ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA

PROVOZNĚ EKONOMICKÁ FAKULTA

BAKALÁŘSKÁ PRÁCE

TÉMA:

ZABEZPEČENÍ POČÍTAČE

Autor bakalářské práce: **Daniel Eger**

Vedoucí bakalářské práce: **Ing. Richard Černý, CSc.**

Prohlášení:

Prohlašuji, že jsem bakalářskou práci „Zabezpečení počítače“ vypracoval samostatně pod vedením „Ing. Richarda Černého, CSc.“ a uvedl v seznamu požitých zdrojů všechny použité literární a odborné zdroje.

V Praze, dne 26. června 2007 *……..…..*

Daniel Eger

Poděkování:

Tímto bych rád poděkoval vedoucímu této bakalářské práce „Ing. Richardovi Černému, CSc.“ za mnoho cenných rad a odborné vedení při přípravě této práce.

Zabezpečení počítače

(PC security)

Souhrn

Cílem práce je představit problematiku zabezpečení počítače. Seznámit čtenáře s hrozbami a škodami, které mohou nastat v případě, že zabezpečení počítače nebude věnována dostatečná pozornost. Práce přibližuje jakou formou může být počítač (server, síť) napaden a definuje nebezpečí, které se skrývá za termíny virus, spam, spyware, phishing a dalšími. Formy napadení jsou podrobněji analyzovány a je předpovězen jejich budoucí vývoj. Na základě těchto poznatků jsou doporučena bezpečnostní opatření a prostředky, pomocí kterých lze většinu forem napadení odvrátit a eliminovat. Setkáme se s termíny firewall, antivir a přiblížíme si novou technologii zabezpečení lokálních sítí SIG (Secure Internet Gateway).

Summary

The aim of this bachelor thesis is to introduce PC security, acquaint a reader with threats and damages, which can come in case there is not given sufficient attention to a computer security. The thesis shows a way, how can be a computer (server, network) attacked and defines a danger hidden in matters like virus, spam, spyware, phishing and others. The forms of attack are analyzed in detail and there is also specified their future evolution. There are recommended some safety arrangements on basis of these fact, which can foil and eliminate every form of attack . A reader also will be made familiar with terms firewall and antivirus. This thesis also shows new technology of local network security SIG (Secure Internet Gateway).

Klíčová slova

Zabezpečení počítače
Počítačová infiltrace
Malware
Počítačové útoky

Key words

PC security
Computer infiltration
Malware
Computer attacks

1 Úvod

Počítače jsou nepostradatelnou součástí našeho každodenního života. Zabezpečují chod velkého množství rutinních aktivit. Pro znásobení výkonu, využití komunikačních služeb a sdílení dat se využívá připojení počítačů do sítě. Sítě ve firmách bývají většinou lokálního charakteru, stejně tak jako malé domácí sítě. Lokální sítě se připojují do globální sítě – Internetu. Výpočetní technika dokáže být velkým pomocníkem, usnadňuje nám práci, dokáže za nás vykonat tisíce operací, které by nám trvaly dobu mnohem delší.

Vzhledem k množství dat, které denně těmito sítěmi proudí se Internet stává tzv. datovou dálnicí, kde proudí data z celého světa, ze všech možných hospodářských odvětví a soukromých subjektů. Existuje však i stinná stránka celé věci. Po datové dálnice lze „jezdit“ oběma směry, a tak není problém se přes Internet dostat až k lokální síti, nebo samotnému počítači. Existuje mnoho forem napadení a škodlivých útoků (o kterých bude pojednáno dále), které mohou citlivá firemní i soukromá data poškodit nebo zcizit a využít je v konkurenčním boji, či dokonce pro kriminální činnost. Stále častěji tak do našeho života vstupuje problematika zabezpečení počítače.

Únik citlivých dat může znamenat velké nepříjemnosti a s tím spojené finanční ztráty. Řada menších subjektů se domnívá, že nikdo nebude mít zájem poškodit právě je, když existuje velké množství mnohem zajímavějších cílů. Jenže právě tyto subjekty bývají díky podcenění zabezpečení snadným cílem napadení.

“Jedním z největších problémů v oblasti zabezpečení počítačů je, že uživatelé nevěří, že by se právě jim mohlo stát něco špatného – dokud k tomu nedojde.“[5]

2 Cíle práce a metodika

Práce si klade za úkol podat ucelený obraz problematiky zabezpečení počítače. Budou zmapována a zhodnocena možná rizika a nástrahy, které mohou ohrozit bezpečnost počítače. Poukážeme na jednotlivá rizika a naznačíme cesty jak se jim vyhnout, nebo jak se proti nim účinně bránit. Součástí práce je i ukázkový návrh zabezpečení pomocí technologie SIG (Secure Internet Gateway), který může sloužit jako základ pro návrh zabezpečení firemní sítě.

První část práce, zabývající se možnými formami napadení a riziky, která mohou nastat v případě nezabezpečeného, nebo špatně zabezpečeného přístupu k počítači, poukazuje na důsledky, které může způsobit nevěnování pozornosti této tematice. Každé z rizik bude podrobněji analyzováno a naznačíme základní metody pro minimalizaci a eliminaci napadení a vzniku následných škod.

V další části budou přiblíženy prostředky, které se používají pro kvalitní zabezpečení přístupu k počítači. Tato část práce by měla sloužit jako vodítko při návrhu zabezpečení počítače.

V závěrečné části práce bude na ukázkovém příkladu serveru (počítače) připojeného k síti implementována technologie zabezpečení SIG.

Rešerší část se opírá o poznatky publikované odborníky na zabezpečení, kteří se v oboru pohybují řadu let a podíleli se na významných projektech. Kromě odborných zdrojů bylo čerpáno také z Internetu. Problematika zabezpečení má velmi flexibilní charakter, informace a jejich aktuálnost se v čase rychle mění, a proto se Internet jeví být nejvhodnějším zdrojem pro získání aktuálních informací. Práce zohledňuje znalosti a osobní zkušenosti autora, který se o danou oblast zajímá již delší dobu.

3 Formy napadení

3.1 Historie virů a spamu

Počátek počítačových virů, spamu a s tím první spojené narušení bezpečnosti systému počítače sahá pár desítek let zpět. Již v roce 1949 dokázal John von Neuman popsat program, který se sám replikoval, ale program, který by se dal označit za virus se objevil až počátkem 60.let.

Software, který lze označit jako počítačový virus se jmenoval „Core Wars“. Jednalo se o hru, která se sama reprodukovala a zabírala místo v paměti počítače. Paradoxní je, že tvůrci viru byli i první tvůrci antiviru. Vytvořili program, který nesl jméno „Reeper“ a sloužil k odstranění hry (viru). Program byl však velmi málo rozšířený, takže se o jeho existenci příliš nevědělo.

První vir, který se začal šířit veřejně vznikl v roce 1981, se jmenoval ELK Cloner. Virus napadal osobní počítače Apple II. Jednalo se o hru, která při každém 50 spuštění zobrazila básničku. Virus byl sice velmi nakažlivý, ale téměř neškodný. Virus ELK Clonek byl následován mnoha dalšími.

Za zmínku jistě stojí první virus pro PC „©Brain“ za kterým stojí bratři Asit a Amjat Farooq Alviovi, pákistánští programátoři. Vir patřil mezi tzv. boot viry. Jeho úkolem měla být ochrana autorských práv. Vir dokonce uváděl telefonní kontakt na oba bratry, čímž se velmi „proslavili“.

V roce 1988 vznikl virus nazvaný „Morrisův červ“. Vytvořil R. T. Morris za účelem své diplomové práce na Corrnell University. Chtěl zjistit, jak velký je Internet. Jeho produkt tehdy napadl 6000 serverů, což v té době byla desetina serverů z celého Internetu, podařilo se mu dokonce infiltrovat do oddělení NASA, kde se pracovalo na tajném vládním projektu.

Rozvojem a rozšířením operačního systému MS DOS přišlo také masové rozšíření virů. Opravdové žně však zažívají virové nákazy počítače až s rozvojem Internetu a e-mailu. Velká světová epidemie přišla v roce 1999

v podobě viru Melissa a v roce 2000 pod jménem LoveLetter. V dnešní době můžeme zaznamenat velké množství tzv. červů, které bývají (avšak ne úplně správně) zařazovány mezi viry.

Odborné publikace se různí v názoru na to, kdy byl vyslán vůbec první spam a jakého byl znění. Dle [14] se první spam (nevyžádaná pošta) objevil v roce 1978. V té době ještě neexistoval Internet, ale teprve se vyvíjen ze sítě ARPANet. V rozesílané zprávě stojí cosi o prezentaci produktu z řady DECSYSTEM, která se bude konat v úterý 9. května 1978.

3.2 Budoucí vývoj

Problematika spamu je velká i v České republice, ale situace není tak kritická jako v některých jiných státech. Představme si, že by veškerá nevyžádaná pošta, která dorazí do naší schránky byla v českém jazyce. E-maily s předmětem „dokončení Vaší registrace“, nebo „pozvánka na party“ potom nechají těžko čtenáře chladným.

Laboratoře, věnující se zabezpečení, vyvíjejí nové technologie pro filtraci nevyžádané pošty (odhalovaní spamu), virů, neautorizovaných přístupů. Stejně tak se zdokonaluje i spam a viry, které jeho tvůrci upravují tak dlouho, dokud zabezpečení neobejde a filtry „neproleze“.

Za několik let bude zcela běžné, že většina zařízení (domácí spotřebiče, automobily, atd.) bude trvale připojeno k síti (k Internetu) – tedy možnost vzdáleného přístupu a napadení. V této souvislosti bude pravděpodobně nutné provést jakousi formu regulace Internetu, doplnit chybějící legislativu a omezit „volnost“ na Internetu.

3.3 Formy napadení

Dle druhu napadení počítače lze bezpečností hrozby rozdělit do několika skupin, které se však úzce prolínají. Některé formy napadení tedy nelze přesně zařadit pouze do jedné skupiny.

3.3.1 Malware

„Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému.

Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware. V právní terminologii je malware někdy nazýván počítačová nečistota (angl. „computer contaminant“), například v zákonech států Kalifornie, Západní Virginie a několika dalších členských států USA. Malware je někdy pejorativně nazýván scumware. Jako malware by neměl být označován software, který sice obsahuje chyby, ale byl napsán pro legitimní účely.“[4]

3.3.2 Viry

„Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů tzv. malware, zákeřného software. V obecném smyslu se jako viry (nesprávně) označují i např. červi a jiné druhy malware.

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či

po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji.“[4]

Hlavním kanálem pro šíření virů se stala globální síť Internet, doplňkovým nosičem mohou být paměťová média (flash disky, CD-ROM, diskety, atd.). Výhodou internetu pro šíření virů je rychlost a masové šíření viru. Nejčastější způsob infiltrace do počítače bývá spuštěním programu, který do počítače zanese virovou nákazu. S takovými programy se nejčastěji setkáme na pochybných webových stránkách, nebo v přílohách „nevyžádané pošty“.

Virus se nejčastěji infiltruje do souborů typu EXE a dalších spustitelných souborů (COM, BAT, VBA). Virus může být infiltrován i v souborech typu MP3, JPEG a jiných. V tomto případě se však jedná pouze o přechování viru. Soubor JPEG, MP3 ani jim podobné nemohou zajistit replikaci viru a například při přehrávání MP3, nebo prohlížení JPEG je připojené tělo viru k souboru považováno za smetí a je ignorováno.

I v odborné literatuře bývají pojmem „virus“ označeny i další formy napadení počítače (trojské koně, červy, atd.). Trojské koně a červy lze chápat jako virus, protože jejich ničivý dopad je podobný, ale způsob šíření je jiný než u virů. ***Pro zjednodušení se někdy pod pojem „virus“ zahrnují i trojské koně a červy.***

3.3.3 Trojské koně

„Trojský kůň je uživateli skrytá část programu nebo aplikace, o jehož přítomnosti uživatel neví. Název Trojský kůň pochází z antického příběhu o dobytí Tróje. Ve většině případů použití trojského koně se jedná o škodlivou činnost. Trojský kůň může být například přidán do stávající aplikace, která je poté šířena pomocí peer-to-peer sítí, nebo warez serverů. Uživatel stažením kopie aplikace (nejčastěji bez platné licence nebo jako volně šířený program z

nedůvěryhodného serveru), může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou.

Drobný rozdíl mezi počítačovým virem a trojským koněm je ten, že trojský kůň nedokáže sám infikovat další soubory svojí kopií. Ale může existovat počítačový červ, který na napadeném počítači instaluje různé trojské koně.“[4]

Trojský kůň získal své jméno zejména proto, že zpočátku se trojští koně tvářili jako užitečné programy a utility a byli nabízeny zdarma. Pokud by Vám přišel e-mail s textem: „Ahoj v příloze ti zasílám nejnovější antivirus od McAfee, stačí spustit a nainstalovat“. Odolali byste ?

Existuje celá řada trojský koní a dělí se do mnoha dalších podskupin podle činností, které mají za úkol vykonávat. Někdy se činnost trojských koní úzce prolíná se „spyware“.

3.3.4 Keyloggers

Druh trojského koně, který sleduje stisk jednotlivých kláves, nashromážděná data pak odesílá na adresy svému tvůrci, který tak může vyčíst např. Vaše přístupová hesla.

3.3.5 Backdoors

Backdoors (zadní vrátka) lze považovat za trojského koně, ale je možné jej zařadit i mezi červy. Jedná se o metodu, která útočníkovi umožňuje přistupovat do systému a zároveň umožňuje tento přístup zachovat skrytý před běžnou kontrolou. Kvalitní backdoors se dokáží vydávat například za webový prohlížeč, takže je např. firewall bez problému propustí.

Takto ovládnutý systém útočníkovi může sloužit jako tzv. bílý kůň (termín z kriminální činnosti). Útočník může díky backdoors prostřednictvím Internetu ovládat počítač na druhém konci světa a využívat jej k rozesílání virů a spamu (používá se také označení Trojan Proxy). Útočník si tak zachovává svojí anonymitu.

3.3.6 Dialers

Program, který si můžeme i dobrovolně stáhnout. Nejčastěji se s takovým programem setkáme např. na stránkách obsahujících pornografický materiál. Provozovatel stránky může uvádět, že pro přístup na jeho stránku je nutné tento program nainstalovat (spustit). Škodlivý je v případě, že jste k internetu připojení prostřednictví telefonní linky a využíváte vytáčeného připojení (nikoliv technologie ADSL). Dialer změní nastavení Vašich přihlašovacích údajů a vytáčené číslo Vašeho poskytovatele. Počítač se potom připojuje prostřednictvím dražšího tarifu (90 Kč / min i více), který platíte např. právě provozovateli erotické webové stránky.

3.3.7 Červy (worms)

Červy lze z určitého pohledu chápat jako zvláštní skupinu virů, ale způsob jejich šíření a infikování počítače je jiné než u klasických biologických virů. Červi se šíří v podobě souborů, nebo infikovaných paketů v počítačové síti. Šíření červů může vést až k zahlcení nejen podnikové sítě (viz případ Morrisova červa).

Infikovaný systém červ využívá k odesílání svých kopií na další systémy a to prostřednictvím sítě. Červy využívají bezpečnostních děr v operačním systému, nebo software. Úspěšnost jejich šíření je závislá na rozšíření konkrétního operačního systému, nebo software. Většina červů je proto vyvíjena pro různé verze systému Windows, který je stále nejrozšířenějším systémem.

3.3.8 Spyware

Jak již název napovídá, jedná se o špionážní software, který sbírá a odesílá data bez vědomí uživatele. Lze sem zařadit celou řadu trojských koní např. „keyloggers“ (viz výše) . Spyware shromažďuje např. statistická data, údaje z registrů, údaje o nainstalovaném software, prohlížené webové stránky, seznamy otevíraných souborů, které potom zasílá na zadané adresy. Tato data bývají využita např. pro zobrazování cílené reklamy.

Samotná existence spyware není nelegální a bývá součástí některých sharewarových programů. Techniky spyware používá i operační systém Windows.

3.3.9 Nevyžádaná pošta (spam)

Termín spam označuje nevyžádanou poštu ve schránce, tedy zprávu, která byla uživateli zaslána bez jeho souhlasu. Jedná se především o e-maily, které jsou nositelem virů, reklam a dalších zpráv, které pro uživatele většinou nemají valný význam. Nevyžádaná elektronická pošta v roce 2006 tvořila 86,2%[7] z veškeré elektronické pošty. Spam je velmi velkým problémem elektronické korespondence a znevýhodňuje její používání.

Masové rozšíření spamu má na svědomí velké množství e-mailových schránek a rychlost rozesílání pošty. Celá řada malware (trojské koně, spyware) má za úkol pouze sledovat uživatelovu činnost a odesílat jeho e-mailové kontakty a procházené stránky za účelem pozdějšího rozšiřování spamu. Je velmi pravděpodobné, že pokud spyware vysleduje, že navštěvujete především stránky zabývající se např. elektronikou, odešle tuto informaci. Vám po té začnou chodit nevyžádané e-maily s reklamou na elektroniku. Jde vlastně o cílenou reklamu (direkt marketing), který je aplikován pomocí netaktních praktik.

Pro účely šíření spamu existují dokonce tzv. vyhledávací roboti (tento princip využívají i internetové vyhledávače). Tyto roboti procházejí internetové stránky, diskuze, inzeráty a vyhledávají e-mailové adresy všude kde jsou uvedeny. Databáze e-mailových adres jsou velmi rozsáhlé.

Doposud zde mluvíme jen o e-mailu, což by mohlo způsobit mylný dojem, že nevyžádaná pošta se týká pouze elektronické pošty. S pojmem spam se ale můžeme setkat i v dalších oblastech:

- Nevyžádané zprávy existují i v oblasti komunikačních programů, tzv. Instant Messengerů (např. ICQ, Miranda IM, QIP)

- V diskusních fórech (i pod různými články – vložená reklamní zpráva i zde osloví široké spektrum uživatelů)

Nevyžádaná pošta působí velké ekonomické ztráty ve firmách, ale i v domácnostech. Pokud není filtrována, je její množství obrovské (považme, že jen 27,3% odeslaných e-mailů nebyl spam – tedy pouze každý 4. e-mail). Vyřizování takové pošty znamená časovou ztrátu a déle strávený čas u připojení k Internetu (větší množství přenesených dat, která nepožadujeme), s tím spojenou větší spotřebu elektrické energie, atd. Ztráty způsobené spamem u velkých společností pak čítají milióny i stamilióny korun.

3.3.9.1 Hoax (falešné zprávy, mystifikace)

Hoax je druh nevyžádané pošty. Jedná se o falešnou zprávu, nebo mystifikaci kterou rozesílají sami uživatelé. Příkladem hoaxů je např. varování o neexistujícím viru, falešné prosby o pomoc, petice a výzvy, pyramidové hry, řetězové dopisy. Hoax lze snadno identifikovat. Závěr e-mailu obsahuje výzvu k rozeslání e-mailu na další adresy (např. pošlete tento e-mail minimálně 5 lidem a splní se Vám přání).

Velmi známým se v této oblasti stal např. e-mail varující před nastraženými infikovanými jehlami v prostředcích MHD. Konec e-mailu opět obsahoval výzvu: „Rozešlete e-mail všem svým známým“. Dle pozdějšího vyjádření odborníků však k ničemu takovému nedošlo a nedochází, některé e-maily (hoaxy) však i přes svojí stupiditu kolují dodnes.

3.3.9.2 Phishing

Problematika phishingu je poslední dobou velmi diskutovaným problémem. Z hlediska zařazení se jedná o druh spamu. Jde však o problematiku tak závažnou, že se většinou řeší samostatně.

Termínem phishing (můžeme přeložit jako rybaření – jedná se o zkomoleninu anglického fishing) označujeme podvodné získávání citlivých dat od uživatele (např. hesel, čísel kreditních karet, atp.). Počátkem phishingu bývá rozesílání podvodných e-mailů (spamu), které vyzývají adresáta k zadání, nebo zaslání citlivých údajů. Rozeslané e-maily vypadají jako oficiální žádost banky či podobné instituce.

Na obr. 3.1 je zobrazen e-mailu, který byl rozesílán klientům banky Citibank. Jedná se o typický phishing. E-mail nabádá klienta ke kliknutí na odkaz který jej přesměruje na webové stránky.


citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.

Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

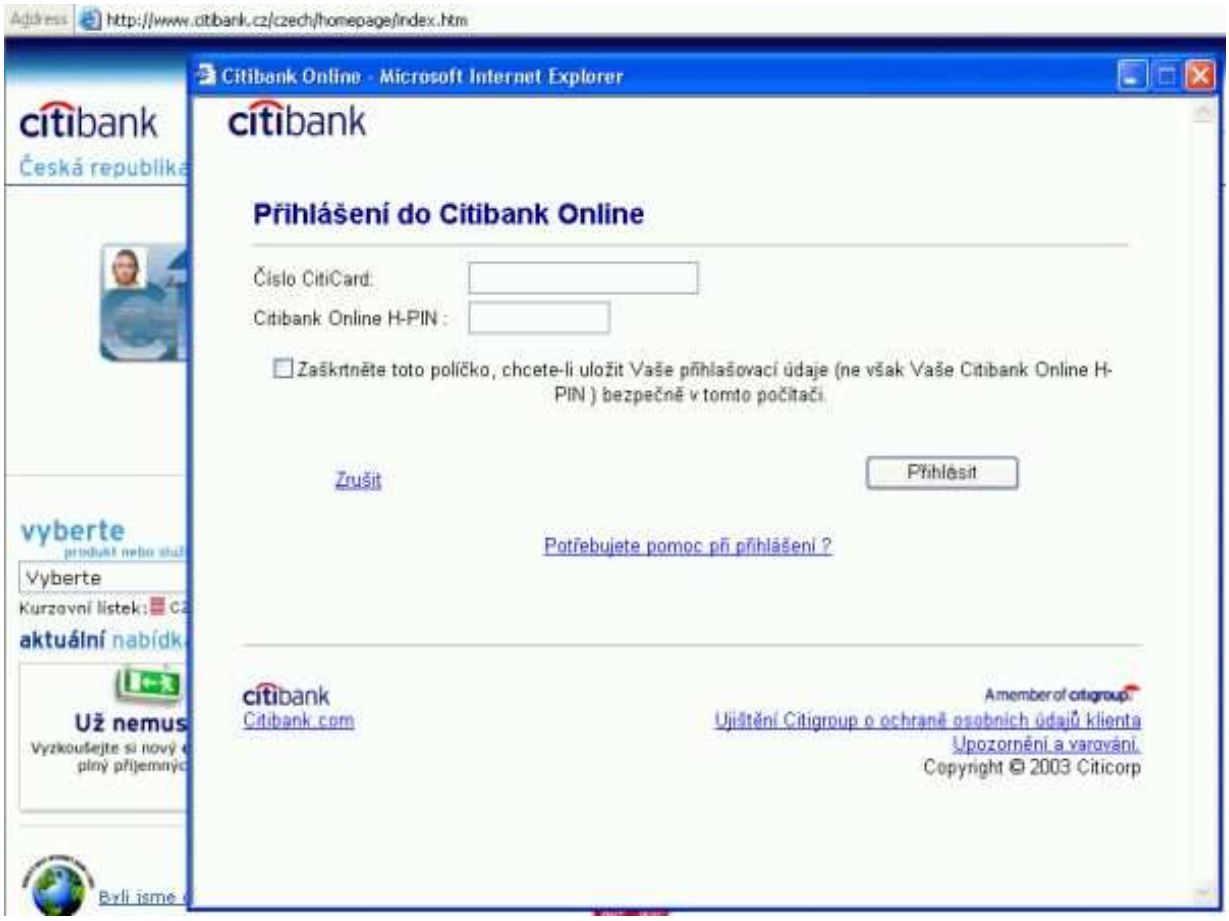
Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Obr. 3.1 Podvodný e-mail zasílaný klientům Citibank

Po kliknutí na odkaz se otevřela originální úvodní stránka Citibank a pop-up okno, které nabádá klienta k zadání citlivých údajů pro potvrzení platby. Pop-

up okno, ale vůbec nepatří k webové stránce Citibank a je dílem podvodníka (obr. 3.2).



Obr. 3.2 Pop-up okno vyzývající k zadání citlivých údajů

Po zadání údajů do okna byli citlivé údaje odeslány útočníkovi, který je po té mohl zneužít a odčerpat finanční prostředky z účtu klienta.

Nástupcem phishingu se stává pharming, ten funguje podobně, ale je mnohem nebezpečnější. Útočníci napadají DNS (Domain Name Systém) servery, které mají za úkol po zadání adresy URL (Uniform Ressource Locator tj. např. www.kb.cz) nasměrovat uživatele na správný server. Místo toho je uživatel po zadání adresy nasměrován na jiný server, kam bez obav zadá své údaje v domnění, že je na URL, které zadal.

3.3.10 Adware

Označení adware (Advertising supported software) se používá pro software, jehož součástí je reklama. Adware se do počítače instaluje za souhlasu uživatele. Bývá součástí vybraného programu (povětšinou freeware), který je sponzorován právě zobrazovanou reklamou. Je diskutabilní, zda lze adware považovat za malware, když jsme jeho instalaci sami odsouhlasili potvrzením licenčního ujednání EULA (End User Licence Agreement).

Existují však různé způsoby a stupně agresivity s jakou je reklama zobrazována. Pod pojmem adware si totiž můžeme představit obyčejné reklamní banery, ale také agresivní vyskakující pop-up okna, vnucování webových stránek a změny domovské stránky.

Adware také velmi často využívá dat, které získá od spyware. Na základě těchto dat je uživateli zobrazována cílená reklama.

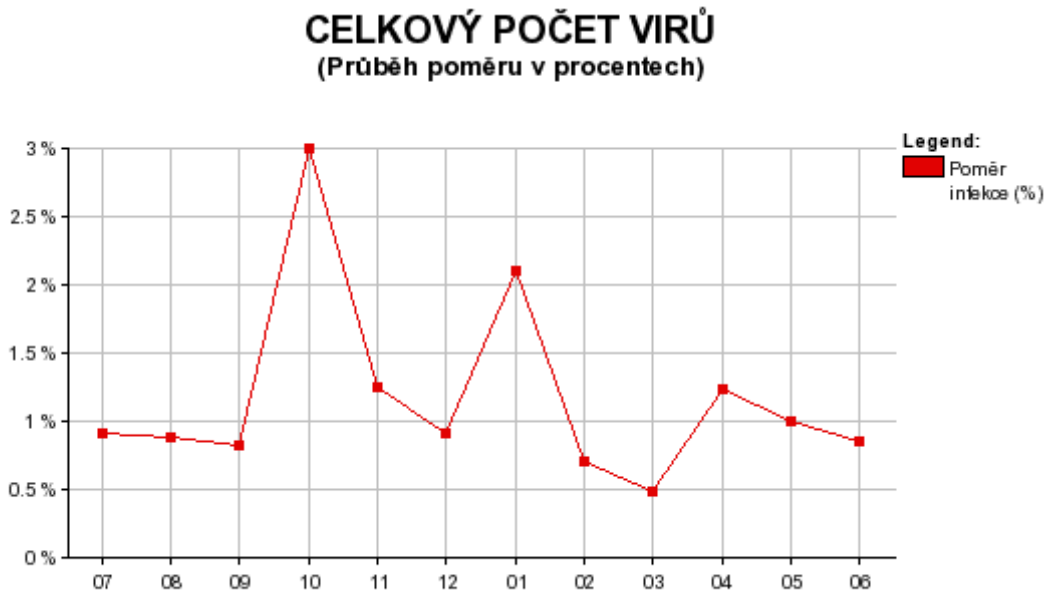
3.3.11 Cílené útoky

Jde útoky hackerů, které jsou přímo zaměřeny na určitý subjekt (např. za účelem zcizení dat, poškození firmy, atd.). Problematika těchto útoků zejména v poslední době stoupá. Hacker vyčkává a pomocí speciálního software, který není problém stáhnout z internetu, skenuje porty na počítači své oběti. Pokud je některý z portů nezabezpečený, nebo se uvolní (otevře), útočník jej využije pro napadení počítače. Obrana proti těmto útočníkům je velmi obtížná. Pokud se jedná o zkušené softwarové inženýry, dokáží obejít i firewall (viz dále).

4 Analýza forem napadení

Server www.virovyradar.cz, který je zřízený pod záštitou společnosti Eset s.r.o. (Eset je známý díky svému antivirovému produktu NOD32, který obdržel mnohá prestižní ocenění) má za úkol monitorovat e-maily, které prochází českým internetem.

Na obr. 4.1. jsou výsledky analýzy, které server www.virovyradar.cz provedl. Obrázek znázorňuje situaci za poslední rok od července 2006 do června 2007. Lze si povšimnout, že trend je velmi nestabilní a kolísavý. Tento jev je způsoben neustálým zdokonalováním bezpečnosti systémů a vývojem nových virů. Je-li ošetřena bezpečností díra do systému, šíření viru se zastaví. Ovšem je jen otázkou času, kdy bude vyvinut další virus, který bude využívat jiné díry v bezpečnosti. Takový virus má možnost se masově šířit, ovšem jen do doby, než je přidán do databází antivirů, nebo bezpečností díra v systému je opravena.

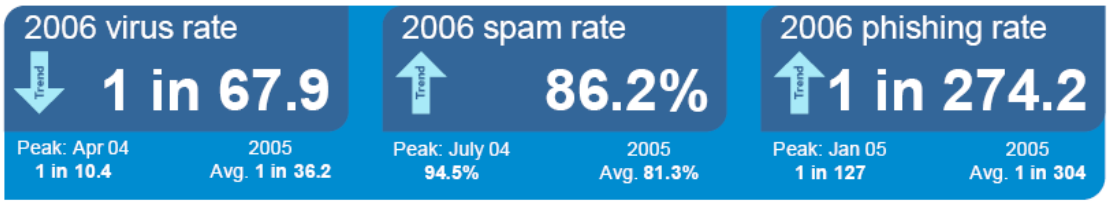


Obr. 4.1 Celkový počet virů v analyzovaných e-mailech Zdroj: www.virovyradar.cz[7]

Průměrný počet infikovaných e-mailů za sledované období byl 1 infikovaný z 83,8 e-mailů. Jednoduchým výpočtem tedy zjistíme, že dle

virového radaru bylo virem infikováno 1,19 % ze všech elektronických zpráv v českém internetu.

Podobným měřením, ale v globálním měřítku se zabývá i společnost Message Labs. Výsledky měření Message Labs jsou na obr. 4.2. Bohužel data v tomto případě jsou za období leden – prosinec 2006 a nelze je tedy přímo srovnat s měřením serveru virový radar. 1 zavirovaný e-mail z 67,9. To odpovídá 1,47 % zavirovaných e-mailů ze všech odeslaných zpráv. Rozdíl o 2 desetiny procenta oproti měření virového radaru je způsoben jiným sledovaným obdobím a lokalitou. V českém republice se totiž vyskytuje méně útoků než v zahraničí, což je způsobeno tím, že většina virů vzniká v anglicky mluvících zemích. Oproti výsledkům v roce 2005 lze pozorovat klesající trend.



Obr. 4.2 Výsledky měření Message Labs

Zdroj: http://www.messagelabs.com/resources/mlireports[8]

Data z reportu Message Labs nám poskytují i další zajímavé informace. Průměrně 86,2% ze všech odeslaných e-mailů v roce 2006 patřilo do kategorie nevyžádané pošty (spam). Zvýšení zaznamenává phishing. Phishing se stává velkou hrozbou, protože je velmi obtížně rozeznatelný a pokud uživatel není obezřetný (viz. případ Citibank) může bez jeho vědomí dojít např. k odčerpání finančních prostředků z jeho účtu.

4.1 Analýza množství virových nákaz

Díky dlouhodobému měření lze zobrazit vývoj v oblasti výskytu virových nákaz (obr. 4.1.1). Při podrobnější analýze výsledků lze jednoznačně říci, že trend množství virových nákaz je klesající. Graf zobrazuje vývoj za období roků 2005 a 2006. Klesající trend naznačuje, že uživatelé i výrobci software začali brát problematiku virů vážně a díky implementaci nových bezpečnostních prvků a osvětě uživatelů se riziko nakažení virem v posledních letech snižuje. Navíc poškození uživatele virem nepřináší nikomu žádný užitek, snad pouze v případě, že jde o poškození konkurence způsobením škody.

Obr. 4.1.1 Virus rates – množství virových nákaz v e-mailech

Zdroj: http://www.messagelabs.com/resources/mlireports[8]

4.2 Analýza množství spamu

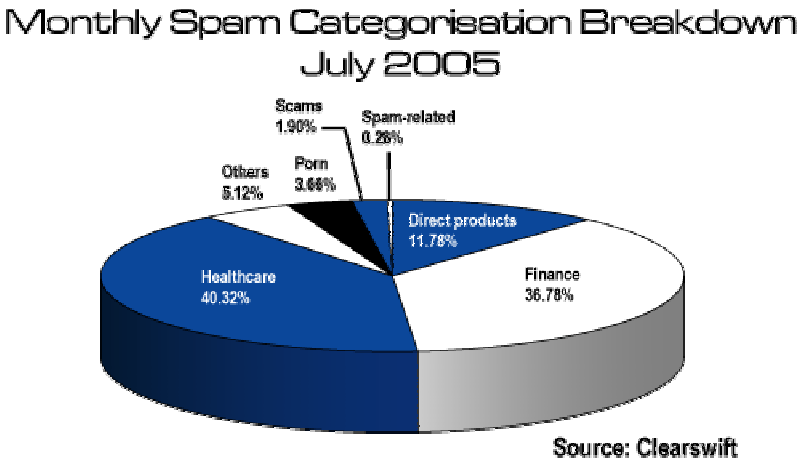
Množství spamu poslední dobou velmi narůstá. Je to především proto, že spam je základním nositelem pro všechny možné druhy počítačové infiltrace. Hlavní pohonnou silou spamu jsou finanční prostředky, které přináší spamová reklama. Nevyžádaná pošta jako nositel reklamy je jednoduchá, rychlá, relativně levná, celoplošná a díky spyware i cílená. Množství zachycené nevyžádané pošty za období 2005 a 2006 zobrazuje graf na obr. 4.2.1. na další straně.

Obr. 4.2.1 Spam rates – množství nevyžádané pošty

Zdroj: http://www.messagelabs.com/resources/mlireports[8]

4.3 Analýza struktury spamu

Analýzy společnosti Clearswift z června r. 2005 (viz obr. 4.3.1) zobrazují strukturu spamu, který byl rozesílán ve Velké Británii. Výsledky měsíčních analýz se mění maximálně o jedno procento, takže výsledky lze považovat za směrodatné i po delší časové období.



Obr. 4.3.1 Struktura spamu za měsíc červen 2005

Zdroj: http://www.clearswift.com [9]

77,1% veškerého spamu tvoří zprávy a reklamy z oblasti financí a zdravotnictví. Ve zdravotnictví jde nejčastěji o nabídku potravinových doplňků, podpůrných prostředků pochybné kvality, které slibují např. kvalitnější sexuální život. 11.78% zaujímá nabídka konkrétních produktů a 3,66% spamu je

z oblasti pornografie. 1,9% zaujímají podvodné e-maily, které se snaží uživatele oklamat, či finančně poškodit.

4.4 Analýza množství phishingu

Velmi nebezpečný nárůst zaznamenal phishing (phishingové zprávy jsou součástí nevyžádané pošty). Organizované gangy se stále častěji pokoušejí vydávat za některou z finančních institucí a pod záminkou se snaží z uživatele vymámit jeho přístupové údaje. Díky tomu, že tento způsob kriminality je finančně velmi výnosný, zažívá v poslední době masový nárůst (viz graf na obr. 4.4.1) a trend je vzestupný.

Obr. 4.4.1 Phishing – vývoj výskytu phishingu v e-mailech

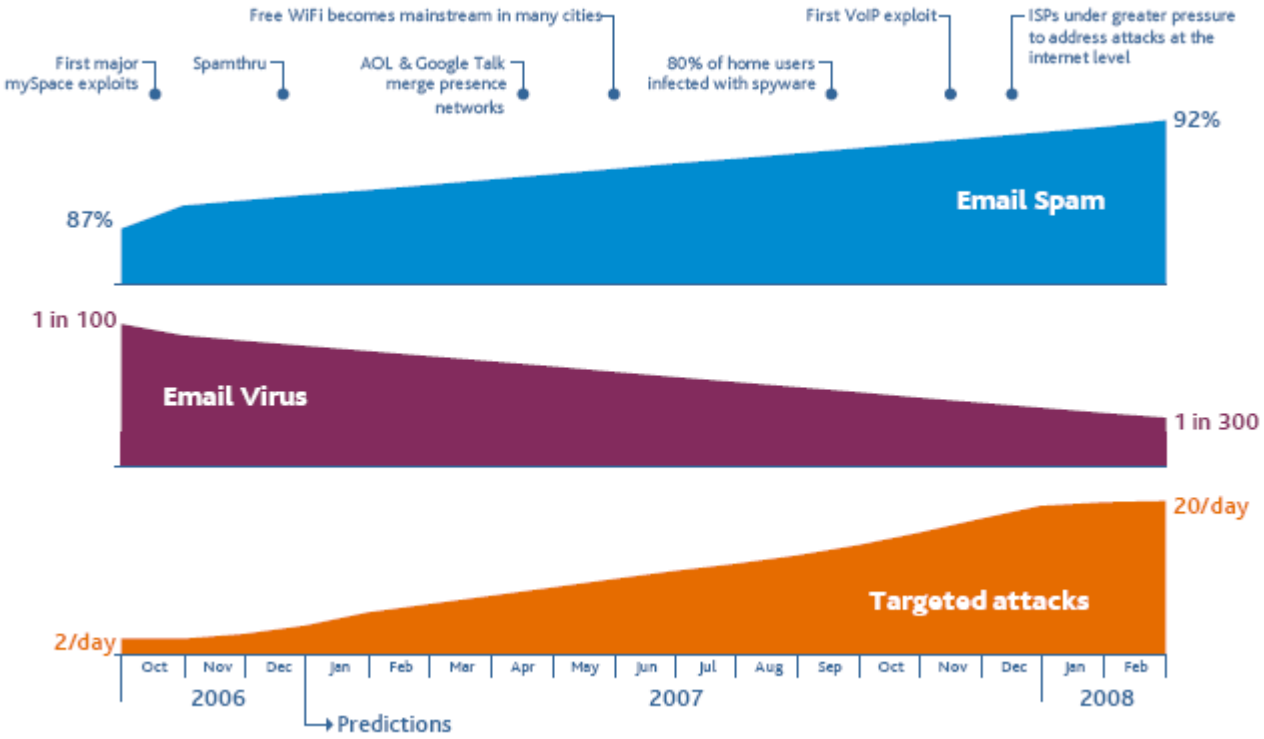
Zdroj: http://www.messagelabs.com/resources/mlireports[8]

Útočníci využívají údajů získaných phishingem k odčerpání finančních prostředků z účtů uživatelů Částky, které měsíčně odčerpávají mohou dosahovat pouze několika korun, takže si toho uživatel ani nevšimne, nebo tomu nevěnuje pozornost. Takto malou částku někdy považuje za nějaký poplatek bance. Útočníci této metody mohou využívat u tisícovek uživatelů a přijít tak pravidelně k velkým finančním obnosům.

4.5 Prognóza vývoje

Na základě dosavadních výsledků sledování je možné stanovit další vývoj různých forem napadení (viz obr. 4.5.1).

Množství spamu v e-mailových schránkách se bude nadále zvyšovat. Naštěstí už i většina tuzemských tzv. free e-mailových schránek (seznam.cz, centrum.cz, atd.) poskytuje kvalitní anti-spamové filtry, které nevyžádanou poštu nepropustí do naší schránky, takže množství spamu ve schránce koncového uživatele není tak horentní.



Obr. 4.5.1 Prognóza dalšího vývoje

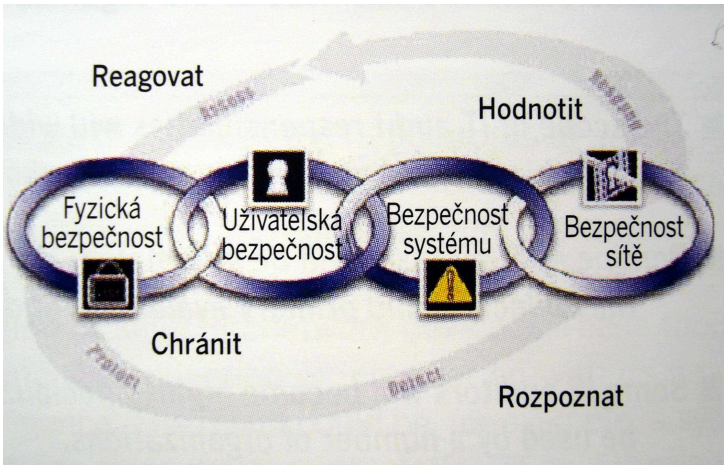
Zdroj: http://www.messagelabs.com/resources/mlireports[8]

Virových nákaz bude i nadále ubývat. Mimo již zmíněné důsledky k tomu přispívá i určitá větší rozmanitost používaných operačních systémů a zabezpečovacího software. Pro každý PC je tak potřeba jinak modifikovaný virus. Oproti tomu do se do budoucna častěji setkáme s cílenými útoky (obr. 4.5.1. graf „Target attacks“). Sem se zařazuje i phishing. Jde o útoky na

vybrané uživatele, firmy (např. na klienty určité banky, uživatele určitého softwarového produktu, atd.).

5 Prostředky prevence a obrany

Velmi názorné je schéma na obrázku 5.1. Zobrazuje principy zabezpečení počítače. Mluvíme-li o zabezpečení počítače, je třeba si uvědomit, že ochrana proti počítačové infiltraci není jedinou úrovní zabezpečení počítače. I ten nejlépe softwarově i hardwarově zabezpečený počítač (notebook) může odcizit zloděj a způsobí tak škodu mnohem větší než veškerá počítačová infiltrace.



Obr. 5.1 Úrovně zabezpečení

Zdroj: Vize informační bezpečnosti [3]

Úrovně zabezpečení počítače lze rozdělit do následujících 4 kategorií (obr. 5.1) :

- Úroveň fyzické bezpečnosti
- Úroveň uživatelské bezpečnosti
- **Úroveň bezpečnosti systému**
- **Úroveň bezpečnosti sítě**

5.1 Úroveň fyzické bezpečnost

Jedná se o zabezpečení počítače proti odcizení nebo zničení. Jde o zabezpečení na nejnižší úrovni, ale i tato úroveň bývá někdy podceňována. Firma (uživatel) musí zabezpečit, aby přístup k výpočetní technice měli jen

oprávnění pracovníci. Notebooky nesmí zůstávat bez dozoru, případně lze využít zabezpečení speciálním zámkem (notebook lze uzamknout ke stolu, PC lze zabudovat do speciálních uzamykatelných stolů, monitory lze také uzamknout ke stolu). Pozornost je třeba věnovat i zabezpečení médií (diskety, CD, flash disky) a grafických i jiných výstupů. Pokud např. důležitý dokument zůstane dlouho ležet nevyzvednutý v tiskárně, hrozí také riziko jeho zcizení.

5.2 Úroveň uživatelské bezpečnosti

Ne všichni uživatelé potřebují přístup ke všem datům, je třeba stanovit vhodnou politiku přístupu a určit jednotlivým uživatelům pravomoce práce s počítačem. Dnešní operační systémy poskytují kvalitní služby v oblasti přístupových práv. V menších firmách je ideálním postupem nastavit všem pracovníkům jen základní omezená přístupová práva a ty potom postupně rozšiřovat v závislosti na tom, jak se rozšiřuje jejich pracovní nasazení a kam je vyžadován přístup.

5.3 Úroveň bezpečnosti systému a bezpečnosti sítě

Zabezezpečení počítače na této úrovni se podrobněji věnujeme. Systém je ohrožován riziky popsanými ve článku „formy napadení“. Proti těmto útokům je zapotřebí systém účinně chránit, aby nedošlo k infiltraci do systému. Pro zabezpečení systému a sítí se používají následující prostředky.

5.3.1 Bezpečnostní pravidla

Nejdůležitějším prvkem při navrhování zabezpečení jsou pravidla, které uživatel musí dodržovat. Pokud budeme dbát na jejich striktní dodržování, můžeme předejít mnoha rizikům, a to i v případě že používáme špatné zabezpečení (nebo nemáme žádné).

- Používat správně nakonfigurovaný bezpečnostní software (firewall, antivir)
- Pravidelná instalace aktualizací softwarových produktů
- Používání „silných hesel“
- Nenavštěvovat nedůvěryhodné webové stránky (blokovat je)
- Neotevírat neověřené přílohy e-mailů
- Zálohovat důležitá data

5.3.2 Antivirové programy

Antivirový software má za úkol chránit počítač (server) proti virům, trojským koním a další počítačové infiltraci. Jeho úkolem je sledovat, zda na všech vstupech a výstupech počítače (portech) nedochází k neoprávněné infiltraci. Zároveň provádí průběžnou kontrolu stávajících dat (skenery). Infiltraci se snaží rozpoznat díky databázi, ve které jsou zapsány sekvence virů, které program vyhledává v souborech. Antivirový program sleduje i podezřelé chování souborů a na jeho základě dokáže vir odhalit.

Virus Bulletin je prestižní ocenění udělováné antivirovým programům, které dokáží detekovat 100% současné nejrozšířenější počítačové infiltrace (malware) bez falešných poplachů. Výsledky pravidelných testů jsou zveřejňovány na serveru www.virusbtn.com. Díky tomu, že je většina antivirových produktů testována pravidelně od r. 1998, je možné sestavit tabulku (tab. 5.3.2.1 na další straně), která bude porovnávat úspěšnost antivirů

od r. 1998 do r. 2007. Data jsou uvedena pouze pro vybrané nejznámější produkty, které jsou běžně dostupné na českém trhu.

Názvy produktů softwarových společností se mění a testy jsou prováděny vždy na produktech vydaných za celé období, kdy je daná společnost zařazena do testu (nejčastěji od. r. 1998, pokud nevznikla později). Výsledky tedy nelze vztahovat pouze ke konkrétnímu softwarovému produktu, ale k úspěšnosti antivirového software, který společnost dosud vydala.

Společnost	Současný produkt	Testů celkem	Z toho úspěšných	Z toho neúspěšných	Úspěšnost antivirového programu v testech
Alwil Software	Avast!	42	23	19	54,76%
BitDefender	BitDefender Antivirus	20	14	6	70,00%
CA eTrust	CA eTrust	42	30	12	71,43%
Eset	***NOD32***	***47***	***44***	***3***	***93,62%***
F-Secure	F-Secure Anti-Virus	39	26	13	66,67%
Grisoft	AVG	39	17	22	43,59%
Kaspersky	Kaspersky Antivirus	52	38	14	73,08%
McAfee	McAfee Virus Scan	50	31	19	62,00%
Symnatec Norton	Norton Antivirus	44	38	6	86,36%
Trend Micro	PC-cilin	24	16	8	66,67%

Tab. 5.3.2.1 Úspěšnost antivirových programů v testech Virus Bullentin

Zdroj testů: www.virusbtn.com [10]

Dlouhodobě nejúspěšnější v detekci nejrozšířenější počítačové infiltrace je společnost ESET s.r.o., která je známá svým antivirovým programem NOD32. Tuzemská společnost Grisoft, která vydává antivirový program AVG z testů vychází jako outsider.

S velmi zajímavým nápadem přišel Rakušan Andreas Clementi. Rozhodl se, že ozkouší úspěšnost antivirových programů odhalovat nová rizika (tedy především úspěšnost tzv. heuristické analýzy). Vždy k určitému datu „konzervuje“ nejaktuálnější verze antivirových programů a tři měsíce po té zjišťuje jak tyto neaktuální verze reagují na nové počítačové hrozby. Tento test nazývá „Retrospective / ProActive test“ (tab. 5.3.2.2 na další straně)

Společnost	Testovaný produkt	Verze	Rychlost vyžádaného skenování	Počet falešných poplachů	Detekovaných počítačových infiltrací (z nových)
Alwil Software	Avast! Professional	4.7.942	průměr	málo	26%
GriSoft	AVG Anti-Malware	7.5.441	pomalá	hodně	8%
F-Secure	F-Secure Anti-Virus	7.01.126	pomalá	velmi málo	31%
Kaspersky Labs	Kaspersky AV	6.0.2.614	průměr	velmi málo	9%
McAfee	McAfee VirusScan	11.1.124	rychlá	málo	24%
Eset	***NOD32 Anti-Virus***	***2.70.23***	***rychlá***	***velmi málo***	***68%***
Symnatec	Norton Anti-Virus	14.0.0.89	rychlá	žádný	24%

Tab. 5.3.2.2 Úspěšnost antivirových programů v testu odhalování nových infiltrací (květen 2007)
Zdroj dat testu: www.av-comparatives.org [11]

Nejlépe nové hrozby detekuje NOD32 Anti-Virus od společnosti Eset s.r.o. Detekoval 68% nových počítačových infiltrací z portfolia, a to s velmi málým počtem falešných poplachů (tzn. , že infiltrace skoro vždy detekoval správně). I při těchto parametrech zůstává jeho skenování rychlé.

Tuzemský Grisoft s produktem AVG Anti-Malware opět zůstal oproti ostatním testovaným produktům velmi pozadu. Produkt AVG Anti-Malware detekoval pouze 8% z portfolia nových hrozeb a přitom měl velký počet falešných poplachů (detekoval hrozby tam, kde žádné nebyly) a jeho skenování bylo pomalé, takže delší dobu zatěžovalo počítač.

Jako bezpečností řešení pro ochranu před viry lze tedy jednoznačně doporučit NOD32 Anti-Virus od ESET s.r.o., který uspěl v obou měřeních.

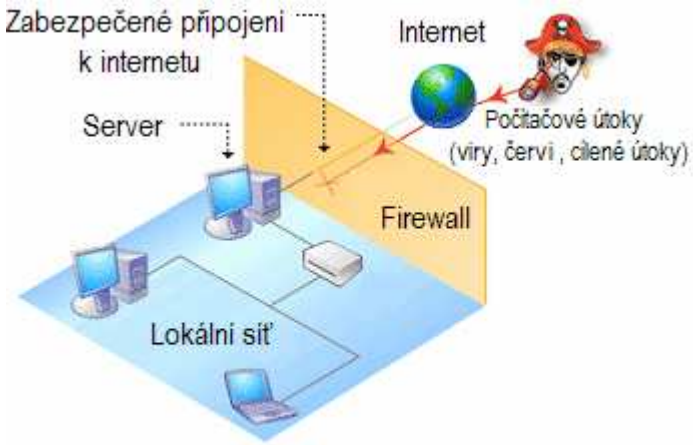
5.3.3 Antispyware

Atispyware poskytuje ochranu proti trojských koním, keyloggers a jinému spyware. Dnešní trend směřuje k integraci do tzv. all-in-one (vše v jednom) produktům, takže se můžeme čím dál častěji setkat např. s antivirovým programem, který má integrovaný i antispyware. Taková kombinace je mnohem výhodnější, protože spyware prohledává soubory podobně, jako antivirové programy. Kombinace all-in-one produktů je méně náročná na výkon, než oddělené řešení. Některé činnosti (např. skenování souborů) díky integraci totiž

nemusí být prováděny paralelně, každým programem zvlášť. Mezi nejlepší antispyware patří Lavasoft Ad-aware, ZoneAlarm Anti-Spyware, Spybot Search and Destroy. Některé z těchto programů lze v základní verzi stáhnout zdarma.

Základní zabezpečení proti spyware již systém Windows XP i Windows Vista obsahuje. Jde o program Windows Defender. Někteří možná pamatují antispywarový program „GIANT AntiSpyware“. Ten byl jedničkou ve svém oboru. V roce 2004 společnost GIANT zakoupil Microsoft a GIANT AntiSpyware převzal pod svá křídla a přejmenoval jej na Windows Defender.

5.3.4 Firewall



Obr. 5.3.4.1 Nasazení firewallu

Zabezpečení připojení do sítě provedeme pomocí firewallu. Firewall zabezpečuje počítač proti útokům „zvenčí“. Blokuje veškerou neautorizovanou komunikaci, tj. přijetí počítačových virů, červů, zamezuje hackerským útokům (obr. 5.3.4.1). Firewall však nedokáže zabránit otevření příloh infikovaných e-mailů, neblokuje ani nevyžádanou poštu. Virů a červů, které již počítač obsahuje se prostřednictvím firewall také nezbavíme (k tomu slouží antivirový software). Největší nebezpečí počítači hrozí je-li připojen přímo k Internetu, tedy pokud má veřejnou IP (Internet Protocol) adresu (např. vytáčené připojení, kabelové připojení UPC a Chello). Pokud se k síti Internet připojuje prostřednictvím poskytovatele služeb Wi-fi nebo ADSL, pravděpodobně nebudeme mít veřejnou IP adresu, ale budeme „schováni“ za zabezpečeným serverem poskytovatele. To ovšem neznamená, že nás nemůže vůbec nikdo ohrozit, ale riziko je podstatně nižší. Firewall by měl být nepostradatelnou součástí každého počítače, který je připojen k síti.

Dle realizace firewallu jej lze dělit na **softwarový** (nebo-li personální) a **hardwarový**. Oba nabízejí podobnou kvalitu zabezpečení. Hardwarový firewall navíc nazatěžuje výkon hostitelské stanice a je rychlejší. Obecně se považuje za nejvhodnější řešení firemní přístupové servery vybavit hardwarovým firewallem a klientské, či domácí počítače, vybavit softwarovou variantou firewallu.

Pokud imlementujeme firewall na serveru (zabezpečení LAN), doporučuje, se dle velikosti a použití sítě, implementovat i softwarové firewally na připojené počítače. Hardwarový firewall na serveru zabezpečí síť proti útoku „zvenčí“, ale pokud do firemní sítě někdo připojí např. nakažený notebook nebo přinese počítačovou infiltraci na jiném nosiči (flash, CD), může dojít k napadení sítě „zevnitř“. Takovému napadení by samotný hardwarový firewall implementovaný na serveru zabránit nedokázal.

Mezi kvalitní zástupce firewallu lze zařadit řešení firem Outpost, ZoneAlarm, Kerio, Symnatec.

Při instalaci firewallu je třeba věnovat zvýšenou pozornost jeho konfiguraci. Je nutné přesně stanovit, které přístupy k počítači jsou povolené a které nikoliv. Špatně nakonfigurovaný firewall neplní svojí funkci a počítač účinně nechrání.

Někteří výrobci označují termínem firewall i **packetové filtry**. Označení není nesprávné, ale packetové filtry (jsou součástí směrovačů) neposkytují účinnou obranu počítače. Tyto filtry rozlišují příchozí packety pouze podle zdojové a cílové IP adresy a portu. Neumožňují informovat uživatele o podezřelé aktivitě.

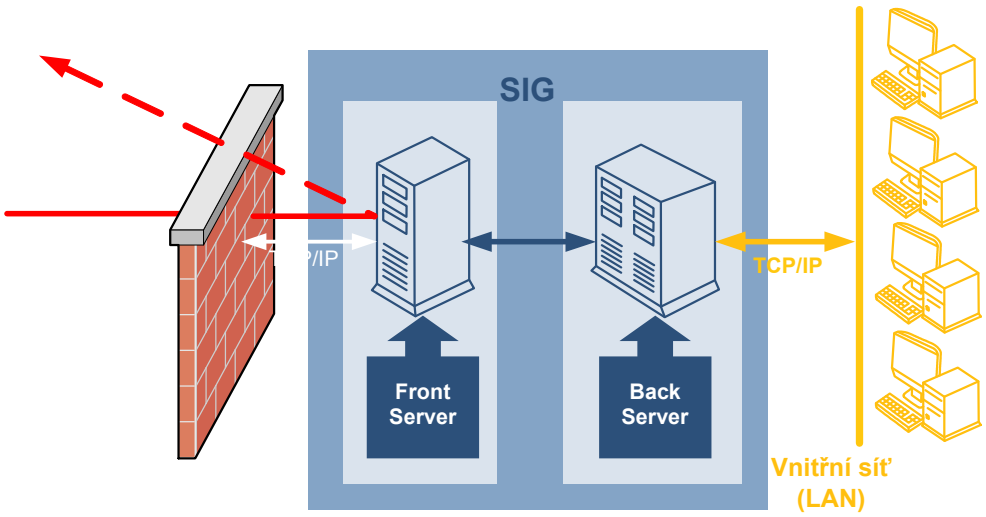
Velice účinné řešení představuje **stavový firewall**. Umožňuje nastavit pravidlo pro navazování připojení pouze z vnitřní sítě ven. Provoz z venkovní strany (internetu) je blokován. Umí odhalit i útoky typu spoofing (podvržené pakety, které se tváří, jakoby se vracely do sítě).

Firewall typu proxy rozumí obsahu paketů. Je třeba upravit klientské programy. Nevýhodou je nižší výkon, protože proxy je třeba vytvořit pro každou aplikaci a službu přistupující k Internetu.

5.3.5 Technologie SIG

Velmi zajímavý počin společnosti A && L soft, který implementuje více bezpečnostních prvků a riziko napadení počítače (nebo lokální počítačové sítě) zvenčí eliminuje. Bezpečnostní řešení SIG (Secure Internet Gateway) řeší propojování sítí zcela nekonvenčním způsobem a nabízí tak vyspělou ochranu před útoky z Internetu.

Řešení se základá na propojení dvou oddělených sítí – vnitřní sítě LAN (Local Area Network) a vnější sítě Internet, prostřenictvím dvou serverů (Back server a Front server). SIG pracuje jako síťový most, který propojuje dvě



Obr. 4.1.1 Zapojení Secure Internet Gateway Zdroj: http://www.alsoft.cz [12]

TCP/IP (Transmission Control Protocol/Internet Protocol) sítě a směruje povolené příchozí spojení z jedné sítě do druhé. Zapojení znázorňuje obrázek 5.3.5.1.

Front server je připojen k síti Internet (na typu připojení k Internetu nezáleží). Front server nemá vlastní konfiguraci a je zcela řízen Back serverem. Připojený firewall jen zdvojuje ochranu.

Back server řídí celý bezpečnostní systém, spravuje i konfiguraci Front serveru, verifikuje navázaná spojení a zasílá příkazy pro Front server. Back server je pro útočníky z Internetu nedostupný.

Front server je proprietárním protokolem point to point pomocí sériové linky (RS 232) připojen k Back serveru. Mezi oběma servery nexistuje jiné propojení. Prostřednictvím sériové linky se nepřenáší žádné systémové údaje o TCP/IP připojení.

Problematikou celého sytému je, že propustnost RS 232 je pouze 921 kbit/s. Rychlost je tedy zapotřebí zvýšit (znásobit), což lze provést použitím multiportové karty (viz obr. 5.3.5.2), která rozšíří počet portů pro RS 232 a to v závislosti na modelu karty až na 16 portů.

Obr. 5.3.5.2 Multiportová karta pro sběrnici PCI-E
Zdroj: http://www.moxa.cz

5.3.5.1 Implementace technolgie SIG

Většina firem již nějaký server pro zprostřekování připojení má. K tomuto serveru je nutné připojit multiportovou kartu pro RS 232 (cena se pohybuje od 2 do 10 tis. Kč dle počtu portů). Dále je třeba zřídit nový server (Back server), který také bude mít multiportovou kartu (nejlépe úplně stejnou jako Front server). Prostřednictvím sériových linek se oba servery propojí. Připojení k internetu spolu se zabezpečením, které bylo realizováno na původní firemním serveru, můžeme používat i nadále (firewall, antivirový program, atd.), jen lokální síť je třeba připojit k Back serveru. Pro funkci Back serveru zcela postačuje běžný kancelářský počítač, takže náklady na jeho zřízení nemusí přesáhnout 15 tis. Kč. Nejsložitější operací je instalace systémů pro servery a konfigurace obou serverů. Dle požadavků bude instalace případ od případu odlišná, a proto nelze stanovit obecný postup, jak při konfiguraci postupovat.

6 Závěr

Práce „zabezpečení počítače“ podává ucelený obraz o problematice v oblasti bezpečnosti přístupu k počítači a poukazuje na jednotlivé možnosti nebezpečí v podobě virů, trojských koní, adware a jiného škodlivého software.

Práce hodnotí současnou situaci a ukazuje, že problematika je mnohem rozsáhlejší, než si připouštíme. 1,47% ze všech odeslaných e-mailů je napadeno virovými nákazami, 86,2% elektronické pošty spadá do kategorie spamu a 1 z 274,2 (0,36 %) odeslaných e-mailů je z oblasti phishingu. Spam je v této oblasti velmi významným hráčem, protože je i nositelem virových nákaz, spyware, phishingu a dalšího malware (data z r. 2006).

Prognózy dalšího vývoje naznačují, že množství nevyžadané pošty i nadále poroste. Množství zpráv nakažených viry by se podle předpokladů mělo snižovat, ale cílené útoky zaznamenají prudký vzestup. Mezi cílené útoky zařazujeme i phishing.

Problematika nevyžádané pošty v ČR není tak velkou hrozbou, protože spam pochází především z anglicky mluvících zemí, takže nevyžádanou poštu, která i přes dobře nastavené filtry projde až do naší schránky dokážeme jednoduše odlišit od ostatní pošty. Struktura spamu zůstává neměnná – 77,1% tvoří zprávy a reklamy z oblasti financí a zdravotnictví (nejčastěji se jedná a reklamu na pochybné finanční služby a potravinové doplňky).

Díky těmto faktům se do pořadí zájmu dostávají prostředky obrany a prevence proti bezpečnostním hrozbám. Průkopníkem v oblasti zabezpečení lokálních sítí je technologie SIG (Secure Internet Gateway), která zcela eliminuje riziko napadení sítě „zvenčí“

Firewall se stává běžnou integrovanou součástí modemů sloužících pro připojení k internetu. Operační systémy již v základu poskytují ochranné prvky a programátoři poskytují aktualizace bezpečnosti systému v závisloti na ohrožení novými infiltracemi. Nepostradatelným je i kvalitní antivirový program, který je

účinným prostředkem nejen proti již infikovanému počítači, ale slouží i jako preventivní nástroj proti infiltraci.

Pokud se v tomto směru bude situace i nadále zhoršovat, nevyhneme se přísnějšímu legislativnímu rámci, který bude regulovat používání Internetu a prezentaci na webu. Světová síť by tak mohla ztratit svoji pověstnou „volnost".

Odpověď na otázku, zda se situace vyvine tímto směrem, přinese budoucnost.

7 Použité zdroje

[1] Kasík, P. *První počítačové viry byly docela hodné* [online]. [cit. 23. 11. 2006]. URL: <http://technet.idnes.cz/prvni-pocitacove-viry-byly-docela-hodne-f05-/software.asp?c=A070112_184415_bezpecnost_dno>

[2] Všetečka, R. *Viry jsou staré několik desetiletí. Chcete znát jejich vývoj?* [online]. [cit. 23. 11. 2006].
URL: < http://technet.idnes.cz/viry-jsou-stare-nekolik-desetileti-chcete-znat-jejich-vyvoj-plv-/software.asp?c=A041103_5285981_bezpecnost>

[3] Humlová. A. – Seige V. a kol. *Vize informační bezpečnosti 2002/2003*. Vydání první. Praha: Tate International, 2002. ISSN 1211-8737.

[4] *Internetová encyklopedie Wikipedia* [online]. [cit. 8. 12. 2007].
URL: <http://cs.wikipedia.org>

[5] *Průvodce zabezpečením pro malé organizace* [online]. Microsoft . [cit. 23. 1. 2007]. URL: <http://download.microsoft.com/download/6/5/9/659a0534-b0c1-4e42-b09d-d907bc297c5d/eSecurityGuideCZ.pdf>

[6] *HOAX.cz* [online]. [cit. 8. 3. 2007]. URL: <http://www.hoax.cz>

[7] *Virový radar on-line* [online]. [cit. 5. 6. 2007]. URL: <http://www.virovyradar.cz>

[8] MessageLabs Intelligence: 2006 Annual Security Report [online]. [cit. 5. 6. 2007]. URL: <http://www.messagelabs.com/resources/mlireports>

[9] *Clearswift* [online]. [cit. 6. 6. 2007]. URL: <http://www.clearswift.com>

[10] *Virus Bulletin* [online]. [cit. 10. 6. 2007]. URL: <http://www.virusbtn.com>

[11] *AV-comparatives* [online]. [cit. 13. 6. 2007]. URL: <http://www.av-comparatives.org>

[12] SREBE, M. - PERKINS, Ch. *Firewally a proxy-servery: Praktický průvodce*. Vydání první. Brno: Computer Press, 2003. ISBN 80-7226-983-6.

[13] *A && L soft, s. r. o.* [online]. [cit. 15. 6. 2007]. URL: <http://www.virusbtn.com>

[14] WOLFE, P. a kol., Antispam. Brno: Computer Press, 2004. ISBN 80-251-0479-6.