo nikoli. Výsledky kontroly program předkládá uživateli. Prakticky všechny dnešní antivirové programy umožňují nastavování automatického spouštění definovaných "úkolů" - např. po každém spuštění počítače, pravidelně jednou za týden nebo pokaždé po určité době nečinnosti počítače (podobně jako se spouští šetřiče obrazovky). Pokud antivirový program skenuje na základě řetězců, je vhodné nastavit on-demand skenování tak, aby se spustilo vždy po každé aktualizaci databáze virových signatur. Jedině tak je možné okamžitě odhalit nové viry, které přibyly od předchozí verze.

On-line skenování se také nazývá rezidentní ochrana. Je založena na jednoduché myšlence, která předpokládá, že nejlepší okamžik pro antivirovou kontrolu je těsně před použitím podezřelého souboru. A proto tvůrci antivirových programů vytvářejí pro jednotlivé operační systémy ovladače, které se napojují přímo na souborový systém a mají ho plně pod kontrolou. Před každým požadavkem aplikace na otevření souboru

předloží ovladač těsně před povolením jeho otevření soubor antivirovému motoru, který rozhodne o jeho čistotě. Pokud je soubor vyhodnocen jako čistý, je jeho otevření povoleno. Protože při běžné uživatelské práci se často otevírají obvykle stále tytéž soubory (např. spuštění aplikace typu MS Word vyvolává otevírání desítek nezměněných souborů), snaží se antivirové programy kontrolovat pouze ty soubory, které se od poslední kontroly změnily. Tak se sníží zatížení systému způsobená zapnutím on-line antivirových mechanismů.

5.4.1 Komponenty antivirových řešení

Protože v praxi se používá celá řada různých operačních systémů i různé uspořádání sítí, podívejme se nyní na jednotlivé komponenty antivirových řešení.

Zabezpečení stanic

Všechny firmy zabývající se antivirovou problematikou obvykle mají v této oblasti co nabídnout. Jedná se o programy vybavené jak on-line, tak i on-demand technologií. On-line technologie zde však obvykle kontroluje pouze přístupy na disk, o něž žádají programy pocházející přímo z této stanice a ne ze sítě. To může způsobit určité rozčarování pro uživatele malých sítí typu peer-to-peer, kde nejsou antivirové prostředky nasazeny na všech stanicích. Dalším problémem je, že pro každý operační systém používaný na stanicích musí být takovýto program vyvinut zvlášť. Velcí antiviroví producenti nabízejí řešení pro DOS, Windows, ale i pro další platfromy, jako jsou OS/2 nebo stanice typu Macintosh. Rozdíly mezi těmito produkty nalezneme v možnostech jejich centralizované instalace v rámci lokální sítě, jejich síťové správy a například v možnosti centralizované sumarizace výsledků kontroly u zodpovědné osoby. Nejnovější antivirové programy pro stanice umožňují mimo ochrany souborového systému také kontrolu souborů připojených k přijímané elektronické poště nebo souborů stažených pomocí FTP a kontrolu Java appletů či ovládacích prvků ActiveX.

Zabezpečení souborových serverů

Tato řešení jsou taktéž založena na on-line a on-demand skenování souborů, ale tentokrát ukládaných na souborové servery. Na rozdíl od řešení pro stanice však kontrolují i soubory ukládané nebo čtené ze serveru

okolními stanicemi. Výrobci obvykle poskytují řešení pro všechny běžné systémy používané na serverech (Windows 2000, Novell NetWare, Unix…).

Zabezpečení souborů elektronické pošty

Jedním z mýtů o virech je, že se mohou šířit prostřednictvím zpráv elektronické pošty a uživatel může spustit virus pouhým otevřením určité zprávy. To však v žádném případě není pravda. Při otevírání zpráv se nevykonává žádný spustitelný kód, který by byl připojen ke zprávě. Jedinou metodou, jak je možné obdržet virus prostřednictvím elektronické pošty, je pomocí souboru připojeného ke zprávě. Protože tento soubor může být jakéhokoli typu, může to být i typ, který je hostitelem viru. Proto vznikají antivirové programy, které se snaží zajistit kontrolu připojených souborů už na straně serveru a zavirované zprávy pokud možno virů zbavit. Tato řešení kontrolují jak příchozí/odchozí poštu, tak veškerou vnitropodnikovou poštu. Podle použitého principu lze rozlišit dvě základní řešení. Plug-in modul, který se zasune přímo do poštovního serveru a který umožňuje on-line i on-demand skenování složek s poštou. Problémem je, že toto řešení je vždy určené pro konkrétní typy poštovních serverů. Dnes jsou tyto moduly implementovány pro MS Exchange a Lotus Notes, kde jsou schopny odhalovat i groupwarové viry. Typickým představitelem takového řešení je například produkt GroupShield firmy Network Associates. Obecné řešení, napojující se na obecnou bránu SMTP. V tomto případě je řešení nezávislé na konkrétním poštovním serveru. Představitelem takového programu je například WebShield SMTP opět od firmy Network Associates.

Zabezpečení vstupních bodů do internetu

Je důležitým úkolem pro antivirové programy. Z internetu se mohou šířit prakticky všechny jmenované typy virů, tj. programové, makroviry, škodlivé applety Javy nebo ActiveX i speciální viry. Proto je vstupní brána do internetu téměř ideálním kandidátem pro antivirovou kontrolu. S připojením na internet je však spojen i jiný problém - zajištění bezpečnosti dat v lokální síti před útočníky z internetu. Pro tento případ se zavede firewall, který podle předem definovaných pravidel "hlídá" komunikaci s okolním světem (firewally se zabývá kapitola 7). A odtud už je jen krůček ke spojení obou služeb - bezpečnostní i antivirové. Proto byla do nastavení firewallu doplněna funkce CVP umožňující zasílat všechna data, která procházejí přes

firewall, antivirovému programu. Ten je analyzuje se zřetelem na přítomnost virů a pokud jsou v pořádku, tak je zašle zpět na firewall, který je dále propustí do vnitřní sítě nebo do světa. Na firewallu lze kontrolovat soubory připojené k elektronické poště, soubory přenášené protokolem FTP nebo Java applety a ActiveX, které mohou obsahovat škodlivé kódy. Velkou výhodou celého řešení je nezávislost výrobců firewallu na producentech antivirového software. Jedinou podmínkou je přítomnost služby CVP na firewallu. Představme si například situaci, že zpráva elektronické pošty obsahuje připojený soubor napadený virem. Zpráva je při průchodu firewallem pomocí CVP technologie zaslána antivirovému programu, který zprávu zkontroluje. Pokud je virus odstranitelný, může být soubor automaticky "vyléčen" a zaslán zpět na firewall, který jej doručí adresátovi. Pokud virus nelze odstranit, bude e-mail zadržen a přesunut do karantény až do doby, kdy administrátor rozhodne, jak s ním naložit. Kromě toho lze antivirový program nastavit tak, aby po rozeznání viru v elektronické poště automaticky zaslal upozornění odesílateli. Přestavitelem tohoto druhu softwaru může být například F-Secure Antivirus pro firewally od firmy DataFellows.

6 Šifrování a autentizace

Kdyby se nemuselo používat šifrování, bylo by to samozřejmě daleko jednodušší, nicméně šifrování pomáhá významným způsobem zajišťovat bezpečnost a ochranu dat. Šifrováním jsou chráněna data pro případ odcizení hardware, dat či hackerského útoku, kdy přesto, že se nepovolaná osoba zmocní citlivých dat, nebudou pro ni mít v zašifrované podobě žádný význam. Zároveň lze pomocí šifrování zajistit kontrolu přístupu k datům, kdy se stanoví jasná pravidla, kdo má k jakým informacím přístup. V neposlední řadě je důležité, že člověk používající šifrování zvyšuje svou vlastní důvěryhodnost, neboť dává okolí jasný signál, že dbá na ochranu citlivých údajů a informací.

6.1 Šifrovací systémy

Každý, kdo manipuluje s daty v elektronické podobě, by měl mít zájem na tom, aby data byla přístupná a čitelná jen oprávněným osobám. K zajištění nečitelnosti elektronických dat pro neoprávněné osoby nebo útočníky se používá *šifrování*. Zašifrování změní dokument z čitelného textu na sled znaků, který může rozluštit jen ten, kdo zná dešifrovací klíč.

6.1.1 Symetrické šifrování

Symetrické (neboli souměrné) šifry používají stejný šifrovací klíč jak pro proces šifrování dat, tak pro jejich uvedení do původní podoby, tedy dešifrování. Výhodou symetrického šifrování je potřeba pouze jednoho jediného klíče, který se používá ke všem úkonům se zpracovávanými daty. S tím souvisí také vyšší rychlost práce počítačů při šifrování a dešifrování. Tato výhoda se ovšem stane nevýhodou ve chvíli, kdy dojde k prozrazení tohoto klíče, neboť tím jsou odkryta všechna zašifrovaná data.

Mezi nejznámější symetrické šifry patří následující algoritmy:

- **DES** – Byl vyvinutý v laboratořích IBM v sedmdesátých letech, v roce 1977 se stal americkou vládní normou pro šifrování. Používá klíče, který má délku 56 bitů. Vzhledem k vývoji výkonu

výpočetní techniky se za poslední dvě desetiletí přestává již DES dostačovat současným požadavkům. Tuto šifru se podařilo rozluštit, a to za pomoci tzv. útoku „hrubou silou“ (tedy zkoušením všech možných kombinací).

- **3DES (Triple-DES)** – Jde o zesílenou variantu algoritmu DES, při jejímž použití jsou data šifrovaná algoritmem DES třikrát přešifrována. Triple-DES pracuje s klíčem dlouhým 112 nebo 168 bitů. Při použití 112 bitového klíče jsou data šifrována tak, že je z klíče vzata první polovina a data jsou jí přešifrována. Poté jsou druhou polovinou klíče data zašifrována podruhé. Následně jsou data potřetí zašifrována první částí klíče.
- **IDEA** – Algoritmus s klíčem dlouhým 128 bitů, který se vyznačuje vysokou rychlostí. V porovnání s DES je při nesrovnatelně vyšším stupni bezpečnosti několikanásobně rychlejší.
- **BlowFish** – Algoritmus s proměnnou délkou klíče, a to od 32 do 448 bitů. Obvykle se používá 128 bitový klíč. BlowFish je poměrně rychlý a bezpečný, navíc jej lze volně užívat, není ani patentovaný.
- **CAST** – Rychlostní i bezpečnostní charakteristikou je velmi podobný výše uvedenému algoritmu BlowFish. Obvykle se používá s délkou klíče 128 bitů, jsou ale možné i jiné varianty.

6.1.2 Asymetrické šifrování

Při tomto způsobu šifrování jsou používány dva klíče – jeden pro šifrování a jeden pro dešifrování. Při generování klíče pomocí specializovaného software se jedná o jeden klíč, který je posléze rozdělen na dvě částí. Tou první je tzv. *veřejný klíč*, který případný příjemce poskytne všem odesílatelům, od kterých chce dostávat šifrovaná data. Druhou částí je *soukromý (privátní) klíč*, který je tajný a zná ho jen jeho držitel. Pokud někdo získá přístup k privátnímu klíči, dostane se k datům, která měla být chráněna šifrou. Privátní a veřejný klíč dohromady tvoří klíčový pár.

Přesto, že veřejný klíč může mít k dispozici prakticky kdokoliv, nelze z jeho znalosti odvodit klíč privátní. Asymetrické šifrovací algoritmy totiž

používají takové matematické postupy, jejichž reverzní funkce je neproveditelná (při současném stavu vývoje). Data může veřejným klíčem zašifrovat kdokoliv, nicméně dešifrovat a přečíst tato data může pouze držitel privátního klíče.

Mezi nejznámější asymterické šifry patří následující algoritmy:

- **RSA** – Algoritmus pro výměnu klíčů a tvorbu digitálního podpisu, který patří mezi neoficiální standardy. Bezpečnost algoritmu RSA je založena na skutečnosti, že je velmi obtížné rozložit velká čísla, z nichž každé je součinem dvou velkých prvočísel. Velmi však záleží na délce použitého klíče. Pokud má délku 384 bitů, je rozluštitelný poměrně snadno. Jako dostatečné se díky rychlému vývoji možností výpočetní techniky nejeví ani 768 bitové klíče. Při současném stavu je reálné používat klíče o délce 1024 bitů, do budoucna pak 2048 bitů.
- **ECC (Eliptické kryptosystémy)** – Jedná se o moderní algoritmy založené na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. Jejich hlavní výhodou je značná bezpečnost při použití poměrně krátkého klíče. K dosažení stejné bezpečnosti jako RSA s délkou klíče 2048 bitů, potřebují šifrovací algoritmy ECC klíč dlouhý 160 až 180 bitů.

6.2 Digitální podpis

Digitální podpis je prostředek k zajištění elektronické autentizace autora (podepisovatele) a integrity podepisovaných dat. V souvislosti s elektronickou autentizací se často objevuje také termín elektronický podpis. Elektronický podpis je poněkud širší termín zahrnující obecnější elektronické metody prokázání totožnosti. Digitální podpis je speciálním případem elektronického, kdy dochází k ověření původu dokumentu na bázi šifrování. V podstatě se jedná o implementaci určité matematické funkce prostřednictvím specializovaného programu, jejímž připojením k určitému dokumentu dochází k ověření jeho pravosti.

Digitální podepisování probíhá tak, že se pomocí jednocestné hash funkce vytvoří tzv. otisk zprávy, který je zašifrován soukromým klíčem

a přidán k této zprávě. Příjemce dešifruje získaný zašifrovaný otisk veřejným klíčem a opět za pomoci hash funkce vygeneruje z datového souboru nový otisk, přičemž oba porovná. V případě, že jsou totožné, je zřejmé, že nedošlo k žádné modifikaci zasílaných dat a odesílatel byl identifikován a ověřen. Pokud ověření pravosti nesouhlasí, znamená to, že data byla někým modifikována či s nimi bylo nějakým způsobem manipulováno. Digitální podpis v takovém případě pozbývá platnosti.

V praxi jsou digitální podpisy používány převážně ve spojení s elektronickou poštou. Časté je také digitální podepisování souborů stahovaných pomocí FTP. Dalším způsobem využití je například podepisování částí programových kódů. Výrobci software se takto chrání před porušováním autorského zákona, který zakazuje komukoli mimo autora zasahovat do jeho díla.

S digitálními podpisy souvisí také problém záruky, zda nabízený veřejný klíč, který se použije k šifrování dat, skutečně náleží osobě, jíž jsou informace a data určena. Tento problém řeší *certifikační autority*, které potvrzují vazbu mezi totožností uživatele a jeho veřejným klíčem. Certifikační autorita je nezávislý subjekt zabývající se vydáváním a správou digitálních *certifikátů*, který podepisuje svým soukromým klíčem veřejný klíč žadatele o vydání digitálního certifikátu. Pokud chtějí poté dva subjekty spolu bezpečně komunikovat, mohou navzájem prověřit svou identitu prostřednictvím certifikační autority. Poté stačí důvěřovat veřejnému klíči certifikační autority.

6.2.1 Certifikáty

Certifikát je listina svazující fyzickou totožnost subjektu s jeho veřejným klíčem. Pomocí certifikátu je možné identifikovat subjekty v elektronické komunikaci. Základním údajem certifikátu je veřejný klíč certifkovaného subjektu, který je digitálně podepsán klíčem certifikační autority. Kromě veřejného klíče jsou součástí certifikátu i informace o subjektu, kterému certifikát patří. Tyto informace pak umožňují příjemci certifikátu rychlou identifikaci jeho vlastníka, neboť jeho veřejný klíč je jen nevypovídající shluk bitů. Obecně používané certifikáty

obsahují rovněž dobu vypršení platnosti, jméno certifikační autority, která certifikát vydala a pořadové číslo.

O certifikát je možné požádat osobně u certifikační autority nebo elektronickou formou na její webové stránce. Podle typu žádosti a úrovně identifikace dostane pak certifikát vyznačení patřičné úrovně důvěry-hodnosti. Autentizace uživatele při podání elektronické žádosti se provádí pomocí poštou zaslaných kopií identifikačních dokumentů, které musí být notářsky ověřené.

Certifikáty jsou rozděleny do několika kategorií – od těch s menší váhou až po ty s vyšším stupněm důvěryhodnosti:

- **Class 1 Trial** – Tato úroveň je vydávána pouze pro testovací účely, přičemž certifikáty jsou platné pouze po limitovanou dobu. Certifikační autorita neposkytuje žádnou záruku na používání těchto certifikátů. Jejich použití a údaje v nich uvedené jsou plně na odpovědnosti žadatele. Takovéto certifikáty jsou bezplatné.
- **Class 1** – Tato úroveň je užívána pro aplikace, které zpracovávají informace poměrně nízké hodnoty v prostředích, která se vyznačují nízkou úrovní rizika. Certifikáty této úrovně nezajišťují podrobnosti o svém vlastníkovi, při jejich vytváření je pouze kontrolována všemi dostupnými prostředky existence e-mailové adresy. Žadatelovy informace uvedené v certifikátu, jako je jméno a ostatní registrační informace, jsou považovány za neověřené. Tyto certifikáty poskytují nejnižší stupeň důvěry. Nejsou určeny pro komerční použití v případě nutnosti prokázat svoji totožnost. Jejich účel je především použití pro osobní potřebu. Certifikační autorita na tyto certifikáty neposkytuje (stejně jako na Class 1 Trial) žádné záruky.
- **Class 2** – Tato úroveň je užívána pro aplikace, které zpracovávají informace nízké hodnoty v prostředích, která se vyznačují nízkou nebo střední úrovní rizika. Při vytváření certifikátu je ověřováno, zda neobsahuje informace, které by byly v rozporu s kopií občanského průkazu, řidičského průkazu či cestovního pasu. Tyto certifikáty poskytují přijatelné ověření identity jejich vlastníka, které je založeno na porovnání s podepsanou kopií

identifikačního dokumentu. Při používání certifikátu je třeba brát v úvahu způsob jeho vytvoření a z toho vyplývající omezení.

- **Class 3** – Tato úroveň je užívána pro aplikace, které zpracovávají informace střední a vysoké hodnoty v prostředích, která se vyznačují nízkou nebo střední úrovní rizika. Při vytváření tohoto certifikátu je vyžadována fyzická přítomnost budoucího vlastníka u certifikační autority a předložení identifikačních dokladů. Certifikáty Class 3 se vydávají jak osobám, tak organizacím, přičemž za certifikát vydaný organizaci je zásadně zodpovědná jediná osoba, oprávněná za organizaci jednat a podepisovat se, jejíž jméno je uvedeno v certifikátu a která se také identifikuje vůči registrační autoritě. Certifikát této kategorie je možno použít pro bezpečný elektronický obchod, pozitivní identifikaci jeho uživatele, k bankovním transakcím apod.
- **Class 4** – Tato úroveň je vyžadována pro aplikace, které zpracovávají informace střední hodnoty v prostředí s vysokou úrovní rizika. Certifikáty vydané v této třídě poskytují nejvyšší možné ověření identity jejich vlastníka. Při vydávání certifikátu je třeba, aby se budoucí vlastník dostavil do pobočky certifikační autority a předložil požadované dokumenty, u nichž mohou být vyžadovány další vlastnosti (minimální zbývající délka doby platnosti apod.). Je požadováno předložení rodného listu. Příslušné klíče jsou uchovávány v hardwarových zařízeních.
- **Class 5** – Tato úroveň je stanovena pro aplikace, které zpracovávají informace vysoké hodnoty v prostředích, která se vyznačují vysokou mírou rizika. Požadavky na identifikaci jsou stejné jako u Class 4. Dalším požadavkem je ovšem použití hardwarových modulů pro provádění kryptografických operací.

Většina bezpečnostních programů umožňuje také vytváření tzv. *Self-Signed Certificate*. Jedná se o certifikát, který jeho vlastník podepíše sebou samým. Veřejný klíč a připojené informace nejsou podepsány ani ověřeny žádnou z certifikačních autorit, ale pouze uživatelem samotným. Význam takového podpisu spočívá pouze v kontrole integrity samotného certifikátu.

Důvěryhodnost takovéhoto certifikátu, pokud jeho vlastníka neznáme a nejsme schopni jeho totožnost ověřit osobně, je nulová.

6.3 Autentizace

Pojem autentizace úzce souvisí s pojmem *identifikace*. V oboru počítačové bezpečnosti se identifikací rozumí neověřené prohlášení (osoby, počítače, programu apod.) o své identitě. Příkladem může být přihlášení uživatele do počítače, do lokální sítě nebo informačního systému pod svým uživatelským jménem, zkratkou apod. Naproti tomu *autentizace* je proces ověření, zda přihlašovaný uživatel je skutečně tím, za koho se prohlašuje. Často je však autentizace chápána jen jako kladný výsledek procesu ověřování. Pojmy identifikace a autentizace bývají občas směšovány nebo zjednodušeně nazývány buď jen identifikací nebo jen autentizací. K tomu přispívá fakt, že v mnohých elektronických systémech není oddělení obou činností jasně viditelné.

Příkladem identifikace je vložení jména (identifikátoru) na výzvu *login:* při přihlašování do sítě. Jiným příkladem může být vložení platební karty do bankomatu (člověk vkládající kartu se identifikuje jako vlastník této karty).

Autentizace probíhá tak, že něco, co je subjektem předkládáno jako důkaz identity (autentizátor) se porovnává s něčím, co je autentizačnímu zařízení o autentizovaném subjektu známo.

Autentizace osob se tedy dá provádět zejména na základě:

- určité znalosti (heslo, klíč)
- vlastnictví nějakého předmětu (mechanického klíče, magnetické karty, čipové karty)
- určité fyzické vlastnosti uživatele (otisk prstu, obraz očního pozadí).

6.3.1 Hesla

Heslo je řetězec znaků, kterých obvykle není více než 20. Autentizace heslem je nejjednodušším, velmi levným, flexibilním, a proto také nejčastěji používaným systémem. Nevýhodou je malá bezpečnost, kterou ovlivňují a zapříčiňují sami uživatelé, když volí nevhodná a slabá hesla (jména, příjmení, data narození, města, slova ze své branže, slova obsažená ve

slovnících apod.). Obrana proti tvorbě slabých hesel a jejich vynucené změny jsou sice možné, ale i to uživatelé ke škodě bezpečnosti systému obcházejí. Po většině lidí prostě nelze žádat, aby si pamatovali nic neříkající hesla typu gk25hr8s a každý den je měnili. Navíc jen málokdo vystačí pouze s jedním heslem. Proto se uchylují k logickým a odvoditelným konstrukcím hesel nebo je zapisují na málo bezpečná místa (existují i uživatelé, kteří mají hesla nalepená na monitoru nebo na pracovním stole. Další nebezpečí spočívají v okoukávání hesel, jejich zachycování na komunikačních kanálech nebo, nejsou-li dobře zabezpečena, v okopírování souborů, v nichž jsou uložena.

Komplikovanost hesla je dobrou ochranou proti programům, které se snaží heslo uhádnout pomocí porovnávání se svojí databází. Taková databáze samozřejmě obsahuje hesla jako jsou jména, slovníková hesla, apod.). I když budou takováto hesla lehce pozměněná třeba o jednu číslici nebo jiný znak, jsou programy schopné je uhodnout.

V hesle by se neměly používat problematické znaky jako jsou například @, ~, #, &, ¤, $, znaky s českou diakritikou, apod. kvůli jejich nejisté dosažitelnosti z různých klávesnic. Kvůli možné záměně je také lepší se vyhnout znakům *y* a *z*.

V drtivé většině případů systémy rozlišují mezi velkými a malými písmeny. Proto je vhodné využít možnost použití velkých i malých písmen ke ztížení odhalení hesla.

Zásadně by se neměla používat stejná hesla k evidentně nedůvěryhodným službám, jako jsou různé chaty, a k službám, o kterých víme, že jsou relativně bezpečné, např. při přihlašování do ověřeného firemního informačního systému. Žádné heslo by se nemělo používat věčně a je jen ku prospěchu jej čas od času změnit.

Vyšší míru zabezpečení skýtají taková hesla, která nemají dlouhodobější platnost a nelze je použít vícekrát, pro opakovanou autentizaci. Jsou to hesla označovaná jako jednorázová (one-time password), protože je lze použít skutečně jen pro jedno jediné ověření (autentizaci). Pokud by se někdo nepovolaný takovéhoto hesla dokázal zmocnit, například jej odposlechnout při přenosu, stejně by mu nebylo k ničemu, protože podruhé již takovéto

heslo nelze použít. Naopak jeho opakované použití je signálem že něco není v pořádku.

Praktické používání jednorázově použitelných hesel má samozřejmě i svá úskalí. Například není dost dobře možné chtít po uživatelích, aby takováto hesla sami vymýšleli. Stejně tak není smysluplné dát jim do ruky sáhodlouhý seznam jednorázově použitelných hesel, vygenerovaných dopředu a určených k postupnému použití (již jen kvůli riziku, že se tento seznam dostane do nepovolaných rukou). Místo toho musí být jednorázová hesla vhodným způsobem dynamicky generována. Například pomocí hardwarového zařízení, které bude uživatel mít u sebe.

6.3.2 Autentizace pomocí předmětů

Ve většině případů jde o daleko spolehlivější metodu autentizace než v případě hesel. Její jedinou nevýhodou je pro masové nasazení stále ještě příliš vysoká cena snímacích zařízení autentizačních předmětů. To se týká prakticky všech známých druhů karet (čipových, magnetických…). Poměrně novým autentizačním předmětem je tzv. dotyková paměť (touch memory). V tomto případě je levný jak autentizační předmět, tak jeho snímač, který je zhruba o řád levnější než snímače karet.

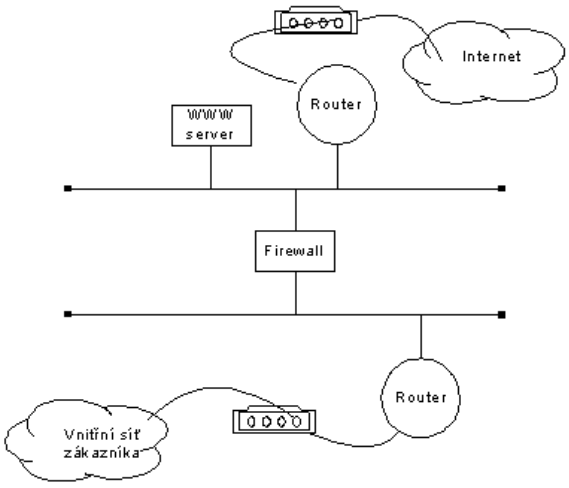
6.3.3 Biometrické metody

Kromě psychologického efektu mají tu vynikající vlastnost, že nevyžadují, aby uživatel s sebou něco nosil, nebo aby si něco pamatoval. Některá řešení však nejsou příliš pohotová nebo uživatelsky přívětivá a zpravidla z možnosti autentizace vyřazují lidi fyzicky postižené nebo indisponované (např. se zánětem spojivek nebo zlomenou rukou). Jejich hlavní nevýhodou je ale cena.

7 Firewally

Když je nějaká privátní síť připojena k internetu, je žádoucí takové připojení zabezpečit. Za tímto účelem se mezi síť a internet vkládá *firewall*. Firewall je systém bránící navazování neautorizovaných spojení mezi sítěmi, nejčastěji mezi privátní sítí a internetem. Firewally mohou být řešeny na úrovni hardwaru, softwaru nebo se může jednat o kombinaci obojího. Pokud je použit hardwarový firewall, pak pracuje jako aktivní prvek – tedy zařízení, do kterého je přivedeno z jedné strany připojení k internetu a z druhé strany je do něj připojen počítač. Hardwarové firewally se používají převážně u serverů nebo rozsáhlých počítačových sítí. Pro potřeby malých nebo domácích sítí jsou vhodné softwarové firewally (například ZoneAlarm Personal Firewall, Kerio Personal Firewall a další), které jsou instalovány přímo na uživatelském počítači a jsou permanentně spuštěny, kdykoliv je připojení k internetu aktivní.

Všechna data, která do privátní sítě vstupují nebo z ní vycházejí, prochází firewallem. To znamená, že každá zpráva nebo blok dat jsou zkontrolovány, zda splňují podmínky, které stanovuje bezpečnostní politika sítě a je tak omezeno nebezpečí průniku do sítě zvenčí. Firewall může zaznamenávat statistické a konkrétní údaje o datech přes něj procházejících. Tyto údaje poté mohou sloužit jako zdroj dat pro kontrolu funkčnosti bezpečnosti systému.



Obr.1: Schema zapojení firewallu

Firewally lze podle použité technologie rozdělit zhruba do dvou základních skupin. Jednak jsou to *paketové filtry* a jednak *aplikační brány (proxy gateways)*. Jako nová kategorie se uvádí *stateful inspection*. Filtrování paketů provádí nejčastěji *směrovač (router)* a rozhoduje se na základě zdrojové a cílové adresy a portu paketu. Administrátor tak může zamezit některým typům útoků a může omezit přístup z internetu a na internet pro vybrané protokoly nebo počítače (podle jejich IP adresy). Paketové filtry jsou na rozdíl od aplikačních bran schopny chránit i samy sebe a vyznačují se daleko vyšší rychlostí a transparentností. Nejsou však schopny zaznamenávat (logovat) informace o povolených nebo zamítnutých spojeních, neupozorňují tedy ani na neúspěšné pokusy o průnik do sítě.

Aplikační brána pracuje odlišným způsobem. Každá aplikace, jejíž spojení prochází aplikační bránou, o ní musí vědět a musí být schopna s ní spolupracovat. Spojení neprocházejí přes firewall přímo, ale klientská aplikace nejprve zkontaktuje aplikační bránu a ta potom zahájí nové spojení na cílový server. Odpověď pak aplikační brána předá klientské aplikaci. Nikdy tedy není navázáno přímé spojení mezi klientským počítačem a serverem, ale je zprostředkováno aplikační bránou. Aby bylo možné toto spojení zprostředkovat, musí aplikační brána znát použitý protokol. Je zde tedy možnost odmítnout nepovolené příkazy, případně přenášená data dále kontrolovat. Úroveň zabezpečení sítě je tedy podstatně vyšší než při použití paketového filtru.

Nevýhodou aplikačních bran je, že podporují velmi omezené množství protokolů používaných na internetu. Jsou navíc málo flexibilní, neboť přidání podpory pro další protokol je náročné a pomalé.

Technologie Stateful Inspection spojuje výhody obou výše zmíněných technologií a snaží se odstraňovat jejich nedostatky. V současné době lze pozorovat postupné přibližování firewallů různých výrobců k této technologii a úplně čistý paketový filtr či aplikační brána jsou spíše výjimkou.

Přehled některých firewallů nabízených na českém trhu je uveden v Tabulce 1.

Název	Výrobce	Provedení	Typ	Platforma (OS)
WinRoute Pro	Tiny Software	SW	PF/SI	Windows 95/98/NT
Gauntlet Firewall	Network Associates	SW	PF/AB	Unix, Windows NT
PIX Firewall	Cisco Systems	SW, HW	SI	vlastní
PrivateWire	Algorithmic Research	SW	PF/SI	Windows NT, Solaris
WatchGuard Firebox	WatchGuard Technologies	SW/HW	PF/AB/SI	Linux
NetRoad FireWall	UKIAH Software	SW	PF/AB/SI	Windows NT, Netware
FireWall-1	CheckPoint Software	SW	PF/SI/AB	Windows NT, Solaris, HP-UX

Tabulka 1: Přehled firewallů

7.1 Architektura firewallů

Tři nejčastější architektury firewallu jsou firewall se dvěma domovskými podsítěmi (dual-homed host firewall), firewall s odstíněným hostitelským počítačem (screened-host firewall) a firewall ochrany podsítí (screened-subnet firewall). Firewall s odstíněným hostitelským počítačem a firewall ochrany podsítí používají kombinaci směrovačů a proxy-serverů, zatímco dual-homed host firewall používá dvě oddělené síťové karty.

7.1.1 Firewall se dvěma domovskými podsítěmi

Firewall se dvěma domovskými podsítěmi (dual-homed host firewall) je jednoduchá, přesto však velmi účinná a bezpečná konfigurace. V případě tohoto firewallu je jeden počítač vyhrazen jako dělící čára mezi lokální sítí a internetem. Tento počítač požívá pro připojení k jednotlivým sítím dvě oddělené síťové karty. Při použití firewall se dvěma domovskými podsítěmi, je třeba zablokovat směrovací schopnost hostitelského počítače tak, aby počítač nespojil tyto sítě pomocí softwaru.

Největší nevýhodou konfigurace se dvěma domovskými podsítěmi je fakt, že uživatel může snadno náhodně umožnit vnitřní směrování, které poruší firewall. Nejkritičtější stránkou bezpečnosti v případě použití firewallu se dvěma domovskými podsítěmi je, že se musí zablokovat vnitřní

směrování hostitele. Při zablokování směrování musí data projít přes škrtící bod (chokepoint), aplikační vrstvu (tzn. stojí na vrcholu sady protokolů), která je jedinou cestou mezi sítěmi nebo segmenty sítě. Pokud by bylo umožněno standardní otevřené interní směrování uvnitř hostitelského počítače, bude firewall zbytečný.

7.1.2 Firewall s odstíněným hostitelským počítačem

Mnoho návrhářů sítí považuje firewall s odstíněným hostitelským počítačem (screened-host firewall) za bezpečnější než firewall se dvěma domovskými podsítěmi. Pokud se vytváří firewall s odstíněným hostitelským počítačem, přidáte k vaší síti ochranný směrovač a umístíte hostitelský počítač mimo internet (jinými slovy, hostitelský počítač není přímo spojen s internetem), tato sestava vám nabídne velmi efektivní a snadno udržovatelný firewall. Ochranný směrovač spojuje internet s vaší sítí a současně filtruje pakety, které pustí dovnitř. Ochranný směrovač nakonfigurujete tak, že vidí pouze jeden hostitelský počítač vaší sítě. Uživatelé vaší sítě, kteří se chtějí spojit s internetem, tak musí učinit pomocí tohoto hostitelského počítače. Ukazuje se tedy, že interní uživatelé mají přímý přístup k internetu, ale hostitelský počítač omezuje přístup vnějších uživatelů.

7.1.3 Firewall s odstíněnou podsítí

Architektura firewallu s odstíněnou podsítí (screened-subnet firewall) více izoluje lokální síť od internetu. Architektura firewallu ochrany podsítí zahrnuje dva oddělené ochranné směrovače a proxy-server. Při návrhu firewallu s odstíněnou podsítí umístí návrhář proxy-server na jeho vlastní síť, kterou sdílí pouze s ochrannými směrovači. Jeden ochranný směrovač řídí provoz blíže lokální síti. Druhý ochranný směrovač monitoruje to, co přichází a odchází na internet.

Firewall s odstíněnou podsítí nabízí impozantní ochranu proti útoku. Protože je hostitelský počítač izolován v samostatné síti, omezuje dopad útoku na hostitelský počítač a dále minimalizuje šanci na poškození interní sítě. Směrovač na lokální síti dále poskytuje ochranu proti nepatřičnému internímu přístupu k hostitelskému stroji.

8 Pojištění rizik

Jednou z cest, jak snížit ztráty ze škod vzniklých počítačovou kriminalitou (nejen na internetu) je pojištění rizik plynoucích z provozu informačních technologií, kterým se zabývají pojišťovny a především pojišťovací makléři. Pojistné produkty, které tato poměrně nová rizika řeší, jsou velice složité a většinou šité zákazníkovi přímo na míru. Nelze tedy lehce specifikovat, co je a co není předmětem pojištění. Jde ale v každém případě o zbytkové riziko za předpokladu, že je všemi dostupnými prostředky zajištěna bezpečnost dat a vlastních informací. Alespoň určitou náhradu škod nabízí mnohé ústavy, u kterých se lze pojistit proti:

- podvodnému vložení dat do systému, z toho vyplývajícím vzniklým škodám jak pojištěnému, tak jeho zákazníkům
- ztrátě elektronických dat pojištěného v důsledku záměrného zničení či pokusu o ně jakoukoliv osobou v kteroukoli dobu
- ztrátě, poškození či zničení médií pro elektronické zpracování dat v důsledku krádeže, vloupání, odcizení či nevysvětlitelného zmizení
- škodám vzniklým následkem počítačového viru
- škodám vzniklým změnou elektronické informace včetně škod vzniklých na elektronických papírech.

Z toho vyplývá, že si dnes společnost může pojistit škody vzniklé následkem počítačového viru nebo škody vzniklé následkem změny elektronické informace (např. napadení webových stránek a změna informací na nich). Takové pojištění je téměř nemožné realizovat soukromě, bez využití služeb firem, které se touto problematikou přímo zabývají. Při špatné analýze rizika nebo dokonce bez bezpečnostního auditu informačních systémů pojištěného může při vzniku pojistné události dojít k neplnění ze strany pojišťovny.

Většina firem si není úplně jista, zda pojištění rizik plynoucích z provozu informačních technologií pro ně má nějaký význam a mnohdy nevěří, že jim pojišťovna opravdu určitou finanční náhradu při ztrátě dat způsobené například počítačovým virem nebo hackerem poskytne. Na druhou stranu například banky provozující internetové bankovnictví ani nemají jinou možnost, než služeb tohoto pojištění využít a minimalizovat tak

rizika svého podnikání. Zřejmé je, že dokazování a vyčíslování skutečné škody je velice obtížné, i když ne nemožné. V každém případě takovouto možnost ochrany s postupem času a s nárůstem rizik a způsobených škod jistě mnoho firem uvítá.

9 Závěr

Mnohdy není jednoduché přesvědčit okolí o nutnosti systematického řešení otázek bezpečnosti. Stručně shrnuté základní argumenty pro aplikaci bezpečnostních opatření a přijetí bezpečnostní politiky jsou následující:

- Zvýší důvěryhodnost a vylepší jméno společnosti - jasnou bezpečnostní politiku lze považovat za konkurenční výhodu.
- Předchází poškození dobrého jména firmy např. medializací úniků dat tím, že je účinně eliminuje. Dále je přesně určeno, jaký bude postup, když přesto k úniku dat dojde.
- Chrání stabilitu firmy tím, že minimalizuje nebezpečí úniku dat z vnitřního prostředí způsobeného vnějším narušitelem.
- Chrání před útokem hackerů, kteří se snaží proniknout do vnitřního systému, ať už za účelem vydírání nebo jen pro zábavu či z jiného důvodu.
- Chrání před počítačovými viry, které můžou paralyzovat chod firemní sítě.
- Poskytuje pocit jistoty, že například při selhání technického zařízení či jiného problému, je firma na tuto situaci připravena.

Investice do prevence bezpečnosti IS je ve výsledku mnohem levnější než řešení následných škod. Vůbec prvním krokem ke snížení bezpečnostních rizik musí být zmapování stávající situace. Poté by měla následovat analýza rizik, která pojmenuje jednotlivé problémy s doporučením na jejich vyřešení nebo alespoň minimalizaci. Provedená analýza umožní vytvořit tzv. bezpečnostní politiku, ve které jsou popsána bezpečnostní specifika dané sítě či počítače a definována pravidla a zásady bezpečnosti. Poté následuje vlastní implementace bezpečnostních opatření. Posledním krokem je monitorování a kontrola, zda se stanovená pravidla dodržují a zda není třeba reagovat na změny okolního prostředí či nově se objevujícího rizika. Opomenutí posledního kroku často vede k tomu, že po určitém čase se musí s řešením bezpečnosti začínat znovu od začátku.

Pro větší firmy se jako rozumná se jeví kombinace budování bezpečnostních opatření vlastními silami a využití externích specializovaných firem. Analýzu rizik převážně zpracovávají externí specialisté

a další kroky mohou vykonávat vlastní zaměstnanci s pomocí konzultantů. Slabým místem bývají bezpečnostní školení. Firmy nebývají příliš ochotny do nich investovat mnoho peněz. Přitom pravidelné školení minimalizuje rizika spojená s chybami uživatelů, které pramení z neznalosti. Mnoho škod totiž napáchají panikařící uživatelé ve spojitosti s neodbornými pokusy o odstranění závady. Kvalitně vedená školení by se měla provádět v pravidelných intervalech.

Žádná bezpečnostní opatření nezajistí stoprocentní ochranu dat, ale rizika se dají snížit na minimum při dodržení těchto zásad:

- instalace hardwarového i softwarového firewallu
- instalace antivirového programu a provádění jeho pravidelné aktualizace
- časté zálohování, nejlépe pomocí zrcadlení disků
- instalace bezpečnostních aktualizací a oprav chyb operačních systémů a aplikací (tzv. service packy a patche)
- nikdy nespouštět spustitelné přílohy elektronické pošty, pokud není jejich původ bezpečný
- šifrování důležitých dat (za cenu obtížnější správy souborů zůstanou důležité dokumenty pro nepovolané osoby nečitelné) a používání digitálních podpisů.

Literatura

[1] Barrett, Daniel J.: Bandité na informační dálnici, Computer Press, Brno 1999

[2] Dobda, Luboš: Ochrana dat v informačních systémech, Grada Publishing, Praha 1998

[3] Dostálek Libor: Velký průvodce protokoly TCP/IP: Bezpečnost, Computer Press, Brno

[4] Hönigová, Alena, Matyáš, Václav: Anglicko-česká terminologie bezpečnosti informačních technologií, Computer Press, Praha 1996

[5] kolektiv autorů: Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality, Vydavatelství PA ČR, Praha 1997

[6] Naik, Dilip C.: Internet – Standardy a protokoly, Computer Press, Brno 1999

[7] Smejkal, Vladimír: Internet @ §§§, Grada Publishing, Praha 1999

Internetové zdroje:

www.aec.cz
www.decros.cz
www.itsec.gov.uk
www.kpnqwest.cz
www.winroute.cz