Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta – Katedra fyziky

Bezpečnost počítačových sítí s operačním systémem MS Windows

Bakalářská práce

Vedoucí práce: Ing. Michal Šerý

Autor: Milan Batysta

Anotace

Bakalářská práce pojednává o bezpečnostních rizicích osobních počítačů připojených do počítačových sítí. Práce podává ucelený přehled o vývoji zabezpečení jednotlivých verzí OS společnosti Microsoft od jejich historického počátku až po uvedení na trh verze OS Windows Vista koncem roku 2006 a o nejvýznamnějším malware a dalších hrozbách.

Cílem práce bylo praktické ověření možné infiltrace osobního počítače malwarem. Testován byl v praxi nejčastěji používaný OS Windows 2000 a Windows XP. Náležitá pozornost byla věnována i beta verzi OS Windows Vista. Pro zvolené OS jsou v práci definovány bezpečnostní standardy. V rámci testování jsou tyto standardy rozšířeny o další bezpečnostní SW. Výsledky provedených testů potvrdily, že bezpečnost OS se zvyšuje s jeho novějšími verzemi a zvýšení bezpečnosti rovněž zajišťuje aktivní ochrana pomocí dalšího bezpečnostního SW. Tyto ověřené předpoklady nejsou překvapením, ale spíše deklarují pro všechny uživatele PC nebezpečnost používání počítače při porušení bezpečnostních standardů. Práce jak svou teoretickou částí, tak výsledky testů, může přispět k vyšší míře bezpečnostního vědomí nejen specialistů ICT, ale každého uživatele PC.

Annotation

My bachelor research is about safety risks for personal computers connecting in system. My work gives comprehensive view of secure development of successsive verses OS Microsoft from their historical beginning until putting the verse OS Windows Vista on the market at the end of year 2006 and about the most significant malware and other menaces.

The aim of my work was the practical testing of possible infiltration malware into PC. The most frequently used OS Windows 2000 and Windows XP were tested. Appropriate attention was followed also to the beta verse of OS WindowsVista. The security standards in this work are defined for chosen OS. Within the framework of testing are these standards spread to other safety OS. The results of these tests ratified that safety OS is increased with its newer verses and active protection with other safety SW provides increasing of safety too. These verified hypothese are not surprise but they rather declare a danger for all PC users applying computer by breaking safety standards. The work can give both-theoretical part and test results-higher degree of safety consciousness not only for specialists ICT but for every PC user.

Prohlašuji, že předloženou práci jsem vypracoval samostatně a pouze s použitím uvedené (citované) literatury.

V Prachaticích dne 27.11. 2006 Milan Batysta

Děkuji svému vedoucímu diplomové práce Ing. Michalovi Šerému za odborné konzultace, rady a připomínky při tvorbě této bakalářské práce.

OBSAH

1 Úvod

Potřeba propojit osobní počítače do počítačové sítě s sebou přinesla pro uživatele PC nový druh rizik a nebezpečí, jejichž eliminace stojí společnosti i jednotlivce obrovské finanční prostředky a v případě realizace hrozby velké finanční ztráty. Proto manažeři ICT věnují zajištění bezpečného provozu ICT, zejména technologii počítačových sítí, oprávněnou pozornost. Trestná činnost v digitálním prostředí výrazně narůstá a je více organizovaná než v minulosti. Vyplývá to ze zprávy antivirové společnosti McAfee o virtuální kriminalitě. Mezi nové počítačové delikty patří především podvodné získávání hesel nebo čísel kreditních karet, on-line vydírání či investiční podvody. Odhaduje se, že jen počítačové viry ročně celosvětově způsobují finanční škody okolo 20 miliard dolarů. Skutečné škody způsobené používáním internetu jsou však pravděpodobně ještě vyšší, protože řada firem počítačové útoky nezveřejňuje kvůli obavám ze ztráty důvěryhodnosti. Počítače současné doby jsou téměř vždy připojeny do datové sítě, a to buď prostřednictvím LAN, WAN nebo přímo do celosvětové sítě internet. V každém ohledu jsou neustále vystaveny potencionálnímu riziku napadení malwarem. Toto riziko je vždy větší pro podnikatelskou sféru, může být však zdrcující i pro jednotlivé domácí uživatele PC. Je vhodné rozlišovat zabezpečení počítačů pro domácí použití nebo pro podnikovou sféru. Každá z těchto dvou sfér vyžaduje konkrétní specifické postupy a zabezpečení, i když se v některých případech shoduje.

Cílem teoretické části této práce, je popsat aktuální bezpečnostní rizika počítačové sítě s pohledu nejčastěji používaných verzí OS platformy MS Windows. Cílem praktické části, je realizací bezpečnostních testů ověřit stupeň zabezpečení OS a navrhnout optimální doplnění OS Windows o další SW druhých stran tak, aby byla bezpečnost plně integrovaná.

V současné době (rok 2006) je OS MS Windows předinstalován na cca. 90% všech osobních počítačů po celém světě a tím se stává nejpoužívanějším OS. K volbě zpracování tohoto tématu bakalářské práce mne přivedly zejména mé praktické zkušenosti specialisty ICT – správce počítačové sítě. Více jak 20% mé pracovní doby musím řešit bezpečnostní problematiku související např. s plánováním zabezpečení, včasnou detekcí, odhalením a odstraněním nebezpečného malware. Zdroje pro teoretickou část práce jsem hledal převážně na internetu a dále v odborných publikacích

a časopisech. V praktické části práce jsem potom uplatnil své vlastní zkušenosti s administrací integrované bezpečnosti OS MS Windows. Vzhledem k tomu, že Microsoft vydal několik verzí OS Windows, včetně verzí určených pro instalaci na servery, zaměřil jsem se na dvě nejvíce používané desktopové verze, a to Windows 2000 a Windows XP.

V době realizace mé bakalářské práce bylo již známé přibližné datum uvedení nového OS Windows Vista na trh, a proto jsem se zaměřil i na tuto verzi a otestoval beta verzi RC1 Build 5600. Protože uvedení konečné verze tohoto OS je plánováno až na listopad 2006, publikuji v této práci pouze výhody i nevýhody zjištěné testováním beta verze OS Windows Vista.

2 Operační systémy Windows a jejich bezpečnost

2.1 Stručná historie OS Windows

a) MS-DOS

Základy operačního systému Windows sahají až do roku 1981. Tehdy přišel na trh první počítač s nainstalovaným operačním systémem MS-DOS. Tento OS vycházel ze systému QDOS(Quick and Dirty Operating System), jež firma Microsoft koupila za pouhých 50,000 dolarů od firmy Seattle Computer Products. Jednalo se o 16-ti bitovou verzi OS firmy Microsoft. Díky tomuto operačnímu systému prudce vzrostl prodej a rozvoj mikropočítačů.

Přesto že byl MS-DOS velkým krokem dopředu, stále mu chyběli důležité funkce jako multitasking, neschopnost pracovat s operační pamětí větší než 640 kB nebo s disky většími než 30 MB. Dále také chybělo přívětivé grafické prostředí (GUI). OS umožňoval pracovat pouze jednomu uživateli bez jakéhokoli zabezpečení. Na bezpečnost operačního systému MS-DOS nebyl v té době kladen důraz, protože nebyl znám žádný typ virové hrozby. První informace o viru se objevily až v roce 1983.[14]

b) MS Windows 1.0

První verze OS MS Windows 1.0, byla uvedena 20. listopadu 1985 a jednalo se o první pokus společnosti Microsoft implementovat grafické uživatelské rozhraní (GUI) na platformě PC. MS Windows 1.0 byly původně pouze front-end prostředí pro MS-DOS a inspirací se stal MacOS. V této verzi bylo možné se přepínat mezi jednotlivými okny, která se ale nemohla překrývat a musely se skládat vedle sebe do tzv. mozaiky. V roce 1987 byla uvedena verze 2.0, která nedostatek s překrýváním oken odstranila. Přestože v době vydání tohoto operačního systému již byl znám první počítačový virus a další nové vznikaly, nebyl stále kladen důraz na bezpečnost operačního systému.[14]

c) MS Windows 3.x

Velkého rozšíření se dočkala až verze MS Windows 3, která byla uvedena v roce 1990. V následujícím roce 1991 byla vydána verze Multimedia Extension, která umožňovala pracovat s multimédii. V roce 1992 přišel na trh MS Windows 3.1, který se stal nejvíce rozšířeným operačním systémem v té době. Přinesl řadu vylepšení např. podporu OLE nebo lepší podporu tiskových zařízení, větší databázi ovladačů a další.

Později byla ještě vydána verze MS Windows 3.11, která obsahovala podporu sítí a byla tedy primárně určena pro firemní prostředí. Ale i v této verzi byla bezpečnost OS ještě v počátcích a nebylo možné oddělit jednotlivé uživatelské účty.[14]

d) MS Windows 95

Velký zlom nastal v roce 1995, kdy byl na trh uveden OS MS Windows 95. Tato verze s sebou přinesla řadu novinek, a to především podporu dlouhých názvů souborů(do té doby byly podporovány pouze názvy o celkové délce 8 znaků), částečným 32-bitovým jádrem nebo vylepšenou podporou síťového prostředí pomocí implementace TCP/IP protokolu. V neposlední řadě doznalo změn i grafické prostředí, díky kterému můžeme Windows 95 označit za přelomovou verzi MS Windows. Z hlediska bezpečnosti bylo implementováno multi-uživatelské prostředí. Tzn. že každý uživatel si mohl upravit plochu podle svých představ, mohl si svůj účet zaheslovat a pomocí úprav v registrech, se mohly provádět různé restrikce a omezení daného uživatele, a tím částečně zabránit instalaci nežádoucích programů. Tyto restrikce, ale byly zatím proti systému Windows NT velmi omezené. Ukládání uživatelských hesel bylo prováděno do souboru s příponou pwl v nekryptované podobě a z hlediska bezpečnosti se tento systém ukázal jako zcela nevhodný, jelikož zcizení hesla z tohoto souboru bylo otázkou několika vteřin. Navíc oprávnění pro čtení tohoto souboru mají všichni uživatelé. Pro každého uživatele je zvlášť vytvořen příslušný soubor, do kterého se hesla ukládají.[4]

e) MS Windows 98

V roce 1998 byl uveden OS Windows 98. Jednalo se o přepracovaný OS Windows 95, který byl již zcela 32-bitový. Změn doznala i podoba grafického prostředí viz. obrázek níže, i když je znát nepodobnost s předchozí verzí Windows 95. Hlavní novinkou byla fungující podpora USB. Protože tento systém obsahoval některé chyby a nebyl zcela stabilní, byla v roce 1999 vydána další verze, a to MS Windows 98 SE (Second Edition). Bohužel uživatelská hesla se stále ukládala do souboru pwl, takže v této oblasti je bezpečnost hesel stále na nízké úrovni. Pomocí úprav v registrech bylo možné zakázat přihlášení uživatele do OS bez znalosti hesla k uživatelskému účtu. Ve většině případů, ale bylo možné kombinacemi různých kláves tuto restrikci obejít a přihlásit se do systému bez hesla. Další možností jak zabezpečit přihlášení, je vytvoření profilu uživatele, ve kterém se nastaví restrikce pro zadání hesla. Nová verze Internet

Exploreru ve verzi 4 přináší lepší kontrolu nad zabezpečením při surfování internetem. Přesto má další chyby a je postupně aktualizována na vyšší verze. Toto druhé vydání již bylo stabilním a uspokojujícím systémem, který se používá do současnosti.[4]

f) MS Windows Me

Posledním OS v této řadě podporující MS-DOS (ale jen částečně, protože neumožňuje restart do čistého MS-DOS) je Windows Me (Millenium). I tento systém dostal řadu vylepšení, a to nejen grafických ale i funkčních. OS má plnou podporu USB flashdisků, kdy není nutné dodatečně instalovat ovladač ke každému flashdisku, ale systém disk rozpozná a nainstaluje. Dále byl aktualizován multimediální přehrávač Windows Media Player 7 a zdokonalila se podpora multimédií obecně. Přes všechny pozitiva, které nový systém přinesl, bývá často označován jako nejméně stabilní, o čemž jsem se osobně přesvědčil. Právě stabilita OS způsobila, že Microsoft začal vyvíjet stabilní OS určený převážně pro firemní prostředí a servery. Již od r. 1987 Microsoft spolupracoval s IBM na stabilním OS, který měl být oproštěn od nedostatků DOSu. Bohužel vzájemná spolupráce mezi Microsoftem a IBM ztroskotala, a tak každá firma začala vyvíjet svůj operační systém. Bezpečnost tohoto OS je shodná s předešlou verzí Windows 98.[14]

g) MS Windows NT

V polovině roku 1993 se tak dostává na trh OS Windows NT (New Technology). Tento OS měl několik verzí, přičemž tou poslední byla verze 5. Windows NT byla opravdu stabilní a zdařile plnila funkci serverových operačních systémů. Na klientských stanicích a osobních počítačích se používaly Windows 98SE nebo Windows ME.[14]

h) MS Windows 2000

OS Windows NT 5.0 byl později přejmenován na Windows 2000. Tento OS se začal používat nejen jako serverová řešení ale i na klientských stanicích a osobních počítačích. Bezpečnost tohoto operačního systému vychází z OS Windows NT. To znamená, že hesla jsou šifrovány a jejich zcizení je tak daleko těžší než u Windows 98. Ke každému uživatelskému účtu můžeme nastavit bezpečnostní politiku, která určuje jaká práva bude mít daný uživatel a jaké bude moci provádět operace. Např. díky omezení práva instalovat, se do OS dostane daleko méně malware, než do OS bez

omezení. Dále je např. možné určit, který uživatel bude mít právo přístupu na internet nebo do lokální sítě. Každý uživatel má také svoji složku, která pokud je nastaveno heslo k účtu, není pro ostatní uživatele vidět. Právo vidět uživatelská data má pouze administrátor počítače. I tato vlastnost je krok dopředu proti staršímu OS Windows 98. Další vlastností je možnost volby souborového systému, a to buď FAT32 nebo NTFS. Přičemž NTFS nabízí větší zabezpečení a stabilitu. Díky NTFS je možné přiřadit každé složce na pevném disku práva pro dané uživatele a tím kontrolovat přístup k datům. Navíc data na pevném disku jsou šifrována. Tato bezpečnostní politika se stává klíčovým faktorem z hlediska bezpečnosti, a to také potvrdil test v praktické části. Co se týče ukládání hesel, potom tato jsou ukládána pro všechny uživatele do jednoho souboru SAM. Tento soubor je zašifrován a nelze ho přímo editovat. Bohužel i zde je možnost jak prolomit přihlášení do Windows, a to smazat soubor SAM a tím se po restartu systému nastaví nový soubor SAM se standardními uživatelskými účty a prázdnými hesly. Poté se stačí přihlásit jako Administrátor a zabezpečení je pryč. SAM soubor, ale nelze vymazat přímo v prostředí Windows, nýbrž spuštěním počítače např. z instalačního CD Windows 98 a nabootovat do prostředí MS-DOS. V tomto prostředí je pak možné soubor SAM smazat. Existuje samozřejmě řada dalších možností, např. Linuxové distribuce, pomocí kterých je možné SAM soubor editovat a smazat heslo administrátora nebo jiného uživatele. Pro jeho velmi dobrou stabilitu a funkčnost se používá dodnes a definitivní tečku za používáním Windows 2000 udělá firma Microsoft dnem ukončení oficiální omezené podpory tohoto operačního systému. Dle sdělení Microsoftu by omezená podpora Windows 2000 SP4 neměla skončit dříve než 1.1. 2010. Omezená podpora se týká vydávání bezpečnostních záplat OS, ale ne již nových funkcí nebo vylepšení OS.[4][3]

i) MS Windows XP

V roce 2001 byla uvedena na trh nová verze OS nazvaná MS Windows XP (Experince). Tento OS vychází z technologie NT a zároveň z Windows 9x. Dle vyjádření Microsoftu by měl obsahovat to nejlepší z obou systémů a zajistit tak případnou zpětnou kompatibilitu se staršími operačními systémy Windows 9x a zároveň dodržet stabilitu a bezpečnost známou ze systému Windows NT. Přibylo nové grafické prostředí, nový multimediální přehrávač Windows Media Player, podpora internetu a přehrávání multimédií a přepracované grafické prostředí. Podle cílové skupiny uživatelů byly vydány dvě verze tohoto operačního systému. Verze Windows XP Professional je

primárně určena pro firemní sektor a nasazení na klientských stanicích. Verze Windows XP Home je potom určena domácím uživatelům. OS Windows XP začal ihned po svém uvedení postupně nahrazovat starší verze OS Windows 98 a Windows 2000. Protože je však náročnější na hardware, bylo jeho nasazení ve většině případů vázáno na posílení hardwaru a nebo úplnou výměnu stávajícího počítače. Bezpečnostní prvky Windows XP jsou téměř shodné s Windows 2000, a proto je zde již nebudu uvádět. Zlom z hlediska bezpečnosti nastal až s uvedením opravného balíčku ServicePack 2 v roce 2004. Tento balíček s sebou přináší všechny dostupné bezpečnostní záplaty v té době, ale i nové bezpečnostní prvky, které jsou opět krokem dopředu k ochraně uživatele před útoky z internetu, viry a jinými hrozbami.

Inovace a zdokonalení byly orientovány na tři hlavní oblasti:

- **Vyšší stupeň zabezpečení** – ve výchozím nastavení je systém více zabezpečen a byl doplněn o nové bezpečnostní prvky, jako např. firewall. Dále byla v základním nastavení upravena bezpečnostní politika prohlížeče Internet Explorer, který umožňuje automaticky blokovat nežádoucí reklamní okna, či ActiveX prvky. Všechna vylepšení tak znamenají lepší ochranu před hackery, viry a ostatními bezpečnostními hrozbami. Pro firmy pak přináší posílení bezpečnostní infrastruktury.
- **Vylepšená správa zabezpečení** – díky service packu je snazší udržovat počítač stále aktualizovaný a nastavení všech bezpečnostních prvků, jako firewall, antivir či aktualizace systému je umístěno v novém Centru zabezpečení Windows(Windows Security Center). Centrum zabezpečení umožňuje jednodušší nastavení a zároveň upozorňuje uživatele v případě nefunkčnosti daného bezpečnostního prvku.
- **Větší komfort pro uživatele** – v opravném balíčku jsou obsaženy aktualizace klíčových ovladačů, byla zdokonalena podpora technologií jako Wi-Fi či Bluetooth, a to zejména v oblasti bezpečnosti

j) MS Windows 2003

I verze OS Windows 2000 Server se dočkala svého následovníka, a to Windows 2003, který přináší řadu bezpečnostních vylepšení a doplňků, mezi kterými mohu jmenovat např. integrovaný firewall, známý právě s Windows XP. V základním nastavení tohoto OS jsou daleko přísnější pravidla, která tak znesnadňují průnik

malware do OS. Např. v Internet Exploreru jsou nastaveny bezpečnostní prvky tak, aby bez vědomí uživatele nebyl instalován z internetu žádný software.

2.2 MS Windows Vista

Poslední ohlášenou verzí OS MS Windows je Windows Vista. Následovníkem serverové edice Windows 2003 bude Windows Server Longhorn. Vydání tohoto OS Windows Vista bylo v době psaní bakalářské práce dle sdělení Microsoftu vyhlášeno na konec listopadu roku 2006. Windows Vista jako důstojný nástupce s sebou opět přináší řadu grafických vylepšení a fines, které potřebují pro správnou funkci výkonnější počítač. To s sebou nese i další náklady na hardware. Kromě nového grafického prostředí, přináší i novou verzi Internet Exploreru, a to ve verzi 7 a další bezpečnostní prvky.[16]

Internet Explorer ve verzi 7, běží v odděleném režimu a měl by chránit před nebezpečím z internetu. Dalším prvkem zabezpečení, je omezení přidělování uživatelských práv v systému. Do OS byl integrován antispywarový nástroj Defender a za poplatek může být přidán Windows Live OneCare, který poskytuje lepší ochranu proti virům a internetovým červům. Windows Live OneCare rozšiřuje Windows o dodatečné funkce zabezpečení, a to firewall, antivir, nástroj pro defragmentaci a zálohování. Každá část tohoto bezpečnostního balíku se automaticky aktualizuje a tím zaručuje aktuální ochranu počítače.[18]

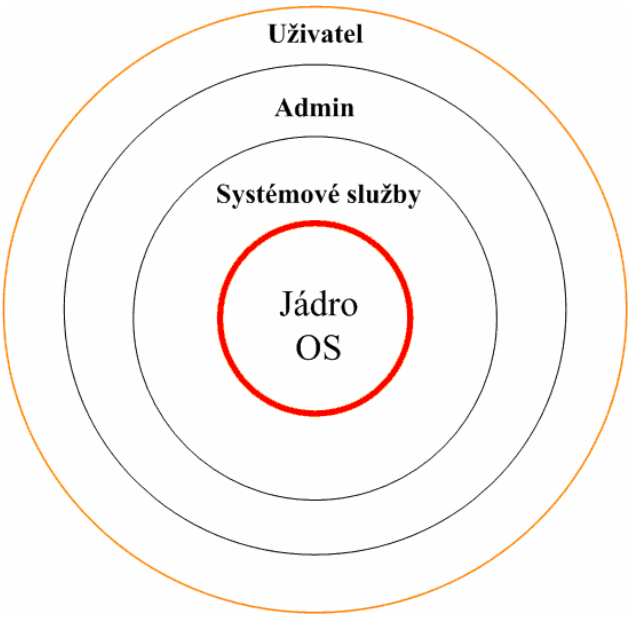
Ve snaze pokrýt celé spektrum uživatelů, přichází Microsoft až se sedmi verzemi, a to Windows Vista Starter, Home Basic, Premium, Professional, Small Business, Enterprise a Ultimate Edition.[15]

2.2.1 Bezpečnostní prvky ve Windows Vista [10]

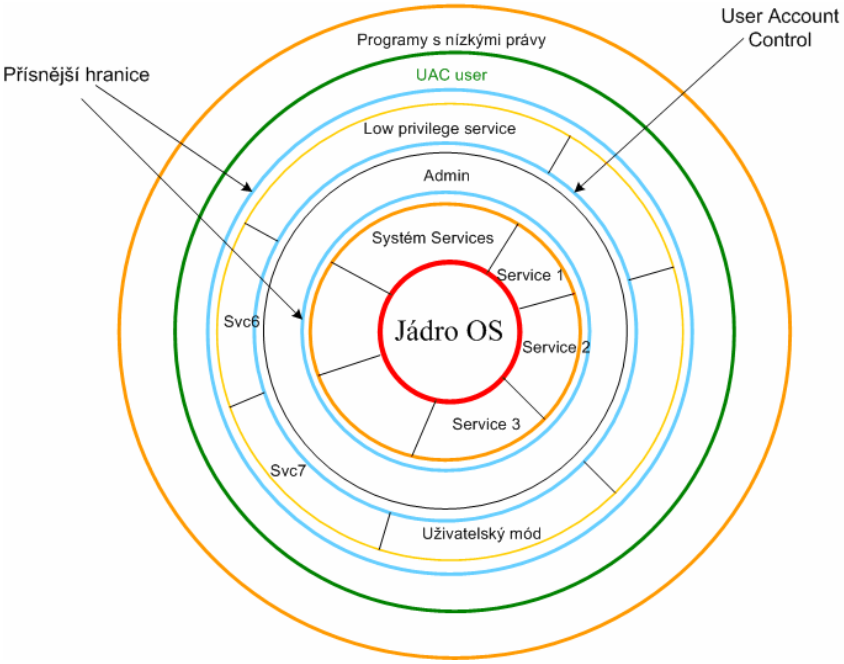
Hlavní změnou oproti Windows XP je, že Windows Vista mají jádro systému, na které se nabalují další moduly, zatímco OS Windows XP byl koncipován jako celek. Tato změna struktury umožnila nejen jednoduché přidávání či odebírání jednotlivých modulů a tím i vznik několika odlišných verzí Windows Vista, ale co je velmi důležité, umožnila používat jednotné bezpečnostní záplaty tzv. hotfixy. Tyto záplaty se budou vydávat pouze v anglickém jazyce, protože jazyk OS je také modul a systém si natahuje jazyk právě z jazykového modulu. Jazyk je psán tak, že místo konkrétního slova, je v systému pouze proměnná, která se za běhu systému nahradí příslušným slovem z jazykového modulu. Jedná se tedy o zásadní zlom, kdy do příchodu Windows Vista byl postup takový, že byly vydány nejdříve bezpečnostní záplaty v anglickém jazyce a

pak se čekalo na ostatní jazykové mutace, které se mohli použít pro konkrétní jazykové verze operačních systémů Windows. Nyní jsou hotfixy neutrální a dají se použít ve všech jazykových verzích Windows Vista po celém světě. Řešení uživatelských práv ve Windows XP je celkem jednoduché. Windows XP obsahuje jen malý počet vrstev, které se liší přidělenými právy. Windows Vista obsahuje těchto vrstev více a nejdůležitější je vznik nové vrstvy UAC mezi vrstvou administrátor a vrstvou user. Jádro systému může v rámci těchto vrstev dynamicky přidělovat a odebírat práva běžícím aplikacím. Aplikace standardně běží v tzv. Low Privilege Service (nízkoprivilegovaný mód), kde mají omezená práva a mohou pracovat pouze s dříve definovanými částmi systému. Tento stav odpovídá nastavení OS Windows XP a je důvodem, proč velké procento uživatelů používá ve Windows XP účet s právy administrátora. Rozdíl mezi vrstvami v OS Windows XP a OS Windows Vista viz. obrázek č.1 a obrázek č.2.

Obrázek 1 Zobrazení bezpečnostních vrstev v OS Windows XP



Obrázek č. 2 Zobrazení bezpečnostních vrstev v OS Windows Vista



2.2.2 User Account Control (UAC)

Windows Vista s sebou přináší samostatnou vrstva UAC, která umožňuje používat účty, která nemají stejná práva jako účet Administrátora. Technologie User Account Control obsahuje účty s právy administrátora, které ale nejsou na stejné úrovni, tzn., že účet Administrátora je jim nadřazen. Standardně běží aplikace v Low Privilege Service, a pokud chce zasáhnout do části systému, do které v rámci LPS módu nemá přístup, musí jí jako uživatel přidělit práva. Při použití běžného uživatelského účtu, informuje systém dialogem o tom, že uživatel nemá pro daný úkon dostatečná práva (např. instalace programu). Pokud je uživatel přihlášen jako administrátor nebo pod účtem s právy administrátora, systém se dotáže, zda může danou aplikaci přepnout do tzv. privilegovaného módu, ve kterém má aplikace přístup do celého systému. Takto zabezpečeny jsou nejen instalace, ale například i změna systémového času nebo utilita msconfig a další. Technologie UAC umožňuje potencionálně nebezpečným programům zapisovat v registrech pouze do větve HK Current User. Tato vlastnost je pro počítač méně nebezpečná, než v případě, kdy mohla daná aplikace zapisovat i do větve HK Local Machine, která obsahuje uložené zápisy a nastavení pro celý počítač.

2.2.3 Internet Explorer 7

Nová verze Internet Exploreru s sebou přináší kromě vylepšeného grafického prostředí, záložek a dalších doplňků, také nové bezpečnostní prvky. Díky nové architektuře může Internet Explorer také využít k zabezpečení technologie User Account Control. Jedním z nových bezpečnostních prvků je Protected Mode. Funkce Protected Mode neumožňuje aplikacím na webových stránkách zapisovat do některých částí operačního systému a tím chrání systém před infiltrací z venčí. Internet Explorer má v Protected Mode omezená práva a nezávisle na tom, zda běží v privilegovaném módu, či nikoli, může zapisovat pouze do definovaných bezpečných částí disku. Součástí Internet Exploreru je nově funkce Compatibility Redirector, která směruje maximum zápisů do složky Temporary Internet Files. V případě, že potřebuje uživatel ukládat obrázky, proběhne kontrola integrity aplikace a uživatel je za pomoci Broker Processu dotázán, zda chce danou akci povolit. Na základě těchto bezpečnostních prvků, nelze změnit nastavení Internet Exploreru tak, aby o tom nebyl uživatel informován.

2.2.4 Zabezpečení sítě

I tento bezpečnostní prvek doznal výrazných změn. Z Windows XP známý firewall byl obohacen o monitoring komunikace, a to v obou směrech. To znamená, že firewall, dokáže monitorovat jak příchozí, tak odchozí komunikaci. Dalším síťovým bezpečnostním prvkem, který byl implementován, je technologie IPSec pro šifrování dat.

2.2.5 NAP (Network Acces Protection)

Jedná se o soubor technologií pro ochranu sítě. NAP zabezpečuje počítač proti odposlechu komunikace nebo proti neautorizovanému připojení k síti. Toto zabezpečení je důležité zvláště v dnešní době, kdy jsou velmi často používány bezdrátová (WiFi) síťová připojení, která bývají velmi často a snadno atakována. NAP dokáže zabránit neoprávněnému průniku do sítě i v případě, že útočník zjistí přihlašovací hesla. Počítač se snaží připojit k vaší síti a pokud souhlasí přihlašovací údaje, je počítač uzavřen do tzv. VPN karantény. Dále se v rámci sítě mohou specifikovat podmínky na hardware připojovaných počítačů. Tato pravidla se mohou dále rozšířit o specifikaci OS, nainstalované hotfixy, antivirové programy nebo aplikace, které musí nebo naopak nesmí být nainstalovány. Pomocí těchto pravidel můžeme zamezit připojení cizích počítačů k síti.

2.2.6 Skupinová politika

Již z OS Windows NT jsou známé skupiny uživatelů, kterým lze přidělovat a odebírat jistá práva. Windows Vista ale v tomto směru přichází s novinkou, která bude velkým přínosem. Většina pracovníků ICT se potýká s problémem bezpečného používání paměťových médií. Např. zaměstnanci firmy, jejíž síť spravují, mohou neomezeně používat paměťová média jako jsou diskety, USB flashdisky, MP3 přehrávače, CD a DVD média apod. Nejen, že tato výměnná média jsou potenciálním nebezpečím pro celou síť z hlediska možného výskytu virové infekce, ale uživatel má možnost na tato média kopírovat data. Tím může dojít k nežádoucímu úniku citlivých dat a kromě finanční ztráty i poškození dobrého jména firmy. Ve Windows XP bez pomoci softwaru druhých stran není možné USB porty zabezpečit. Windows Vista v rámci skupinové politiky přichází s možností přímo definovat přístup k výměnným médiím. V případě připojení výměnného média je možné povolit nebo zakázat jeho instalaci. Restrikce ale pokračuje dále. Pokud je instalace výměnného média povolena, je možné dále přidělit nebo odebrat práva pro čtení, zápis nebo spouštění.

2.2.7 Ukládání hesel

Pokud uživatel nemá k dispozici EFS nebo Bit Locker, jsou jeho data v ohrožení. Získání hesla administrátora není obtížné a zkušení uživatelé ho mohou získat během několika minut. Existují utility, kterými je možné vytvořit bootovací disketu, nebo bootovací CD, kterou vložíte při startu do počítače. Na disketu se stáhnou všechna uživatelská jména a hesla. Následně stačí soubor s hesly uploadovat na internet a pomocí jednoho z dešifrovacích programů, lze získat všechna hesla

2.2.8 HW ochrana

Ochrana PC není důležitá jenom po dobu jeho provozu, ale i při jeho startu nebo při vypnutém stavu. Pro tento účel ochrany vyvinula firma Microsoft několik technologií.

Technologie Bit Locker (známá také jako Secure Startup and Volume Encryption) se stará o to, aby byla data odolná proti odcizení a dále zabezpečuje digitální podepisování knihoven při startu systému. Při čtení chráněných dat je pak tento podpis ověřován, a proto je nemožné po nabootování jiného systému data přečíst. Tato softwarová část hardwarové ochrany musí být podporována BIOSem.

Další možností využití technologie Bit Locker je použití s čipem TPM (Trusted Platform Module), kterým budou osazovány základní desky. S pomocí tohoto čipu

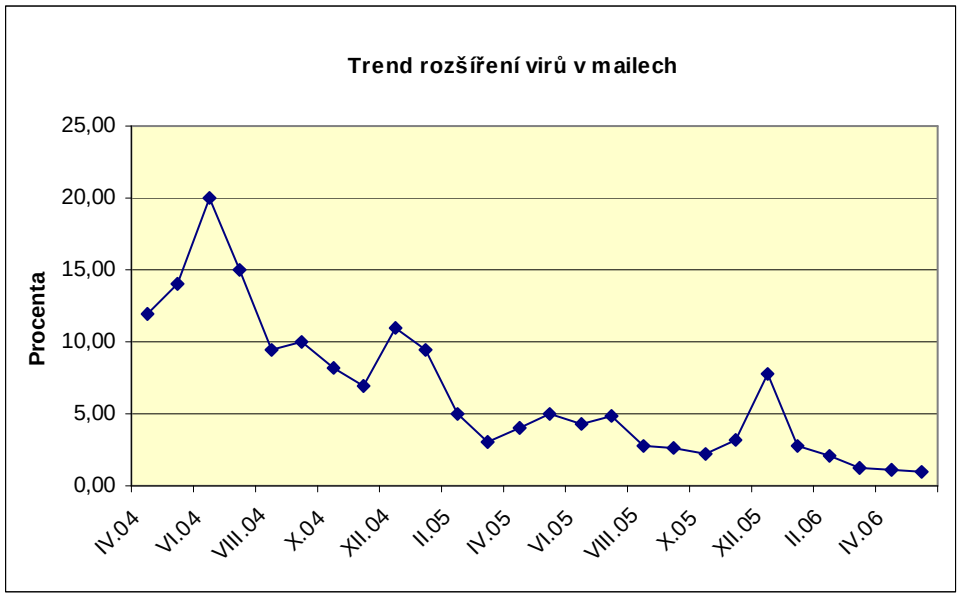
mohou být data na pevných discích šifrována (tzv. Volume Encryption - sektorové šifrování, které probíhá již při startu systému). Data budou šifrována od okamžiku spouštění systému a nebude možné spustit takto chráněný systém bez daného TPM čipu. Data lze v rámci Bit Lockeru zabezpečit na několika úrovních:

- TPM
- symetrický či asymetrický klíč na USB flash
- TPM + PIN kód
- TPM + symetrický či asymetrický klíč na USB flash
- TPM + symetrický či asymetrický klíč na USB flash + pin kód

3 Malware a jiná počítačová rizika

Pryč jsou doby, kdy mohl být počítač infiltrován pouze z přenosného média, čili diskety. S rostoucím vývojem výpočetní techniky roste i vývoj telekomunikačních technologií a bohužel s tím související vývoj nebezpečných aplikací jako virů, adware, spyware a dalších. Co si můžeme představit pod pojmem infiltrace? Jedná se o neoprávnění průnik do systému počítače za účelem např. krádeže soukromých dat. Tyto škodlivé programy můžeme označit souhrnným názvem MALWARE (malicious software) nebo-li škodlivý software. Bezpečnostních rizik, se kterými můžeme setkat, je mnoho. Příkladem mohou být viry šířící se formou přílohy v emailu viz. obrázek č.3. V následujících kapitolách se pokusím přiblížit alespoň ty nejdůležitější a nejčastější.[8][5]

Graf č.1 Rozšíření virů v emailech



3.1 Viry a jejich původ

Mezi nejznámější škodlivý software patří viry. První zmínky o viru, tedy počítačovém viru pochází z roku 1983. V té době Dr. Frederik Cohen prováděl první pokusy s kódem, který se sám replikoval. Naštěstí nebyly v té době dostupné potřebné technologie, které by umožnily šíření podobných virů. Vůbec prvním aktivním virem pro osobní počítače byl virus Brain, který vznikl cíleně pro počítač IBM PC kompatibilní. Jeho vznik se datuje k r. 1986. Naprogramovali ho dva bratři Amjan a Basid z Pákistánu. Virus Brain sice vznikl v r. 1986 ale jeho největší dopad se projevil

až o rok později. Napadal boot sektory disket typu $5^{1/4"}$ o kapacitě 360 KB a způsobil neschopnost počítače rozpoznat vloženou disketu.[5]

Stručný přehled z historie virů:

1987	**Pakistani Brain** – první virus, který se začal celosvětově šířit
	Christmas Tree – virus, který způsobil první epidemii, po spuštění zobrazil na monitoru obrázek vánočního stromečku
1988	**Stoned** – první virus, který útočí na master boot record pevného disku
	Jerusalem – virus, který jako první zůstává v paměti a můžeme jej označit jako rezidentní
	Cascade – první virus, který byl zašifrován
1989	**Dark Avenger** – je schopen infikovat otevírané soubory i přes antivirovou ochranu
1990	**Flip** – jeden z prvních polymorfních virů
1991	**Michelangelo** – virus, který se usídlil v paměti počítače a čekal na 6. března, kdy přepsal soubory na disku náhodnými znaky
1992	**Michelangelo** – virus stále vzbuzuje zájem médií
1993	**Tremor** – virus, který byl schopen vypnout antivirovou ochranu
1994	**OneHalf** – velmi populární virus té doby, původem z východního Slovenska, který měl za cíl znehodnotit pevný disk
	GoodTimes – již v té době první poplašná zpráva o neexistujícím viru
1995	**Concept** – první existující makrovirus pro Microsoft Word
1996	**Boza** – první virus napadající Windows 95
	Tentacle – první virus, který byl schopen se šířit pod Windwos 3.x
	Laroux – první existující makrovirus pro Microsoft Excel
1997	**Esperanto** – virus určený jak pro MS Windows tak pro Mac OS
1998	**BackOrifice** – jeden z prvních útoků na webové prohlížeče
1999	**Melissa** – opět makrovirus napadající MS Word a šířící se pomocí MS Outlook
	BubbleBoy – první virus určený pro MS Outlook. K aktivace viru stačilo pouze otevřít email
	Chernobyl – virus, který byl zaměřen na poškození BIOSu počítače
2000	**Istaller** – první virus pro OS MS Windows 2000
	LoveLetter – virus, jinak také přezdívaný **I love You**, se šířil pomocí

elektronické pošty formou podvrženého milostného dopisu a měl za cíl, zahltit poštovní servery. Způsobil tak miliardové škody

2001 **Anna Kournikova** – virus, který vznikl pomocí virového generátoru na základě stanoveného zadání. Infikovaný email nabízel fotografie světoznámé ruské tenistky. Po otevření zprávy došlo k jeho aktivaci, přičemž se automaticky rozeslal na adresy obsažené v počítači.

Magister - virus, který se opět šíří skrze elektronickou poštu a nebo přes sdílené disky v počítačové síti

Sircam – virus, který byl následovníkem viru Magister

Code Red I a II – příklad internetových virů, které prováděli masivní útoky

Nimda – virus, který se šířil formou emailu, přes síťová připojení, webové servery, službu IIS, lokální a síťové disky

2002 **Benjamin** – první virus využívající ke své šíření výměnné sítě typu Kazaa

2003 **SoBig** – virus, který měl v sobě obsažen vlastní SMTP server pro odesílání emailů varianta **SoBig.F** dokázala k 25.8.2003 nakazit cca. 1 400 000 počítačů

Klez.H – je schopen rozeslat náhodné dokumenty z infikovaného počítače

Slammer – proslavil se tím, že dokázal infikovat počítače na celém světě během několika minut

2003 **Blaster** – také označován jako **LovSan** nebo **MSBlast**. Napadal pouze OS MS Windows a využíval bezpečnostní chyby v OS Windows NT, 2000, XP, 2003.

2004 **MyDoom** – virus přezdívaný také jako **Novarg** nebo **Shimgapi** otevíral infikovaný počítač pro přístup z venka. Spuštěním přílohy infikovaného emailu se spustí programy zahlcující počítačové sítě. Virus byl naprogramován k útokům na servery Sun, Microsoft.

2005 **Zotob** – virus, který se zaměřuje především na OS MS Windows

Sober.O – virus, který je součástí zazipované přílohy a po aktivace se sám šíří na další adresy v počítači

Bagle – virus šířící se pomocí spustitelných příloh v emailech

Mytob – virus, který zabraňuje spuštění utilit jako msconfig, regedit, cmd, taskmgr a¨dále bojuje proti pokusům o odvirování systému

2006 **Stration** – nový typ viru, který se šíří jak pomocí elektronické pošty, tak přes instant messangery jako např. ICQ. Vir jakmile je aktivován, se snaží deaktivovat rezidentní
antivirovou ochranu a rozesílat sám sebe na další adresy. Dále zobrazuje informativní hlášení o restartu počítače v intervalu jedné minuty.
Win32/Warezov – mutace viru Station, který se šíří elektronickou poštou a spolu s textem je odesílána i infikovaný příloha, která se tváří jako bezpečnostní záplata pro OS.[11] [17][5]

V dnešní době si můžeme pod pojmem počítačový virus představit programový kód a nebo jeho část, která může aktivně fungovat v počítači aniž by o tom majitel počítače věděl. Virus může provádět různé nebezpečné činnosti, sám sebe replikovat a zároveň v případě připojení do internetu odesílat na získané emailové adresy z napadeného počítače. Rychlost, kterou se viry šíří se odhaduje na statisíce infikovaných počítačů denně.[5]

3.2 Rozdělení virů

3.2.1 Bootviry

Jedná se o nejstarší skupinu virů, která je zaměřena na určitou část oblasti systémového disku. Mezi tyto oblasti patří boot sektor diskety a nebo MBR (Master Boot Record) pevného disku. Virus se typicky přenášel pomocí disket a projevuje se tím, že přepíše boot sektor svým vlastním kódem a původní část boot sektoru zapíše na jiné místo disku, např. nevyužité systémové clustery, využité systémové clustery nebo systémové oblasti. K infikování tedy stačilo, aby disketa přišla do styku se zavirovaným počítačem. Bootviry byl koncipovány pro OS MS-DOS, a to pro jeho jednoduchost, nevelké možnosti kontroly v tomto prostředí a také v častém používání jednoduchých příkazů jako je zápis, čtení, kopírování. Virus se po infikování operačního systému nainstaluje do paměti a zapíše své tělo do MBR pevného disku. Dále setrvává v operační paměti jako rezidentní a při dalším zavedení operačního systému infikuje boot sektor disket, kterou nejsou ochráněny proti zápisu např. při kopírování na disketu. Původní boot sektor je uložen na jiné místo diskety nebo pevného disku. Pokud virus zapíše původní boot sektor do oblasti obsahující např. tabulku FAT a nebo hlavní diskový adresář, může dojít ke nenávratné ztrátě dat. Infekce bootvirem se dá rozpoznat např. při výpisu programu CHKDSK, kdy se zobrazí kapacita systémové paměti

nejméně o 1024 bytů menší než je ve skutečnosti instalovaná (instalovaná 512 KB, ale zobrazí se 511 KB). Jednoduchou obranou proti bootvirům je zákaz startování operačního systému z diskety a povolení startu z pevného disku nebo z nepřepisovatelného CD-ROMu.[8]

Virus lze odstranit spuštěním počítače např. z čisté diskety a následně spuštěním příkazu FDISK s parametrem /mbr. Pokud se virus nenachází ještě v dalších částech počítače, stačí dále spustit antivirový program, který již dokáže bootvir detekovat a také odstranit.[5]

3.2.2 Souborové viry

Druhou skupinu tvoří viry souborové. Jak už vyplývá z názvu, tento typ viru se soustředí na jednotlivé soubory, které infikuje. Proto aby se mohl dále šířit, potřebuje infikovat právě spustitelné soubory jako exe, com, bat a další. Souborové viry se podle typu a funce dělí na další skupiny.[8]

3.2.3 Přepisující viry

Při infekci dojde k přepsání části původního kódu programu tělem viru. Část původního programu je zničena a spuštěním infikovaného souboru dojde k aktivaci viru, který se snaží o další replikaci. Tento typ nepatří mezi rezidentní, tudíž nezůstává v paměti aktivní.[8]

3.2.4 Makroviry

Tyto viry využívají tzv. makrojazyka, který je vložen do souborů pro zpracování dat např. tabulkové procesory, textové editory, grafické editory a další. Typickým příkladem může být soubor typu MS Word nebo MS Excel. Výše jmenované programy umožňují přidávat specifická makra k souborům nebo kopírovat makra do jiných souborů.Jako programové prostředky slouží interpretační jazyky, a to Word Basic a Visual Basic. Viry získávají řízení počítače především při spuštění a zavření infikovaného souboru a následně napadají další otevřené soubory. Jejich chování odpovídá rezidentním virům na úrovní MS DOSu. Makroviry tedy mohou být aktivní i bez otevření příslušného dokumentu a k jejich aktivace stačí otevřít např. pouze aplikaci MS WORD. Tato aplikace umožňuje používat automatická makra jako např. AutoOpen, AutoClose, AutoExec,AutoExit, AutoNew, která umožňují automatické spouštění a šíření makrovirů. Dále mohou makroviry přenést svůj kód do globálních maker aplikace MS WORD. Jelikož se při ukončení práce ukládají globální makra do šablony

NORMAL.DOT, může dojít právě k tomu, že se virus aktivuje ještě dříve než se otevře nějaký dokument a k jeho aktivace stačí pouhé spuštění např. aplikace MS WORD. Jednoduchou obranou proti makrovirům může být zakázání automatického spuštění Maker. MS WORD a MS EXCEL má navíc v sobě implementováno automatické varování, které se zobrazí vždy jakmile se uživatel pokouší spustit soubor obsahující makro. Bohužel jednou z možností aplikace MS Word je schopnost šifrovat makra. Infikovaná makra pak mohou být v zašifrovaném tvaru a tím se stává jejich odhalení obtížnějším. Výsledkem napadení systému makrovirem je např. to, že není možné konvertovat dokument do jiného fomátu nebo není možné uložit dokument do jiného adresáře. Infikované soubory se tváří zpravidla jako šablony a v případě infekce konvertuje MS WORD dokumenty na šablony a naopak.[5]

3.2.5 Polymorfní viry

Tyto viry se vyznačují především nejen svojí schopností se maskovat a stát se tak neviditelnými, ale zvláště svou schopností měnit sama sebe.V dřívější době prováděli antivirové programy skenování systému pomocí porovnání kódu souboru s předem definovanou maskou odpovídající kódu viru. Pokud byl výsledek porovnání pozitivní, byl ohlášen nález viru. To znamenalo pro tvůrce virů jediné. Pozměnit kód viru tak, aby se stal neviditelným a přidat další vlastnost, pomocí které se vir stane polymorfním. To znamená, že se virus postupně sám modifikuje, mění velikost souboru, strukturu a svůj kód. Díky těmto vlastnostem jsou polymorfní viry pro antivirové programy hůře odhalitelné. K to mu, aby byly viry neviditelné používají soubor prostředků, které umožňují skrýt virus v systému. Mezi nejjednodušší techniky skrývání patří falšování velikosti souboru. Při výpisu adresáře je u souboru zobrazena původní velikost. Tato technika se nazývá semi-stealth. Příkladem může být virus Brain z r. 1986. Vyspělejší viry využívající techniky neviditelnosti, dokáží zamaskovat tělo viru i při prohlížení souboru. Při otevření souboru dojde k jeho automatickému odvirování a při zavření souboru dojde opět k zavirování. Další možností je poskytnutí kopie původního souboru, který si virus odložil na jiné místo. K odhalení tohoto typu viru se používá heuristická detekce.[5]

3.2.6 Rezidentní viry

Hlavním cílem tohoto viru je umístit se v rezidentně v paměti počítače. Virus nejprve vyhledá dostatečně velké a bezpečné místo a pak se na něj umístí.

3.2.7 Parazitické viry

Jako parazitické viry jsou označovány ty, které se regulérně připojí k proveditelnému hostiteli (souboru) bez toho, aby ho nějak trvale poškodily. Nejčastěji se virus umisťuje za původní soubor. Při infekci je původní soubor upraven tak, aby po jeho následné aktivaci došlo jak k aktivaci viru, tak i původního programu.[8]

3.3 Metody vyhledávání virů

Proto, aby mohl antivirový program bezpečně odhalit potencionální virovou hrozbu, musí použít několik typů detekce k identifikaci viru.
Mezi nejpoužívanější metody patří:

3.3.1 Detekce známých virů

Tato metoda využívá sekvence, která je obsažena ve virové databázi. Díky této sekvence může antivirový program provést důkladnou analýzu a jednoznačně identifikovat případnou virovou nákazu.

3.3.2 Generická detekce

Tato metoda se používá pro identifikaci nových variant již známých virů a jejich mutací. Jestliže antivirový program nenajde shodu v databázi známých virů, začne hledat sekvence podobné těm, které jsou obsaženy u již právě známých virů.

3.3.3 Heuristická analýza

Pomocí této analýzy je možné odhalit virus ještě před tím, než je zařazen do virové databáze. Pro detekci se používají dvě metody, a to statická a dynamická.

3.3.4 Statická heuristická analýza

Tato analýza se soustředí na vyhledávání podezřelých datových konstrukcí.

3.3.5 Dynamická heuristická analýza

Tato analýza testuje v chráněném prostředí virtuálního počítače uvnitř antivirového programu určité chování emulovaného kódu, které by mohlo odpovídat chování pravého viru. Pro příklad mohu uvést program, který vyhledá spustitelné soubory a následně provede u těchto souborů částečné změny.[9]

3.4 Spyware, adware a jiný škodlivý software

V běžném životě, a to jak pracovním tak soukromém, se nejvíce setkáváme právě s těmito druhy škodlivého softwaru. Co se týče falešných zpráv, nemůžeme

mluvit o infiltraci počítačového systému, ale i přesto toto téma s danou problematikou souvisí.

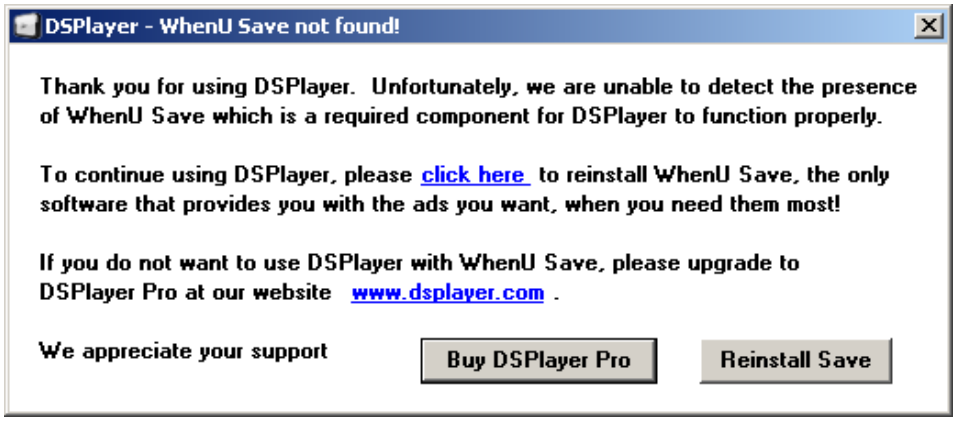
3.4.1 Spyware

Tento program ma za cíl jediné, a to odeslat data z infikovaného počítače pomocí sítě internet, bez vědomí uživatele. V porovnání s činností backdooru, bývají zcizena pouze statická data, která mají ve většině případů informativní charakter např. seznam navštívených stránek nebo nainstalovaných programů. Tyto informace bývají dále využívány pro marketingové účely a cílenou reklamu. Zda tyto informace nebudou zneužity, ale bohužel nikdo neručí, a proto z opodstatněných důvodů není přítomnost spywaru žádnému uživateli milá. Každopádně spyware se šíří především jako součást zkušebních verzí programu tzv. shareware. V praxi to znamená, že autoři o přítomnosti spywaru ví. Bohužel ani v případě odstranění spywaru z počítače pomocí speciálních programů nemá uživatel vyhráno. Program po odstranění spywaru přestane fungovat a tím autor donutí uživatele k reinstalaci programu a tím se opět dostane spyware do počítače. K dalším problémům, které s sebou spyware nese, patří postupné zpomalování připojení k internetu až zpomalení vlastního počítače, který byl spywarem infikován. A právě díky tomuto jevu většina uživatelů zjistí přítomnost těchto programů.[8]

3.4.2 Adware

Adware pracuje trochu jinak než dříve zmíněný spyware, i když motivem k jeho existenci je opět cílená reklama a marketing. Samotný program nesbírá potřebné informace, ale naopak neustále v různých intervalech zobrazuje reklamu. Výsledkem jsou neustále vyskakující reklamní okna během surfování po internetu a přesměrování výchozí stránky na jinou, o kterou nemá uživatel zájem. Adware se šíří opět ve většině případů jako součást sharewarových verzí programů. Uživatel je však při instalaci upozorněn na přítomnost tohoto adwaru a pokud nebude souhlasit, instalace nebude úspěšná. V případě odstranění adwaru z počítače se stane zkušební program nefunkční a pokud uživatel trvá na vyzkoušení, musí provést reinstalaci a adware se opět dostane do počítače. Adware bývá často součástí multimediálních přehrávačů, kodeků DivX a dalších. Ukázkovým příkladem z praxe může být např. program DSPlayer, který slouží pro přehrávání audia a videa. Po odstranění adwaru WhenUSave není program funkční a objeví se varovné hlášení viz. obrázek č.3. Přesto tyto zkušební nebo zdarma použitelné verze programů bývají hodně instalovány, a to proto, že mají v sobě více funkcí než verze sharewarové nebo freewarové.[8]

Obrázek č. 3 Příklad adwaru



3.4.3 Dialer

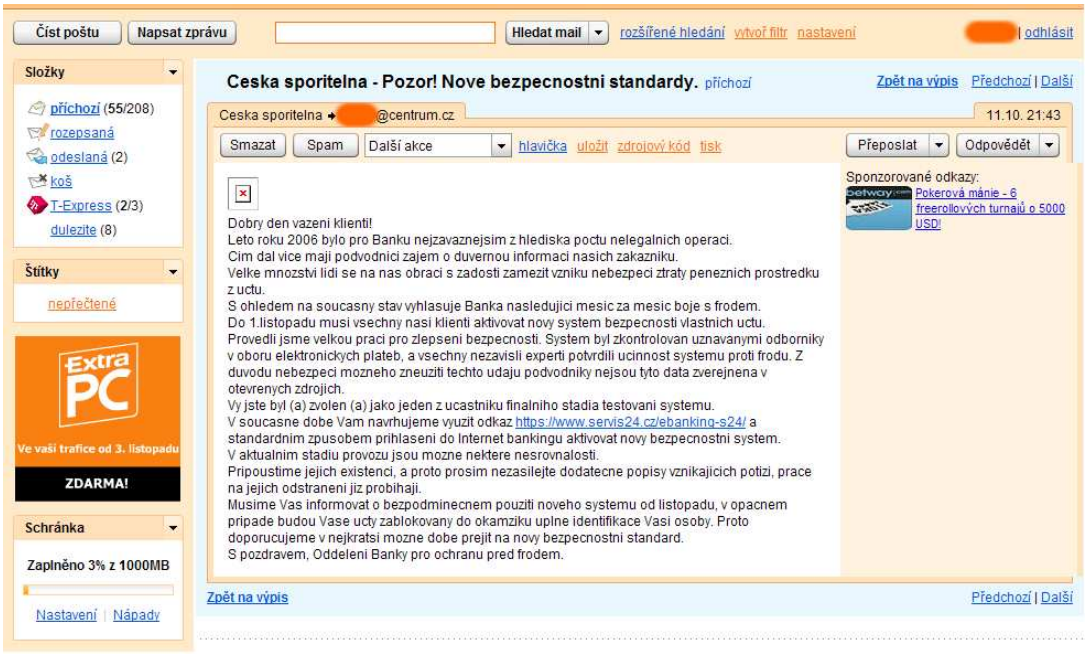
Tento program se od již zmíněného spywaru a adwaru ve své funkčnosti liší. Dealer je program, který cíleně mění konfiguraci připojení k internetu a nebo vytváří zcela nové připojení, které nastaví jako výchozí. Dialer je hlavně zaměřen na vytáčené připojení pomocí analogového modemu, kdy pozmění původní a správné telefonní číslo na číslo se zvláštní tarifikací, např. 60 Kč za minutu (tzv. „žluté linky“). Ve většině případech vše probíhá automaticky a nenápadně a mnoho uživatelů zjistilo podvodné přesměrování až při obdržení faktury za telefon. Dialer se může dostat na počítač např. návštěvou erotických stránek s tématikou pornografie nebo stránek s nelegálním obsahem např. cracky. Ve velké míře je zneužívána technologie Active-X, kdy jsou nejvíce ohroženi uživatelé používající Internet Explorer. Další možností může být spuštění souboru s příponou „.exe“, který je uživateli vnucen při otevření webové stránky. Na možnost či nutnost instalace Dialeru většina stránek, které tento program používají, upozorňuje. A zde je kámen úrazu. Upozornění na Dialer totiž bývá psáno velmi malým písmem a většinou na spodním okraji stránky a nebo na jiném místě, kde může ujít i pozornému uživateli. Dialer tedy může být provozován legálně (uživatel je na jeho instalaci upozorněn a srozuměn s cenou za připojení) i ilegálně (instalace probíhá automaticky a tiše bez vědomí uživatele). Legální Dialer zobrazí uživateli licenční ujednání („EULA“ -End User License Agreement) a až po jeho odsouhlasení dojde k přesměrování připojení. V praxi se však ukázalo, že licenční ujednání čte minimum uživatelů, a tím i tento případ můžeme teoreticky považovat za ilegální. Díky rozdělení na legální a ilegální instalaci může dojít k problému s antivirovým softwarem, který nedokáže rozlišit zda uživatel s instalací Dialeru souhlasil a nebo zda se nainstaloval sám. Antivir identifikuje jakýkoli Dialer jako škodlivý software a nabízí jeho odstranění. Naštěstí doba pokročila a s velkým rozvojem vysokorychlostního

internetu pomocí DSL, kabelové televize či WiFi sítí, začíná Dialerů ubývat a dá se předpokládat, že zcela vymizí.[26]

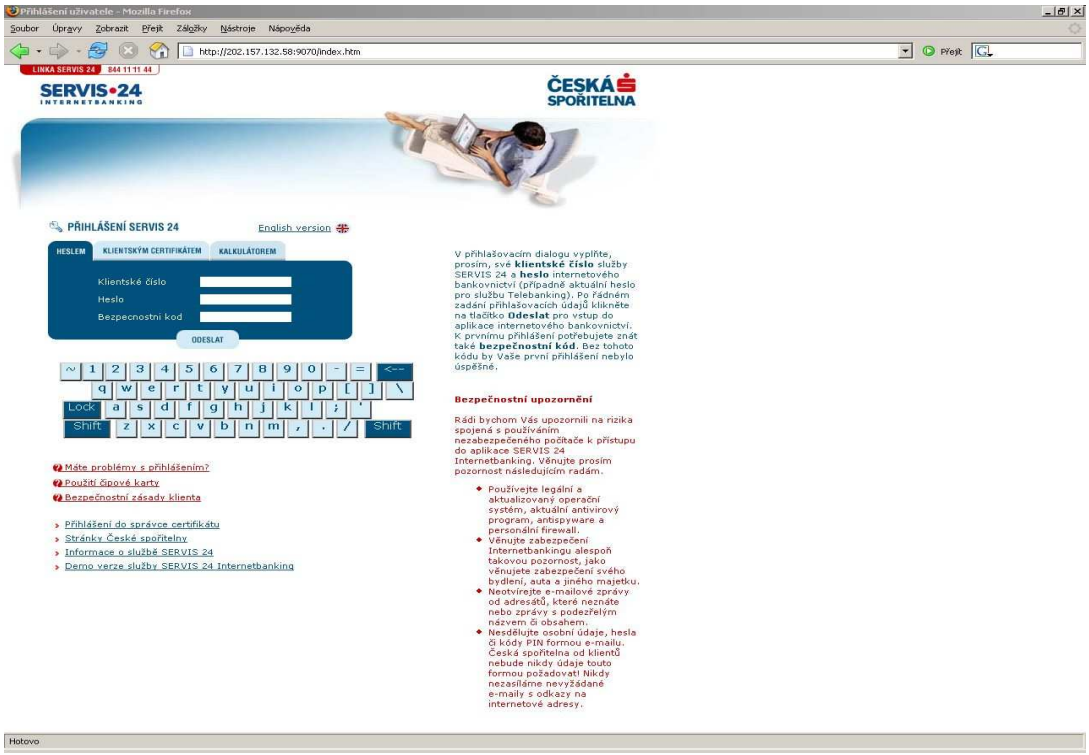
3.4.4 Phishing

Toto slovo v současnosti velmi často medializováno a spojováno především z oblastí bankovního sektoru. Jedná se o podvodné e-maily, kdy jsou na velké množství adres rozeslány podvodné informativní dopisy, které jsou na první pohled velmi důvěryhodné a obsahují důležité sdělení převážně bankovního charakteru. Tyto podvodné emaily využívají tzv. sociální inženýrství. Adresát bývá např. v dopise vyzván k vyplnění elektronického formuláře a pokud tak neučiní, je mu pohroženo zablokováním účtu a nebo jinou sankcí. Součástí emailu je odkaz na tento elektronický formulář a skutečná cílová adresa je skryta tak, aby uživatel neměl nejmenší tušení, že nevyplňuje formulář na stránkách své banky ale na úplně jiném serveru. Podvodné stránky jsou vytvořeny a upraveny tak, aby se uživatel domníval, že je opravdu na stránkách své banky. Tím dochází k tomu, že podvedený uživatel vyplní na těchto stránkách např. číslo účtu, přihlašovací jméno a heslo nebo PIN pro autorizaci transakce. Získané informace je pak velice snadné využít např. pro neoprávněný převod peněz z účtu. Jako příklad z praxe mohu uvést podvodný email viz. obrázek č.4, který jsem obdržel do mé soukromé schránky. Týkal se České Spořitelny a varoval před nasazením nové technologie. Dále obsahoval odkaz na údajnou přihlašovací stránku viz. obrázek č.5, pro ověření přihlašovacího dialogu. Stránka byla samozřejmě podvodná a v mém případě směrovala na IP adresu vedenou v Číně. Stránka s přihlašovacím dialogem jakoby z oka vypadla originální stránce České spořitelny, a.s. Jeden rozdíl, však může každý uživatel již pouhým okem rozeznat při srovnání s originálem. A to políčko pro bezpečnostní kód, kterým se potvrzuje transakce. Toto pole se na originálních stránkách neuvádí.[25]

Obrázek č.4 Vzor podvodného emailu



Obrázek č. 5 Vzor podvodné stránky



3.4.5 Pharming

Tento metoda vychází z phishingu a je novější a nebezpečnější hrozbou. Pharming využívá překladu jména serveru na odpovídající IP adresu a útočí na DNS servery. Změnou záznamů na DNS serverech docílí útočník toho, že je uživateli na dotaz o překlad jmenné adresy odeslána odpověď s podvrženou IP adresou. V případě

zadání adresy internetové banky, obdrží uživatel od DNS serveru modifikovanou odpověď a zobrazí se mu stránky, které jsou identické se stránkami originálními. Nic netušící uživatel poté zadá přihlašovací informace, které se odešlou útočníkovi. Další možností, kterou Pharming využívá, je tzv. technologie *DNS cache poisoning* , která dokáže změnit dočasně uložené záznamy DNS na PC. Aby nemusel počítač neustále odesílat serveru DNS požadavky pro překlad jmenných adres na adresy číselné (IP adresy), ukládá si tyto adresy do dočasné paměti. Často navštívené adresy se ukládají do souboru hosts, který je uložen na pevném disku počítače. Útočník se snaží napadnout počítač nebo skupinu počítačů pomocí virů nebo jiných modifikovaných souborů, které jsou nabízeny prostřednictvím internetu. Tyto škodlivé programy poté modifikují soubor hosts a zároveň posílájí informaci útočníkovi. Útočník vytvoří podvrženou stránku a formou phishingu nutí uživatele ke vstupu na danou stránku a zadání citlivých informací jako hesla, přihlašovací účty a podob. Uživatel nemá ve většině případů žádné tušení, že se jedná o podvod. Tento postup je nepodobný *DNS spoofingu*, tedy zfalšování odpovědí DNS serveru.

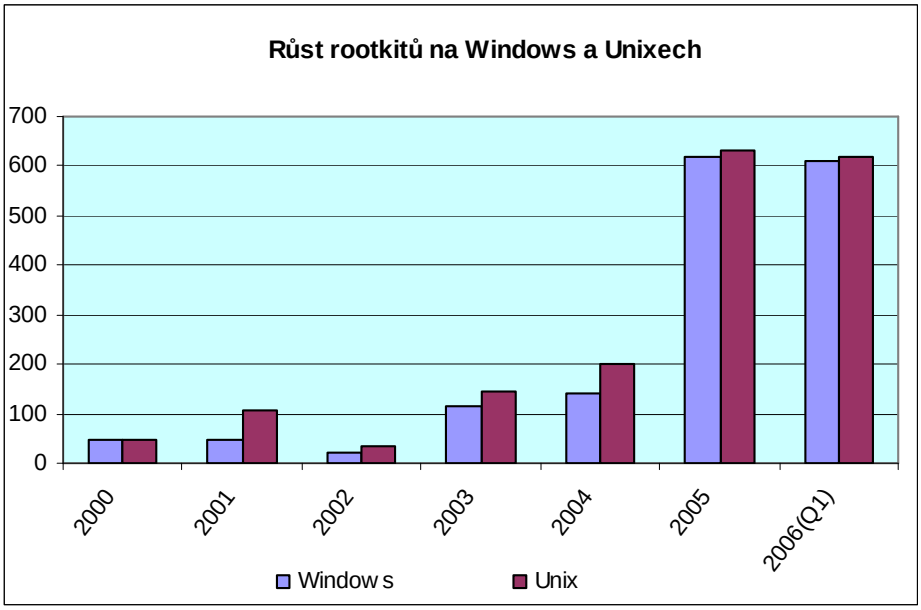
Obranou proti Pharmingu může být kvalitní antivirový program, který bude pravidelně aktualizován. Velkou měrou také pomáhá správně nakonfigurovaný firewall. Existují i aplikace např. Netcraft Toolbar, které dokáží u každé stránky zobrazit doplňující informace jako stát, ke kterému náleží příslušná IP adresa nebo hodnocení jiných uživatelů.[23]

3.5 Rootkity

Na tuto hrozbu byl ve větší míře brán zřetel až poté, kdy na rootkity upozornila firma SONY se svou ochranou proti kopírování. Rootkity se ale vyskytují v IT již dříve než byly díky firmě SONY medializovány. Původně sloužily hackerům pro utajení průniku do systému. Do počítače se infiltrují prostřednictvím kódu, který využívá zranitelnosti OS nebo jiné aplikace. Rootkit se aktivuje nainstalováním modifikovaných nástrojů a knihoven a jejich spuštěním. Tento typ velmi často slouží k zakrytí přítomnosti trojských koňů. Bývá také označován jako „*user-mode rootkit*“. Tyto rootkity pracují v uživatelském režimu a neumí skrýt svou přitomnost před bezpečnostními nástroji běžícími v režimu jádra OS. Složitější rootkity dokáží běžet přímo v režimu jádra OS a jsou mnohem nebezpečnější. Je velmi těžké je odhalit, protože mění chování systému. Mohou např. skrýt přítomnost malware před bezpečnostním softwarem. Dále dokáže rootkit skrýt systémové procesy , soubory, klíče

v registrech nebo některé hodnoty v klíčích registru. Tento kód je velmi obtížné odhalit. Rootkit nazvaný *Rstock.A* se šíří v reálném prostředí a využívá kombinaci ověřených a nových technik, které znemožňují odhalení rootkitu a jím skrytého malware pomocí specializovaných nástrojů. Časový přehled růstu četnosti rootkitů na platformě OS Windows a Unix viz. graf č.2.[24]

Graf č.2 Přehled výskytu rootkitů na OS Windows a UNIX



3.6 Hoax

Slovo HOAX označuje poplašnou zprávu, která obvykle varuje před neexistujícím virem či jinou bezpečnostní hrozbou. Šíření je zcela závislé na uživatelích, kteří takovou zprávu e-mailem obdrží. Obsah emailů přímo nabádá, aby jej uživatelé poslali svým přátelům a spolupracovníkům a tím se stávají šiřiteli těchto poplašných zpráv. Poplašné zprávy týkající se virů, mají níže uvedené charakteristické znaky:

- **Stručný popis bezpečnostní hrozby –** v úvodu bývá stručně popsáno bezpečnostní riziko, které v případě virové infekce OS hrozí, včetně způsobu, jakým se vir dále šíří.
- **Bezpečnostní dopad virové infekce –** v tomto bodě bývá většinou uvedené smyšlené riziko dopadu virové nákazy, včetně vyjmenování některých příkladů jako formátování pevného disku nebo vymazání dokumentů. Někdy bývají vyjmenovány i méně důvěryhodné až nesmyslné příklady jako roztočení HDD opačným směrem, výbuch počítače, poškození monitoru a další.

- **Potvrzení důvěryhodnosti -** ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů např. od firmy Microsoft, IBM a jiných.
- **Výzva k dalšímu rozeslání -** HOAX vždy obsahuje pobídku k zaslání na další emailové adresy. Mnoho nezkušených uživatelů se nechá zprávou zmýlit a výzvu uposlechnou. Díky tomu se HOAX velmi rychle šíří. Do kategorie HOAX se řadí i zprávy, které původně nejsou poplašné a nesouvisí s viry. Typickým příkladem jsou zprávy, kde rodiče prosí o vzácnou skupinu krve pro svého umírajícího syna, jenž leží v konkrétní nemocnici. Vzhledem k tomu, že ale není uveden žádný časový údaj (popř. ho někdo „cestou“ smazal), tato zpráva může kolovat po internetu i několik let.[27]

3.7 Spam

Spam nebo-li nevyžádaná pošta, není sám o sobě tak velkou bezpečnostní hrozbou jako malware, uvedený v předchozích kapitolách. I když i tato forma má svá úskalí. Např. odkazy uvedené v těle emailu často směrují na stránky, které mohou být původcem škodlivého software, např. trojských koní nebo spyware. Nevyžádaná pošta většinou reklamního charakteru plní emailové schránky uživatelů a zahlcuje poštovní servery. Z osobní zkušenosti mohu potvrdit, že více jak 60% veškeré elektronické pošty, která dorazí na poštovní server, tvoří právě spam. Bohužel neškodné emailové zprávy se postupem času začaly měnit na promyšlené podvodné emaily, nabízející různé zboží a služby za příznivé ceny Proti spamu existuje několik způsobů ochran. Na poštovní servery se nasazuje tzv. antispamový filter, který kontroluje doručenou poštu na základě uživatelem definovaných pravidel a také dostupných spamových databází. Databáze již předem známých spamů se nachází na veřejně dostupných serverech a umožňují pravidelně aktualizovat antispamový filter. Bohužel ne všechny databáze jsou dostupné zdarma, a tím přináší antispamová ochrana další náklady pro firemní sektor. Součástí antispamu na serverové části bývá ve většině případů filter SpamAssasin. Jde o technologii, která obsahuje statická pravidla, na základě kterých dochází k bodování zprávy. Filtr např. při výskytu slova „sex“ přiřadí zprávě jeden bod a pokud zpráva dosáhne definovaného počtu bodů, bude označena za spam. Dalšími filtry, který se velmi často používají v oblasti SOHO, jsou samoučící filtry tzv. Bayesianské filtry. Tyto filtry se vyznačují schopností učit a rozlišovat, který email patří mezi spam a který ne. Učení probíhá v závislosti na uživateli, který označuje jednotlivé emaily podle toho,

zda se jedná o nevyžádanou poštu, či ne. Mezi další prvky ochrany proti SPAMu, patří SPF a Greylisting.

Metoda SPF využívá kontroly záznamu DNS versus doména a k ní přiřazené emailové servery. Pokud pochází email z jiného emailového serveru, než který je přiřazen dané doméně a používá jméno této domény, potom je označen za SPAM.

Metoda Greylisting je založena na opakovaném doručení zprávy. Standardně si emailové servery v případě neúspěšného doručení zařadí zprávu do fronty a snaží se ji odeslat znovu. Tzn. že emailový server poprvé zprávu odmítne, zaznamená IP adresu odesílacího serveru a přijme zprávu až při druhém pokusu o doručení z té samé IP adresy, jakou zaznamenal. Spamový SW(robot), který zprávy odesílá ve velkém množství, již nemá čas, aby znovu opakoval odesílání zprávy. Tato metoda je schopna v interakci s ostatními filtry odbourat až 99 % nevyžádané pošty.[22]

3.8 Instant Messangery

Jedná se o specifickou skupinu tzv. chatovacích programů, které slouží k online komunikaci mezi uživateli na celém světě. V době pomalého internetového připojení existovaly až na pár vyjímek pouze textové chatovací programy. V současné době se s rozvojem vysokorychlostního internetu mění i povaha těchto programů, které nyní nabízejí komplexní online komunikaci mezi uživateli. Typickými zástupci této skupiny jsou ICQ, Miranda, QIP, AOL Instant Messenger, Microsoft MSN a Yahoo IM a další. Kromě textové a hlasové komunikace nabízí některé z nich i video komunikaci a přenos souborů. A právě díky textové komunikaci a možnosti zasílání souborů, se stávají obávanou bezpečnostní hrozbou. SPAM se nevyhnul ani této oblasti, a tak jsou uživatelé zaplavováni nevyžádanými zprávami reklamního charakteru, falešnými zprávami a podob. Součástí těchto zpráv bývají i odkazy, které nasměrují uživatele stránky obsahující Trojské koně nebo jiné škodlivé scripty, které mohou způsobit ztrátu dat nebo i kolizi celého systému. Příkladem z praxe může být šíření viru Win32/Stration na podzim roku 2006, který se šířil nejen pomocí elektronické pošty, ale právě i pomocí Instant messangerů. K infiltraci systému došlo kliknutím na odkaz ve zprávě a následně se do počítače nainstaloval virus. Ten nejen že způsoboval kolaps systému (počítač se sám restartoval), ale také např. deaktivoval rezidentní ochranu antivirového programu NOD32. Přestože autoři chatovacích programů začali na tyto hrozby reagovat tím, že se ve zprávách automaticky odstraňuje hypertextový odkaz (u některých programů je tato volba ve výchozím stavu zapnuta, ale lze ji vypnout), největší břemeno spočívá na

uživateli samotném, který se musí rozhodnout, zda na odkaz v nedůvěryhodné zprávě klikne a nebo ne. Rozhodnutí bývá někdy velmi těžké, protože se některé viry rozesílají přímo z kontaktů uložených v napadaném počítači, a tak uživatel nemůže rozpoznat, zda se jedná o důvěryhodnou zprávu či ne. Příkladem může být opět šíření viru Win32/Stration. Ve firemní sféře bývá většinou Instant messaging zakázán. Povolení messagingu stojí firmy nemalé finanční náklady na zabezpečení a další následné investice do firewallu a IPS.

4 Ochrana operačních systémů MS Windows

Zabezpečení OS MS Windows a nejen jich, dnes hraje důležitou roli. Je velmi nerozvážné, připojit nezabezpečený počítač do internetu. Návody a postupy jak zabezpečit počítač jsou často publikovány na internetu nebo v knižních publikacích. Uživatelé je vyhledávají zpravidla až poté, kdy je jejich počítač infiltrován a subjektivně pozorují jeho zhoršenou funkcionalitu nebo došlo k jiné škodě. Nejčastější příčinou porušení bezpečnostních standardů je jejich neznalost, podceňování a nízká informovanost uživatelů PC. Jak tedy počítač správně ochránit, aby byl zajištěn bezpečnostní standard? V následujících kapitolách uvádím standardní postup pro instalaci a následné zabezpečení OS, který jsem doplnil o své praktické zkušenosti. Tento postup byl realizován, jak postupovat při zabezpečení OS Windows 2000 a Windows XP. Rady a tipy vycházejí převážně z mých zkušeností a dlouholeté praxe, a také z odborných publikací a článků. Nyní se pokusím nastínit jakým způsobem počítač zabezpečit, včetně důležitých rad, a to od instalace až do finálního nastavení OS.

4.1 Instalace MS Windows - SOHO

a) **Formátování** - pokud provádíte instalaci OS Windows na disk, který již operační systém obsahuje, vyplatí se vždy před vlastní instalací tento disk naformátovat. Formátováním dojde k odstranění všech informací a škodlivých programů z boot sektoru pevného disku, a tím se zabezpečí, že nově instalovaný systém nebude ihned po instalaci infikován. V případě instalace na nový disk, proběhne formátování také, protože nový disk nebývá ve většině případů formátován. Formátování disku můžete provést pomocí průvodce na instalačním CD MS Windows. Před vlastním formátování si zálohujte důležitá data na jiná média např. CD, DVD nebo jiný pevný disk. Pokud zálohujete instalační soubory některých programů, dobře si rozmyslete, které z nich si ponecháte. Některé programy totiž mohou obsahovat spyware nebo adware a tím může opět dojít k infikování systému. Při rozhodování Vám může pomoci stránka www.google.com. Ve vyhledávači zadáte: *„jméno programu“ adware OR virus OR spyware*. A pokud se na stránkách, které jsou výsledkem hledání neobjeví zmínka o tom, že by daný program obsahoval jaký-koli typ malware, můžete Váš program bez obav zálohovat. I když nic není zcela spolehlivé, bylo by

zbytečné, přeinstalovávat OS a potom znovu instalovat programy obsahující spyware.

b) **Instalace OS** – před instalací se přesvědčte, že používáte originální instalační CD, nebo kopii CD z důvěryhodných zdrojů. Z praxe jsem zažil kopie CD, které byly vytvořeny na infikovaném počítači, a při instalaci došlo k přenosu malware do nově instalovaného počítače. Dále během instalace nepřipojujte počítač do datové sítě, pokud si nejste jisti, že je tato síť bezpečná a chráněná před možnými útoky malware. Toto doporučení platí zejména pro oblast SOHO, kdy jsou počítače připojeny přímo do sítě internet pomocí vysokorychlostního připojení a nepoužívají žádné brány firewall. Ve firemní sféře se s připojením počítače do sítě předem počítá a tato je většinou velmi dobře zabezpečená. Dále je vhodné zvolit při instalaci silné heslo pro účet Administrátora, aby tento nemohl být později zneužit k neoprávněným zásahům do systému.

c) **Dokončení instalace** – po dokončení instalace a nahrání všech dostupných ovladačů, je doporučeno nainstalovat antivirový program a až po té se pokusit připojit k internetu a stahovat další aktualizace. Proč je jako první krok zvolena instalace antivirového programu má svůj důvod. Na internetu je nabízena řada freewarových bezpečnostních programů a bohužel některé z nich právě obsahují škodlivý software a antivirový program může pomoci takový software odhalit ještě před tím, než se stáhne do počítače nebo nainstaluje.

d) **Instalace opravných balíčků a záplat** – po instalaci antivirového programu je nutné stáhnout všechny opravné balíčky pro konkrétní OS a další následné záplaty. Pro OS Windows 2000 je nutné stáhnout ServicePack4 a následně aktualizovat OS. Pro Windows XP potom ServicePack2 a další následné aktualizace. Je doporučeno instalovat pouze poslední opravný balíček. Tento již všechny předchozí aktualizace a opravy obsahuje. Aktualizaci OS si můžete vynutit přímo na stránkách firmy Microsoft a nebo volbou „Windows Update“ přímo v daném operačním systému. V současnosti již bývají servisní balíčky implementovány přímo na originálním CD, a to jak pro Windows 2000 tak pro Windows XP

e) **Uživatelské účty** – účet pod kterým se budete do systému přihlašovat by měl mít omezená oprávnění a v žádném případě se nedoporučuje používat přímo účet administrátora. Administrátor má v systému neomezená oprávnění a získání nadvlády nad tímto účtem může znamenat katastrofu pro celý systém. Pokud

budete používat účet s omezeným oprávněním, značně tím snížíte riziko potencionální infiltrace Vašeho systému. Toto tvrzení jsem se pokusil dokázat v praktické části této bakalářské práce. U OS Windows XP Home Edition se při instalaci nezadává heslo administrátora, a proto je nutné jej zadat až po vlastní instalaci operačního systému. Heslo můžete zadat v příkazovém řádku pomocí příkazu *net user administrator HESLO* , přičemž místo slova heslo dosadíte Vaše heslo pro účet Administrátora.

f) **Bezpečnostní software** – přestože jsou dnes do antivirových programů implementovány skenovací moduly pro detekci spyware a malware, vyplatí se ještě instalovat software druhých stran, pro zvýšení bezpečnosti a důslednější kontrolu systému. Když selže jeden program, druhý ve většině případů uspěje. Programů je možné instalovat více, pouze je nutné dodržovat zásadu, že pouze jeden rezidentní štít z těchto programů bude aktivní.

4.2 Instalace MS Windows – firemní prostředí

Instalace ve firemních sítích bývá prováděna několika způsoby. Pro všechny typy instalací platí, že síť musí být řádně zabezpečena proti útokům a hrozbám z venčí. Instalace probíhají z připravených image OS, který je předem upraven pro dané firemní prostředí. Image obsahuje nainstalované aplikace a jejich bezpečnostní nastavení. Image jsou uloženy na serverech, které jsou dostupné pouze v síti LAN, ale zároveň umožňují instalovat.

4.3 Antivirové programy

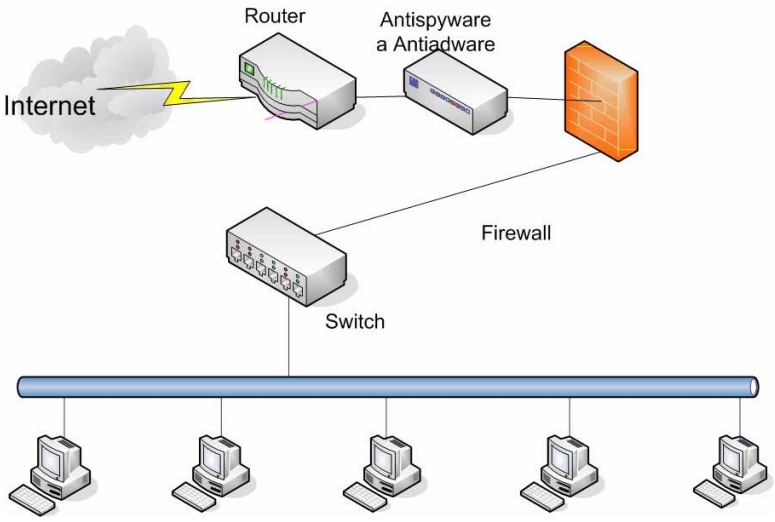
Z vlastní zkušenosti mohu pro oblast SOHO, ale i pro firemní prostředí doporučit jakýkoli antivirový program renomovaných firem jako jsou Grisoft, s.r.o.(AVG Anti-Virus Professional Edition), Alwil Software (Avast! 4), Eset, spol. s r.o.(NOD32 Antivirus), Symantec Corporation(Norton Antivirus) a další. Všechny výše uvedené programy jsou velmi kvalitní a dosahují různých ocenění v testech antivirových programů. Jednou z firem jež nabízí pro oblast SOHO antivirový program zdarma, je firma Alwil Software s programem Avast! 4 Home Edition. Pro jeho roční používání je nutné se zaregistrovat na webu výrobce tohoto software. Další firmou nabízející antivirový program pro oblast SOHO je Grisoft, s.r.o. se svým AVG Anti-Virus Free. Můžete použít kterýkoli z uvedených antivirových programů nebo antivir dalších firem, každopádně musíte dbát na to, aby v počítači byl instalován pouze jeden antivirový program. V případě instalace dvou a více antivirových programů, může dojít

až ke kolizi celého systému. To je způsobeno tím, že antivirové programy v sobě obsahují tzv. rezidentní štít, který na pozadí neustále kontroluje předem definované typy souborů a také síťový provoz. Tím je schopen zastavit virovou infekci ještě dříve, než se dostane do počítače. V případě antivirových programů tedy platí raději méně než více. Ve firemním prostředí se antivirový program instaluje i na tzv. internetové brány nebo firewally, kde kontrolují veškerý síťový provoz. Přesto je však důrazně doporučeno instalovat antiviry i na samotné stanice a zabezpečit tak počítačovou síť systémem tzv. dvojité ochrany, tzn. když selže antivir na internetové bráně, potom může virovou nákazu ještě zastavit antivir na stanici. Tento má za úkol také skenovat vyměnitelná média jako CD, DVD, Flashdisk a podob.

4.4 Antispywarové programy

Antispywarové programy tvoří po antivirových programech nedílnou součást každého OS a mnohdy se staví na téměř stejnou úroveň jako programy antivirové. Opět je řada antispywarových programů, které jsou dostupné pro oblast SOHO zdarma, ale s omezenými funkcemi. Mezi tuto skupinu mohu z vlastní zkušenosti jmenovat např. Spy-Bot, Ad-Aware, Spyware Terminator, AVG Anti-Spyware a další. V neposlední řadě mohu jmenovat také beta verzi programu od společnosti Microsoft Windows Defender, který je prozatím dostupný zcela zdarma, ale pouze oprávněným vlastníkům OS Windows. Další skupinu tvoří antispywarové programy placené. Jedná se buď o výše uvedené programy, které mají v placené verzi dostupné všechny funkce např. rezidentní štít, automatické aktualizace databáze a další, nebo programy další výrobců. Pro SOHO jsou freewarové antispywarové programy dostačující, ale nikoliv stoprocentně bezpečné, protože zavisí pouze na uživateli zda bude tyto programy aktualizovat a spouštět test systému, či nikoliv. Pro firemní prostředí je nutné zakoupit kvalitní a placené produkty, neboť v případě zcizení nebo ztráty cenných dat, hrozí firmě nemalá finanční, ale i jiná ztráta např. poškození dobrého jména firmy. I když antispyware bývá v poslední době integrován přímo do antivirového programu, řeší se ochrana narozdíl od SOHO jiným způsobem. Antispywarový program je nasazen přímo na internetové bráně a nebo před ní a na stanicích je instalován pouze antivirový program s detekcí potencionálně nežádoucích programů viz. obrázek č.6, v lepším případě antivirový program s integrovaným antispywarem.

Obrázek č. 6 Příklad zabezpečení sítě proti spywaru ve středně velké firmě



4.5 Firewally

Firewall je software nebo hardware, který brání a zabezpečuje přístup do počítače nebo datové sítě, a to jak aktivně, tak pasivně. Z těchto několika faktorů, můžeme usoudit, že se firewally dělí na dvě skupiny, a to hardwarové firewally a softwarové firewally.

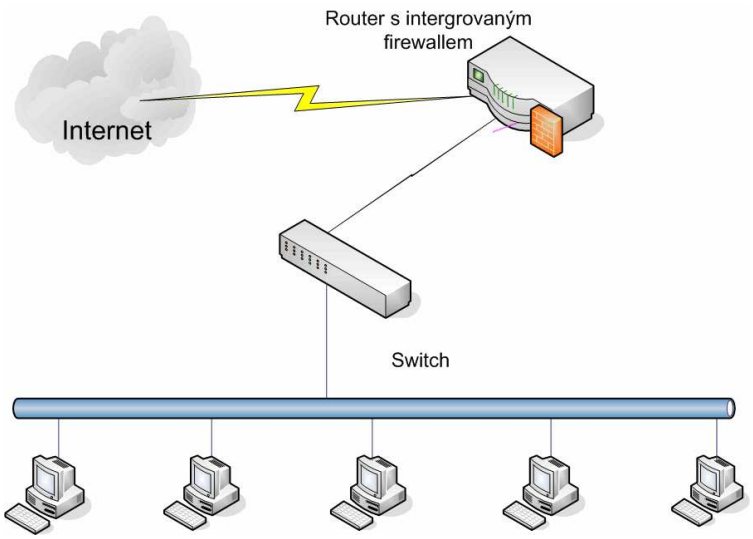
4.6 Hardwarové firewally

Jedná se o dražší variantu firewallů, ale za to kvalitnější, bezpečnější a výkonnější. Tato varianta hardwarového firewallu bývá zpravidla používána spíše ve firemním prostředí, tzn. v malých, středních a velkých firemních sítích. Tyto hardwarové firewally bývají ve většině případů aktivní a poskytují tak velmi kvalitní ochranu s včasnou detekcí a ochranou před průniky do sítě. Firewally aktivně skenují jednotlivé pakety a v případě podezření tyto pakety zastaví ještě před vstupem do sítě. Jejich součástí bývají často systémy pro detekci nežádoucích infiltrací či útoků tzv. IDS a IPS. Dále bývají součástí antivirové a antispywarové programy, které ještě více pomáhají detekovat nebezpečné hrozby z internetu. Zároveň tento typ firewallu poskytuje dostatečný výkon a stabilitu, která je důležitá zvláště ve firemním prostředí. Pasivní hardwarové firewally bývají využívány spíše v malých sítích a slouží pouze jako prvotní ochrana nebo-li zeď proti útokům z internetu. Avšak současný trend zasahuje i do oblasti SOHO, a to právě ve formě hardwarových pasivních firewallů. Tyto bývají integrovány např. společně s ADSL nebo Wi-Fi zařízením, které slouží pro připojení k internetu. Pro uživatele z oblasti SOHO však mají jednu nevýhodu. Tou je

alespoň částečná znalost nastavení a znalost bezpečnostní problematiky a jednotlivých portů.

Z mé zkušenosti však vyplývá, že většina uživatelů tento firewall vůbec nezapíná, a nebo ho pouze nechá zapnutý ve výchozím nastavení, čímž se schopnost detekce a zabezpečení snižuje. Tím je opět vidět, že hardwarový firewall je více směrován do firemního prostředí, kdy si mohou firmy dovolit správce počítačové sítě a nebo outsoursing zabezpečení sítě. Příklad zabezpečení malé sítě s firewallem můžeme vidět na obrázku č. 7.

Obrázek č. 7 Příklad zabezpečení malé sítě s firewallem

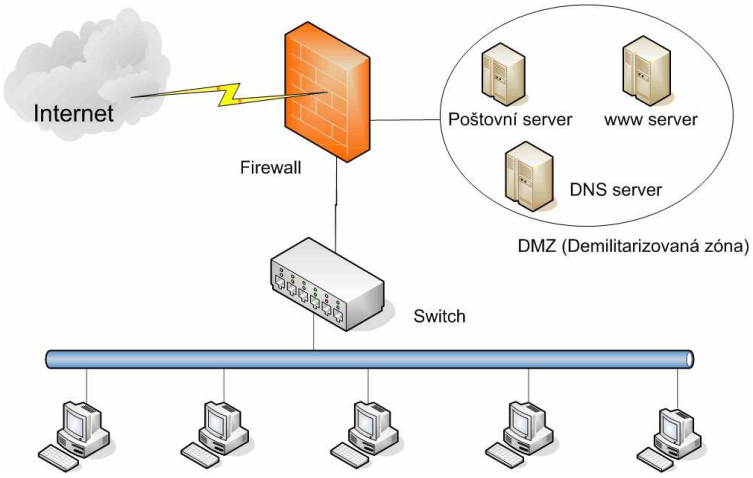


4.7 Softwarové firewally

Tento druh firewallu je používán především v oblasti SOHO a malých firem. Je přívětivý jak svou cenou, tak i možnostmi nastavení. Opět se softwarové firewally dělí na aktivní a pasivní, ale i podle způsobu použití. Softwarové firewally se mohou instalovat buď přímo do osobního počítače nebo na zvlášť vyčleněný počítač nebo server. Takový počítač se pak stává bezpečnostním serverem nebo-li internetovou branou, která zabezpečuje síť před případnými útoky. Mezi aktivní firewally, které se používají přímo na osobním počítači, patří např. produkt Kerio Personal Firewall od firmy Sunbelt Software nebo Zoner Alarm od firmy Zone Labs a další. Kerio Personal Firewall např. umožňuje zvolit, v jakém módu bude pracovat. Tzn. že při instalaci tohoto firewallu, si máme možnost vybrat, zda bude aktivní nebo pasivní. V aktivním módu se nás bude firewall neustále vyptávat, zda chceme danou akci povolit, nebo zakázat. Výhodou aktivního módu je to, že i méně zkušený uživatel má absolutní

kontrolu nad tím, co se děje v jeho počítači a není tak zatěžován složitým a odborným nastavením samotného firewallu. Tento se prakticky postupným dotazováním nastaví na požadovanou úroveň zabezpečení. V aktivním módu mohou firewally zabránit např. podvodným dialerům, které přesměrovávají vytáčené připojení k internetu na jiná čísla s větší sazbou za připojení. Bohužel praxe je jiná. Ze zkušenosti vím, že většina uživatelů po několika dnech obezřetné kontroly a zvažování povolit či nepovolit danou akci, začne bezmyšlenkovitě klikat na dotazovací dialogy. Většinou je to proto, že je dialogy, které se zobrazují několikrát za den obtěžují, nebo proto, že jim nerozumí, a tak ze strachu buď akci zakážou a nebo naopak povolí, což je ta horší varianta. Softwarové firewally používané přímo na stanicích mají ještě jednu nevýhodu, a tou je náročnost na hardware počítače, přesněji na operační paměť. Pokud chceme tedy využívat softwarového firewallu přímo na stanici, je nutné dopředu počítat s větší kapacitou operační paměti. V případě malých a středních sítí s počtem do 100 připojených stanic se ve většině případů používá vyhrazený počítač nebo server s právě nainstalovaným softwarovým firewallem. Operačním systémem bývá většinou některá z Linuxových nebo Unixových distribucí, a to zvláště vzhledem k jejich stabilitě a bezpečnosti. Ale ani to nebývá vždy pravidlem. Např. ISA Server od firmy Microsoft nebo Kerio Winroute Firewall od firmy Kerio Technologies s.r.o. jsou dokladem toho, že se softwarové firewally nevyhýbají ani OS Windows. Opět zde platí, že pro správnou funkčnost firewallu je nutné odborné nainstalování a nastavení. Z praxe mohu ještě zmínit tzv. open source firewallové distribuce např. IPCOP firewall nebo Endian Firewall. Z vlastních zkušeností mohu potvrdit, že zvládnou zabezpečit síť do 100 připojených stanic. Protože se však jedná o open source distribuce a není tedy zaručena žádná podpora a tím ani spolehlivost, mohu tento typ firewallu doporučit pouze pro sítě, kde není kladen velký důraz na bezpečnost dat a nepřetržitou dostupnost internetu. Tyto distribuce pomáhají vytvářet sami uživatelé a počítačoví nadšenci, kteří se sdružují v různých komunitách. Proto se u open source firewallů může stát, že po aktualizaci nefunguje firewall správně a náprava trvá mnohdy několik dní. Tím se stává daná počítačová síť nechráněnou a otevřenou vůči potencionálním hrozbám. Softwarové firewally mají velké pozitivum v možnosti rychlé reakce na nové bezpečnostní hrozby. Příklad zabezpečení středně velké firemní sítě se softwarovým firewallem viz. obrázek č.8.[7]

Obrázek č.8 Příklad zabezpečení středně velké firemní sítě



4.8 IDS a IPS

Mezi další možnosti jak ochránit počítačovou síť, patří systém detekce a prevence IDS a IPS. Jedná se zařízení tzv. senzory, které se umístí jak do nechráněné oblasti před firewall, tak do chráněné oblasti za firewall. Výsledky, které z obou zařízení obdržíme, poté můžeme porovnat a vyhodnotit.[2]

4.8.1 IDS

IDS je systém detekce narušení. Můžeme ho definovat jako soubor nástrojů a metod, které pomáhají identifikovat a hlásit neautorizované a neschválené síťové aktivity. Přestože je IDS označováno za systém detekce narušení, narušení jako takové detekovat nedokáže. Detekuje pouze takové činnosti, které mohou, ale nemusí být narušením. IDS je pouze jedna komplexního zabezpečení, do kterého ještě patří IPS a firewall. Podle toho jak je IDS v síti rozmístěna, můžeme stanovit, zda se jedná o zabezpečenou síť, či nikoliv. Systém IDS má společné vlastnosti s antivirovým softwarem, kdy stejně jako antivirový program, používá známé signatury za účelem rozpoznání potencionálních rizik. IDS se dělí na tři kategorie:

a) Uzlově orientované systémy detekce narušení HIDS – software umístěný na tomto systému, může skenovat aktivitu všech uzlových zdrojů. Dále může zapsat libovolnou událost do bezpečnostní databáze a prověřit případnou shodu se záznamy bezpečnostních rizik obsažených ve znalostní databázi.
b) Síťově orientované systémy detekce narušení NIDS – analyzuje síťové pakety díky nimž může posoudit, zda se jedná o napadení či ne. Monitoruje síťový provoz, zaznamenává, hlásí nebo generuje výstrahu. Dále rekonstruuje datový

(bitový) proud a analyzuje v něm přítomnost vzorů nebezpečného chování. Tyto schopnosti jsou obsaženy ve většině výkonných routerech.

c) Hybridní IDS – kombinuje HIDS s NIDS[7]

4.8.2 IPS

IPS můžeme chápat jako systém prevence proti narušení. IPS se umisťuje v síti a tu následně monitoruje. Pokud dojde k nějaké události, provede se příslušné opatření podle předem definovaných pravidel. Přestože se IPS vyvinulo z IDS, jedná se o odlišné bezpečnostní nástroje lišící se funkčností a účinností. IDS se například oproti IPS neumisťuje do sítě a je pasivní. Systémy IPS se dělí na dvě skupiny:

a) Uzlově orientované HIPS - velmi dobře pracují v ochranných aplikacích
b) Síťově orientované NIPS

IPS se chová tak, že pokud není nějaká činnost uvedena na seznamu povolených akcí ve znalostní databázi, zabrání provedení této činnosti. IPS se dále skládá ze čtyř částí:

- Normalizátor provozu – přerušuje provoz, provádí analýzu a znovusložení paketů, plní základní blokovací funkce
- Monitor služeb – vytváří referenční tabulku, která klasifikuje informaci a pomáhá tvarovači řídit tok informací
- Detekční jednotka – porovnává signálové vzory s referenční tabulkou a vyhodnocuje příslušnou odpověď
- Tvarovač – řídí tok informací

IDS a IPS poskytují nástroj pro řízení a rozpoznání útoků na firemní síť. Mohou vytvářet profily útoků a napomáhají tak k vytváření bezpečnostních opatření. V případě soudního sporu mohou posloužit jako důkaz proti útočníkům. Porovnání obou systému je názorně uvedeno v tabulce č.1.[2]

Tabulka č. 1 Porovnání IDS a IPS

IDS	**IPS**
instalace na segment sítě (NIDS) a uzel (HIDS)	instalace na segment sítě (NIPS) a uzel (HIPS)
funkce pasivního prvku	zapojují se sériově – nejsou pasivní
neschopnost analyzovat šifrovaný provoz	vhodné pro ochranné aplikace
centrální správa řízení	centrální správa řízení
využití pro detekci hackerských útoků	vhodné pro blokovaná webových rizik
upozorňuje výstrahou (reaktivní)	blokování činností (proaktivní)

4.9 Silná hesla

Hesla tvoří nedílnou součást každého OS a zabezpečují tak přístupy do systému nebo jen k otevření souboru. Význam hesel v zabezpečení sítě organizace je často podceňovaný a přehlížený. Hesla představují základ ochrany proti neoprávněnému přístupu nejen do firemní sítě. Systémy řady Microsoft® Windows Server 2003 obsahují novou funkci, která kontroluje složitost hesla účtu Administrator při instalaci operačního systému. Pokud je zadané heslo prázdné nebo nesplňuje požadavky na složitost, otevře se dialogové okno instalační program systému Windows a upozorní na rizika plynoucí z nepoužívání silného hesla pro účet Administrator. Pokud heslo ponecháte prázdné, nebude možné tento účet používat vzdáleně přes síť.

Slabá hesla usnadňují útočníkům snadný přístup k počítačům i síti, zatímco odhalení silných hesel je poměrně složité i pomocí softwaru odhalujícího hesla. Nástroje k odhalení hesel jsou neustále zlepšovány a výkon počítačů používaných k tomuto účelu se stále zvyšuje. Software odhalující hesla používá jednu ze tří následujících metod:

- inteligentní odhadování
- slovníkové útoky
- násilné automatizované útoky - zkouší všechny možné kombinace znaků

Automatizovanou metodou lze odhalit jakékoli heslo, pokud je k dispozici dostatek času. Odhalení silného hesla je však mnohem složitější než v případě slabého hesla.

Zabezpečený počítač má nastavená silná hesla pro všechny uživatelské účty. Silné heslo musí vypadat dle níže uvedených kritérií:

- musí obsahovat nejméně sedm znaků
- nesmí obsahovat uživatelské jméno, vlastní jméno, jména členů rodiny, či příbuzných, název firmy a podob.
- nesmí obsahovat slova, která je možné nalézt ve slovníku
- musí se lišit od předchozích hesel, tzn. že není přípustné opakovat např. Heslo1, Heslo2, Heslo3 atd.
- musí obsahovat alespoň jednu číslici, jedno velké písmeno, jedno malé písmeno a jeden netisknutelný znak[20][6]

4.10 Penetrační testy

Software vytvořený hackery a jinými programátory hledá v počítači chyby nebo slabiny, které využívá pro své útoky. A proto byly vytvořeny různé metody, které pomáhají zjistit míru zabezpečení informační struktury proti běžným a známým typům útoků. Mezi jednu z metod patří právě penetrační testy, jejichž smyslem je zjistit do jaké míry je počítačová síť zabezpečena proti vnějším útokům. Pomocí těchto testů, je možné kontrolovaně napadat počítačové sítě a zjišťovat tím slabá místa. Je doporučováno provádět penetrační testy opakovaně, aby bylo možné předejít bezpečnostním chybám a rizikům, které se mohou objevit. Opakovaným testováním si můžeme také ověřit, zda byly odstraněny všechny nedostatky, zjištěné při předchozím testu. Penetrační testy pracují podobně jako antivirové programy, které hledají viry podle předem definované databáze. Během penetračních testů jsou tedy vyhledávány bezpečnostní slabiny také podle předem daného variantního seznamu. Penetrační testy se dělí do dvou skupin, a to na externí a interní.

a) Externí penetrační testy cíleně vyhledávají možné bezpečnostní slabiny počítačové sítě pomocí simulovaných útoků vedených z veřejné sítě internet. Metodika externích testů je zaměřena na kontrolu zabezpečení běžně používaných technologií, mezi něž patří např.:

- **Firewally** – DoS a DDoS útoky, změny směrování, zranitelnost, otevřené porty, DMZ
- **Backdoory** – programy, které slouží umožňující získání kontroly nad počítačem
- **CGI scripty** - získání plné kontroly nad webovými stránkami

- **DNS systémy** – možnost předstíráním identity síťového zařízení a nasledné přesměrování
- **Mailové systémy** – spam, kontrola elektronické pošty na přítomnost virů
- **FTP systémy** – možnost neoprávněného přístupu k souborovému systému a převzetí kontroly nad serverem
- **LDAP systémy** - zneužití adresářové služby LDAP
- **Síťové odposlouchávání** - špatná konfigurace aktivních prvků umožní síťové odposlouchávání
- **NFS systémy** - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem
- **Systémy založené na RPC** -vzdálené volání procedur
- **Systémy se sdílením zdrojů** - získání neautorizovaného přístupu, k systémům pro sdílení dat např. Samba, SMB, Active Directory
- **SNMP systémy** - bezpečnostních díry v implementaci Simple Network Management Protocolu v aktivních prvcích sítě

Mezi nejznámější firmy zabývající se problematikou penetračních testů, patří např. firma Anect, Autocont a další. Prostřednictvím internetu je možné využít služeb, které nabízejí online test bezpečnosti. Server www.paranoia.cz provádí test zabezpečení firewallu, čili zabezpečení sítě za úplatu a na vyzkoušení nabízí tuto službu 4x do měsíce zdarma. Online testy bezpečnosti a test na přítomnost virů, nabízí i další renomované firmy jako Symantec Corporation a další.[21]

b) Interní penetrační testy slouží především k detekci a zkoumání vnitřních slabin počítačové sítě. Bohužel současný trend ukazuje, že zcizení citlivých dat může být způsobeno nejen útokem z vnějšku, ale především útokem ze vnitř. Autorem vnitřních útoků bývá ve většině případů nespokojený zaměstnanec, který se chce např. obohatit a nebo jen poškodit dobré jméno firmy. Ještě horší jsou případy, kdy je zaměstnanec podplacen konkurenční firmou, pro kterou za úplatu zcizí data firmy u níž je zaměstnán. I když se předpokládá, že zaměstnanec nebude provádět útoky přímo ve vnitřní síti, může ale například díky špatně nastaveným právům poškodit data nebo celé databáze, či spustit Trojského koně, který může citlivá data odesílat do vnější sítě.

Je doporučováno, aby si uživatel nebo správce počítačové sítě neprováděl penetrační testy sám, ale využil specializovaných firem, které tento bezpečnostní audit provádí jako službu a zároveň mohou nezávisle vyhodnotit zabezpečení informačního

systému. Penetrační testy se tedy týkají převážně firemního prostředí než oblasti SOHO, kde tyto metody prověření bezpečnosti nejsou ekonomicky výhodné. Penetrační testy sice nevyřeší zabezpečení informační sítě, ale jsou doporučovaným doplňkem bezpečnostního auditu a patří k nejlepším nástrojům pro prevenci a zabezpečení počítačové infrastruktury.[19]

4.11 Internetové scannery

Pro kontrolu zabezpečení počítačové sítě mohou pomoci také tzv. internetové online scannery. Jedná se o bezplatné nástroje antivirových společností, které pomáhají detekovat malware v testovaném počítači. Bohužel ve většině případů tyto scannery pouze odhalí škodlivý software, ale už nenabízí možnost jeho odstranění. K odstranění malware jsou po provedení testu nabídnuty produkty dané firmy zabývající se bezpečnostním softwarem. Některé firmy nabízí online test jednoho daného souboru, u kterého si nejste jisti, zda je bezpečný. Typický příkladem může být online scanner společnosti Alwil Software. Další možností jak otestovat počítač na virovou infekci nebo přítomnost spywaru, nabízí např. společnost Symantec Corporation nebo McAfee. Vzhledem k šířce a možnosti využití, jsou tyto scannery směřovány především na oblast SOHO.

4.12 Internetové lišty

Jinou možností jak ochránit počítač před malwarem nabízí tzv. internetové nebo vyhledávací lišty. Lišty jsou ve většině případů koncipovány pro webový prohlížeč Internet Explorer a nabízí různé možnosti, od blokování nevyžádaných reklamních oken, po blokování spywaru, phisingu nebo kontroly pošty na spam. Některé dokonce kontrolují soubory na přítomnost virové infekce. Internetové bezpečnostní lišty nabízí známé vyhledávače např. Google, Seznam, Yahoo a další. Lišty jsou nabízeny většinou zdarma a směrovány opět do oblasti SOHO. Z praxe mohu potvrdit, že i když svou funkci plní dobře, nemohou nahradit plnohodnotný antivirový a antispywarový software, který nejen že dokáže komplexně zabezpečit daný počítač, ale také nabízí plnou podporu výrobce, včetně pravidelných aktualizací. Bohužel často se stává, že někteří uživatelé tento fakt neznají, nebo podceňují a spoléhají se pouze na tento bezplatný bezpečnostní software.

5 Praktická část

5.1 Cíl praktické části

Cílem praktické části bylo ověření možnosti a četnosti průniku malware do počítačů s OS Windows 2000 a Windows XP instalovaným dle definovaného bezpečnostního standardu. Pro možnost porovnání byla do některých testů navíc zahrnuta betaverze nejnovějšího OS Windows Vista, protože každá novější verze OS Windows publikuje vyšší úroveň zabezpečení. Toto tvrzení firmy Microsoft bylo výchozím, pro stanovení hypotézy č. 1.

Dále jsme v praktické části chtěli ověřit, že definovaný bezpečnostní standard není dostačující, aby zabránil průniku malware do počítače. Dle doporučení Microsoftu je potřeba bezpečnostní standard OS doplnit o antivirový software třetích stran, který velkou měrou přispívá ke snížení rizika infiltrace malware do OS. Dalším doporučením Microsoftu pro zvýšení bezpečnosti OS, je používat uživatelský účet s omezeným oprávněním. Toto doporučení jsme rovněž testovali.

Pro realizaci praktické části práce, jsme si stanovili následující hypotézy, které jsme ověřovali ve třech testech.

Hypotéza č.1

Menší počet průniků malware bude zaznamenán v OS Windows XP. Rozdíl mezi OS Windows 2000 a Windows XP by měl být markantní.

Hypotéza č. 2

Menší počet průniků malware bude zaznamenán v OS s omezenými právy uživatele, než v OS s právy administrátora.

Hypotéza č. 3

Nejmenší počet průniků malware bude zaznamenán v OS s nainstalovaným antivirovým programem a firewallem druhých stran.

5.2 Bezpečnostní standard operačních systémů

Bezpečnostním standardem rozumíme nejen níže uvedený výčet instalačních komponent u jednotlivých OS, ale i vlastní instalační proceduru, jak je popsána v kapitole 5. Pro testování zabezpečení operačních systémů Windows byly vybrány tři verze:Windows 2000, Windows XP Professional a pro porovnání beta verze operačního systému Windows Vista. Pro věrohodnost testu je nutné, aby systémy splňovaly základní požadavky výrobce na bezpečnost operačního systému. To znamená, že všechny tři systémy obsahují poslední bezpečnostní balíčky, které byly v době testování

dostupné a jsou zbaveny všech bezpečnostních nedostatků Bezpečnostní standard u vybraných OS představuje následující instalaci jednotlivých komponent:

- Windows 2000 – servicepack 4 a všechny dostupné záplaty instalované pomocí procedury Windows update
- Windows XP – servicepack 2 a všechny dostupné záplaty instalované pomocí procedury Windows update
- Windows Vista – dostupné záplaty v době testování pro danou betaverzi, instalované pomocí procedury Windows update

5.3 Metodika testování průniku malware do OS

Od úmyslu použít softwarové nástroje a s nimi spojenou metodiku penetračních testů popsanou v kapitole 4.8, jsem musel ustoupit z důvodu obtížné dostupnosti tohoto software. Společnosti, které penetrační testy komerčně nabízejí si svou metodiku chrání jako své know-how. Při penetračních testech se používají testovací programy, které jsou zaměřeny nejen na testování vlastního operačního systému, ale především na testování zabezpečení sítě. Testovací programy jsou ve většině případů založeny na platformě UNIX nebo LINUX, ale existují i programy pro platformu Windows. Vzhledem k ceně testovacích programů a jejich odborného nastavení, jsem se rozhodl realizovat test na zabezpečení osobních počítačů prostřednictvím vlastní autorsky navržené metodiky.Autorsky navržená metodika vychází z praktických zkušeností specialistů ICT zajišťující podporu koncových uživatelů. V praxi uživatelé PC velmi často vypínají antivirovou ochranu a další bezpečnostní SW. Někdy je pro plně funkční běh některého SW vypnutí bezpečnostního programu doporučeno. Na počítačích v oblasti SOHO jsou nejčastěji instalovány freewarové bezpečnostní programy, proto pro porovnání jednotlivých výsledků byl zvolen tento software. S vybranými SW bezpečnostními programy si může podobný test provést každý uživatel zcela sám. Jako antivirový program, byl vybrán AVAST Home Edition od společnosti Alwil Software. Důvodem je jeho užitná hodnota, tzn. že po bezplatné registraci na stránkách výrobce, je možno tento program používat po dobu jednoho roku v plné verzi edice Home. Dalším kritériem byl velmi dobře propracovaný rezidentní štít, který dokáže blokovat škodlivý software ještě dříve, než se stáhne do počítače. Výběr antispywarových programů stanoven dle zkušeností z praxe a ze statistik nejvíce používaných bezplatných antispywarových programů. Pro lepší porovnání byly zvoleny celkem tři programy, a to Ad-aware od firmy Lavasoft, AVG-Antispyware od firmy Grisoft a Spy-Bot.

5.3.1 Autorsky navržený postup pro test bezpečnosti OS

Praktický test probíhal na počítačové učebně, vybavené celkem 12 osobními počítači. Nebyl předpoklad, že prováděné testy jsou závislé na použité HW konfiguraci počítače, ale spíše na způsobu připojení k síti internet, např. pomocí ADSL, WIFI, kabelové televize, vytáčené připojení. Přesto bylo zajištěno, aby počítače byly shodné HW konfigurace.

Tabulka č.1 Konfigurace počítačů použitých k testování

Procesor	AMD AthlonXP 2500+
Operační paměť	1 GB DDR400
Pevný disk	WesterDigital 120 GB
Základní deska	Epox 3RDA+
Grafická karta	nVidia GeForce 6200 128MB AGP

Jednotlivé testy, ověřující stanovené hypotézy, byly realizovány odděleně. Po ukončení předchozího testu, byl na počítač znovu instalován bezpečnostní standard daného OS. Každý jednotlivý OS byl instalován na dva počítače, které obsluhoval jeden testující pracovník - tester. Tester v každém testu postupoval podle předem připraveného testovacího scénáře, který byl shodný pro všechny tři testy. Před zahájením každého testu byli testeři instruováni pro provedení testu tak, aby byla zajištěna jejich jednotnost. Každý test trval 48 hodin. Aktivní zobrazování internetového obsahu dle testovacího scénáře prováděli testeři celkem 2 hodiny během prvních 24 hodin a 3 hodiny během druhých 24 hodin. Celkem aktivní část testu trvala 5 hodin v každém testu. Počítače byly nepřetržitě připojeny do internetu 48 hodin pomocí vysokorychlostního připojení ADSL. Doba připojení k internetu byla zvolena záměrně, protože k potencionální infiltraci může za určitých okolností dojít i během pasivní části testu. Připojení k internetu bylo realizováno pomocí routeru s funkcí NAT a bez dalšího zabezpečení. Tzn. že počítače mají vlastní IP adresy, které nejsou z vnější sítě viditelné. Vlastní průběh testu spočíval v systematickém navštěvování stránek, u kterých se předpokládá, že obsahují škodlivý software viz. příloha č. 1. Jedná se především o stránky s nevhodným obsahem, tzn. stránky nabízející cracky, erotiku a podob. Dále byly navštěvovány běžné stránky viz. příloha č.2. Po skončení testovací doby byl operační systém otestován pomocí bezpečnostních freewarových programů pro detekci

spyware a adware, a také pomocí antivirového programu Avast4 Home. Všechny po sobě jdoucí testy byly vyhodnoceny a porovnány. Každý test byl jednou opakován po sedmi dnech.

Pro ověření hypotézy č. 1 byl proveden první test. V tomto testu byly na osobní počítače nainstalovány předem připravené image OS Window 2000 Professional, Windows XP Home Edition.a OS Windows Vista. Softwarová konfigurace bezpečnostního standardu byla instalována bez bezpečnostního software druhých a třetích stran. Operační systém byl ponechán ve standardním nastavení se všemi dostupnými aktualizacemi zkontrolovanými pomocí procedury Windows Update a s uživatelskými právy administrátora. Pro ověření hypotézy č.2 byl proveden druhý test. Počítače byly opět nainstalovány s připravených image. Z důvodu nekompatibility jednoho z detekčních programů AVG-Antispyware, byla vynechána instalace OS Windows Vista, protože bez použití všech detekčních programů nelze výsledek testu OS Windows Vista porovnat. OS byly ponechány ve standardním nastavení a uživatelský účet byl u každého OS nastaven na účet s omezeným oprávněním a bez software druhých stran. Operační systémy byly zkontrolovány pomocí procedury Windows Update, zda obsahují poslední bezpečnostní aktualizace.

Pro ověření hypotézy č.3 byl proveden třetí test. Pro věrohodnost byly počítače opět nainstalovány z připravených image. OS Windows Vista byl z výše uvedených důvodů vynechán. OS byly ponechány ve standardním nastavení a uživateli byly přiděleny práva administrátora. Dále byly operační systémy zkontrolovány zda obsahují všechny dostupné bezpečnostní aktualizace. Kontrola byla provedena pomocí procedury Windows Update. Do obou OS byl doinstalován antivirový program Avast4 Home a osobní softwarový firewall Kerio Personal Firewall od firmy Sunbelt Software.

5.4 Výsledky testu č. 1

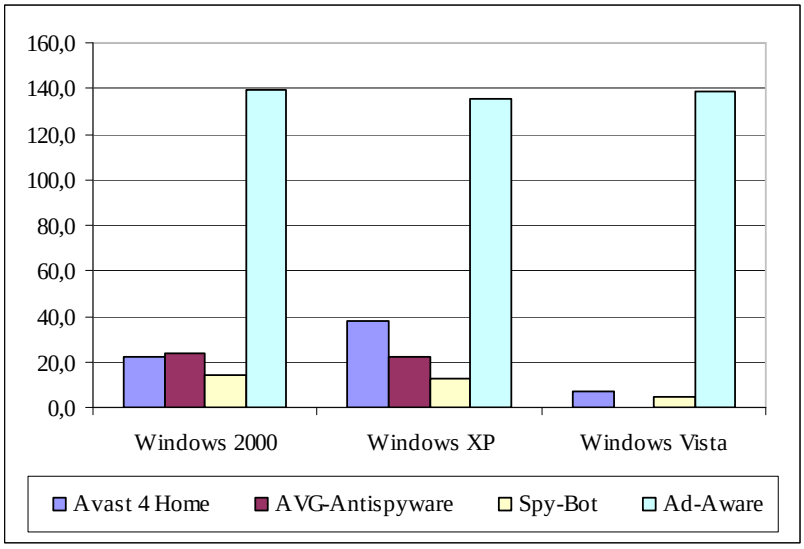
V první části testu byl porovnán počet výskytů všech druhů malware v obou testovaných OS, které se infiltrovaly během aktivního vyhledávání a zobrazování obsahu internetu. Počítač s OS Windows XPa se dostal do stavu, kdy spuštění jakéhokoli programu bylo velmi zdlouhavé a výchozí stránka prohlížeče Internet Exploreru byla neustále přesměrovávána. U Windows Vista se objevila v průběhu testování chyba v aplikaci Windows Defender a v důsledku této chyby přestala aplikace kontrolovat datový tok z internetu. Windows Defender navíc neustále nabízel ke spuštění komplexní test celého počítače. Celý OS Window Vista se stal nakonec

nestabilním a neustále se zobrazovalo chybové hlášení *„Windows Explorer stopping, working and restarting“*. Následkem této chyby docházelo k neustálemu restartu nastavení plochy a systému. Z neznámých důvodů nebylo možné spustit detekční program AVG-Antispyware. Protože se jednalo o test betaverze, není možné určit, zda se jednalo pouze o chybu dané testovací verze OS Vista nebo zda průnik škodlivého softwaru byl původcem pádu systému. Výsledky prvního testu jsou přehledně uvedeny v tabulce, uvedené hodnoty v prvních dvou sloupcích představují počet diagnostikovaného malware. Ve třetím sloupci je uveden průměr nalezeného malware z obou měření. Tento průměr je pro porovnání použit v grafickém znázornění.

Tabulka č. 2 Počet diagnostikovaných malware v testu č.1

Operační systémy	**Windows 2000**			**Windows XP**			**Windows Vista**		
Počet výskytů /Detekční programy	**1. měření**	**2. měření**	**∅**	**1. měření**	**2. měření**	**∅**	**1. měření**	**2. měření**	**∅**
Avast 4 Home	24	21	22,5	37	39	38,0	8	7	7,5
AVG-Antispyware	25	22	23,5	23	22	22,5	x	x	x
Spy-Bot	15	13	14,0	13	12	12,5	4	5	4,5
Ad-Aware	150	129	139,5	141	130	135,5	147	130	138,5

Graf č. 3 Počet nalezených malware v jednotlivých OS pro test č. 1



5.5 Výsledky testu č. 2

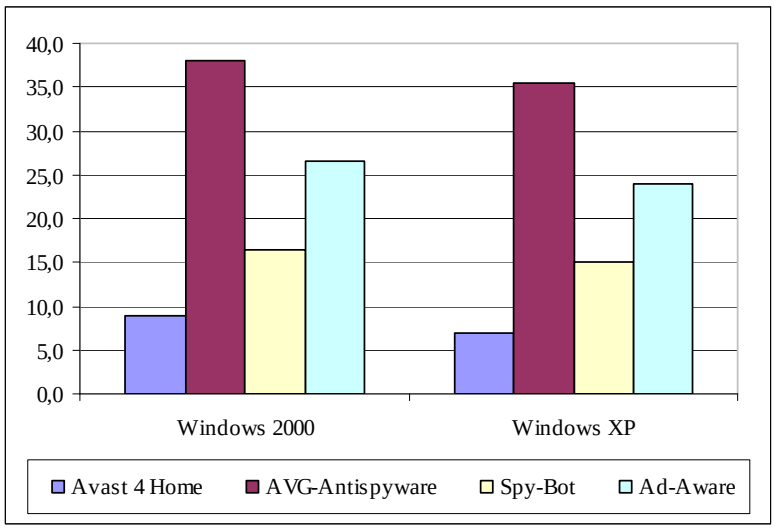
Ve druhé části testu byl opět porovnán počet výskytů všech druhů malware v obou testovaných OS, které se infiltrovaly během surfování po internetu. Žádný z obou testovaných operačních systémů nebyl nestabilní a neprokazoval žádné výrazné známky infiltrace malwarem. Výsledky druhého testu jsou přehledně uvedeny v tabulce,

uvedené hodnoty v prvních dvou sloupcích představují počet diagnostikovaného malware. Ve třetím sloupci je uveden průměr nalezeného malware z obou měření. Tento průměr je pro porovnání použit v grafickém znázornění.

Tabulka č. 3 Počet diagnostikovaných malware v testu č.2

Operační systémy	**Windows 2000**			**Windows XP**		
Počet výskytů /Detekční programy	**1. měření**	**2. měření**	**∅**	**1. měření**	**2. měření**	**∅**
Avast 4 Home	10	8	9,0	8	6	7,0
AVG-Antispyware	39	37	38,0	35	36	35,5
Spy-Bot	16	17	16,5	14	16	15,0
Ad-Aware	27	26	26,5	25	23	24,0

Graf č. 4 Počet nalezených malware v jednotlivých OS pro test č. 2



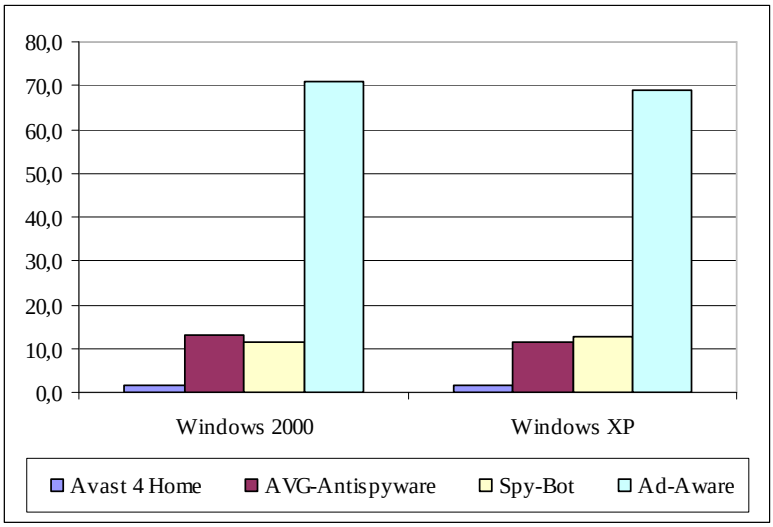
5.6 Výsledky testu č. 3

Ve třetí části testu byl opět porovnán počet výskytů všech druhů malware v obou testovaných OS, které se infiltrovaly během surfování po internetu. Ani jeden z obou testovaných operačních systémů neprokazoval známky infiltrace malwarem. Při testování byly několikrát zobrazeny výstražná dialogová okna, varující před potenciální infiltrací systému. Dialogy byly negovány, tzn. že antivirový program i osobní firewall zakázal všechna nežádoucí spojení, pro která byly zobrazeny výstrahy. Výsledky třetího testu jsou přehledně uvedeny v tabulce, uvedené hodnoty v prvních dvou sloupcích představují počet diagnostikovaného malware. Ve třetím sloupci je uveden průměr nalezeného malware z obou měření. Tento průměr je pro porovnání použit v grafickém znázornění.

Tabulka č. 4 Počet diagnostikovaných malware v testu č.3

Operační systémy	**Windows 2000**			**Windows XP**		
Počet výskytů /Detekční programy	**1. měření**	**2. měření**	**∅**	**1. měření**	**2. měření**	**∅**
Avast 4 Home	2	1	1,5	2	1	1,5
AVG-Antispyware	11	15	13,0	10	13	11,5
Spy-Bot	11	12	11,5	12	13	12,5
Ad-Aware	72	70	71,0	70	68	69,0

Graf č. 5 Počet nalezených malware v jednotlivých OS pro test č. 3



6 Závěr

Test č.1 potvrdil námi uvedenou hypotézu, že novější OS nabízí více bezpečnosti a je odolnější vůči infiltraci nežádoucího malware z internetu. Rozdíl v počtu nalezeného malware v OS Windows 2000 a Windows XP však byl velmi malý. Tím nebyl zcela potvrzen předpoklad markantního rozdílu mezi novým a starším operačním systémem. Dle očekávání dopadla nejlépe betaverze OS Windows Vista. Přestože tato verze OS neobsahovala žádný software druhých stran a uživatelský účet měl práva administrátora, byl výskyt nalezeného malware v OS Windows Vista srovnatelný s výsledky třetího testu. To dokazuje, že vzhledem k předchozím verzím, byl učiněn velký pokrok z hlediska bezpečnosti OS Windows. Bohužel z neznámého důvodu nebylo možné na testovaném OS Windows Vista spustit detekční program AVG-Antispyware, a proto bylo od ostatních testů upuštěno. Dá se však předpokládat, že při použití antivirového programu a firewallu druhých stran, se bezpečnost OS Windows Vista ještě zvýší a tím by mohl dosáhnout lepších hodnot měření. Výsledky testu Windows Vista mohou být ovlivněny také tím, že v době testování nebyla dostupná finální verze, která bude zbavena všech chyb z předešlých betaverzí.

Test č.2 opět potvrdil námi uvedenou hypotézu, že při používání uživatelských účtů s omezeným oprávněním bude infiltrace OS menší než při používání operačního systému ve výchozím (standardním) nastavení a uživatelskými účty s právy administrátora. Je zajímavé, že se výsledky druhého testu blíží více k výsledkům třetího testu než testu prvního. Tím jsme ověřili i četná doporučení ICT specialistů o používání uživatelských účtů s omezeným oprávněním.

Test č.3 potvrdil námi uvedenou hypotézu, že operační systémy doplněné o antivirový program a osobní firewall, budou obsahovat nejmenší výskyt malware. Nejlepšího výsledku bylo dosaženo i přes fakt, že uživatelské účty měly práva administrátora. Tzn. že software druhých stran byl schopen zamezit případné instalaci nežádoucího malware nebo na něj uživatele upozornit.

Provedené testy jednoznačně potvrdily již známé a doporučované bezpečnostní postupy a nastavení, které jsou prezentovány všemi odborníky na bezpečnost OS. Jedná se především o používání uživatelských účtů s omezeným oprávněním, kdy tato volba může v některých případech ochránit počítač téměř identicky, jako počítač na kterém je používán účet administrátora s nainstalovaným antivirovým programem a osobním firewallem. Dále testy potvrdily, že používání antivirového programu a firewallu je

v současné době u počítače připojeného do sítě internet nezbytností. Testy také potvrzují, že časté používání freewarových antispywarových programů má své opodstatnění, a to i přesto, že se jedná o neplacené programy, které jsou ochuzeny o některé důležité prvky. V neposlední řadě se potvrdila teorie, že nový OS Windows Vista přinese lepší zabezpečení celého systému, i když původní očekávání nebylo dosaženo. Nejlepších výsledků dosáhl systém Windows XP s nainstalovaným firewallem a antivirovým programem.

Příloha č. 1

Seznam stránek s potencionálně škodlivým obsahem

http://neworder.box.sk
http://www.cracks.am
http://www.cracking.to
http://www.keygen.ms
http://www.cracks.mu
http://orion.crackteam.ws
http://www.crackdb.com
http://wareznova.com
http://www.freeserials.ws
http://www.serialsdb.com
http://www.crackserver.com
http://crackdb.org
http://serialkey.net
http://www.thekeys.ws
http://www.superserials.com
http://www.easycracks.net
http://www.mscracks.com
http://www.serials.ws
http://bestserials.com
http://www.crackzplanet.com
http://www.keygen.ws
http://www.myfreepaysite.com
http://isafetywarning.com
http://keygen.us
http://malwarewiped.com
http://www.mytraf.info
http://www.powerddl.com
http://www.protectionszone.com
http://www.warezbay.com
http://www.warezdownloads.info
http://www.zcrack.com
http://www.warez-vortex.net
http://www.sex-photo.ru
http://www.securityplugins.com
http://www.pestcapture.com
http://errorsafe.com
http://www.antivermins.com
http://adultfriendfinder.com
http://alldnserrors.com
http://www.antivirusgolden.com
http://asta-killer.com
http://www.cracktop.com
http://www.crackhell.com
http://www.astalavista.box.sk
http://astalavista.us
http://www.cracksdata.com
http://www.crackserver.com

http://download.errorsafe.com
http://easy.box.sk
http://www.easywarez.com
http://ak.exe.imgfarm.com
http://apps5.oingo.com
http://depositfiles.com
http://down.cd

Příloha č. 2

Seznam běžně navštěvovaných stránek

http://www.seznam.cz
http://www.atlas.cz
http://www.google.com
http://www.centrum.cz
http://www.zive.cz
http://www.pctuning.cz
http://www.cdr.cz
http://www.svethardware.cz
http://www.spyware.cz
http://www.hoax.cz
http://www.viry.cz

Seznam literatury

[1] **Bezpečnost Windows 2000/XP, CP, 2003**

[2] **Detekce a prevence počítačového útoku, Grada, 2005**

[3] **Hacking bez tajemství Windows 2000, CP, 2003**

[4] **Slabá místa Windows aneb jak se bránit hackerům, Comp. Media s.r.o., 2004**

[5] **Bezpečná počítačová síť, Verlag Dashöfer, 2006**

[6] **Zabezpečení počítačových sítí bez předchozích znalostí, CP, 2005**

[7] **Bezpečnost počítačových sítí, CP, 2005**

[8] **Moderní počítačové viry, Igor Hák, 2005**

[9] **Jak se vyhledávají viry, časopis ExtraPC, 10/06**

[10] **Windows Vista – Co v sobě ukrývají?, 12.7.2006**
http://www.pctuning.cz

[11] **Viry a jejich funkce**
http://www.viry.cz

[12] **Spyware a jak na něj**
http://www.spyware.cz

[13] **Hoax a jiné podvodné emaily**
http://www.hoax.cz

[14] **Historie operačních systémů Windows, Unix, Mac OS a Linux, 13.4.2006**
http://mujmac.cz

[15] **Jakou edici zvolit, 31.8.2006**
http://vista.zive.cz

[16] **Microsoft představuje novou ochranu uživatelů před padělky a pirátstvím, 11.10.2006**
http://www.zive.cz

[17] **O virech a lidech, 08.10.2005**
http://www.zive.cz

[18] **Drahá bezpečnost, časopis CHIP 12/06**

[18] **Microsoft . Platforma Windows 2000**
http://www.microsoft.com

[19] **Penetrační testy: Aneb sám sobě hackerem, 8/2004**
http://www.automatizace.cz

[20] **Silná hesla, 21.1.2005**
http://microsoft.com

[21] **Bezpečnostní testy a analýzy**
http://www.compunet.cz

[22] **Braňte se před Spamem, časopis Connect, 11/2005**

[23] **Po phishingu přichází pharming, časopis Computerworld, 8/2005**

[24 **Skrytá hrozba Rootkitů, časopis Connect!, 10/2006]**

[25] **Nebezpečí jménem phishing, časopis PCWorld Security, 8/2005**

[26] **Pojmy**
http://www.spyware.cz

[27] **Co je to HOAX**
http://www.hoax.cz

Seznam zkratek

Active Directory	Adresářová služba Windows 2000, obdoba NDS firmy Novell
ActiveX	DCOM objekty nejčastěji využívané jako součásti web stránek
BIOS	Basic Input Output System je v počítačích třídy PC základní komunikační vrstva mezi HW a operačním systémem
Bit Locker	technologie pro šifrování dat na disku
Broker Process	proces, který umožňuje lepší zabezečení při stahování dat z internetu a podílí se na přesměrování stažených dat do dočasné složky.
Cache	Rychlá mezipaměť pro ukládání nejpoužívanějších dat, může být hardwarová nebo řízená softwarově jako ukládání dat na disk
Compatibility Redirector	směruje zápisy do složky
Crack	software, který je vytvořen pro odstranění ochrany zkušební verze programu a zpřístupnění programu v plné verzi
DDoS	zkratka pro distribuované DoS útoky, tzn., že se útoku účastní více počítačů.
DMZ	Demilitarizovaná zóna – bezpečnostní zóna chráněná proti vnějším útokům a zároveň oddělená od vnitřní sítě
DOS útok	Denial of Service – útok probíhá tak, že útočník zahlcuje cílový systém velkým množstvím nesmyslných požadavků
EFS	Encrypting File System - pomocí systému souborů EFS je možné bezpečně ukládat data. Zabezpečení je realizováno zašifrováním dat ve vybraných souborech a složkách systému souborů NTFS.
FAT	File Allocation Table – tabulka alokace souborů
FTP	Protokol pro přenos souborů
Greylisting	ochrana proti SPAMu metodou opakovaného zasílání zprávy
HDD	pevný disk, který slouží pro ukládání dat a instalaci OS
HIPS	uzlově orientované systémy IPS
LDAP	Lightweight directory access protocol)
LPS	Low Privilege Service - nízkoprivilegovaný mód, kde mají uživatelé omezená práva

MBR	Master Boot Record – systémová oblast, která slouží pro zavádění operačního systému
NAP	Network Access Protection – soubor technologií pro ochranu sítě
NFS	Network file system
NIPS	síťově orientované systémy IPS
OS	Operační systém
POP3	Protokol pro přijímání elektronické pošty
RPC	Remote procedure call
SMTP	Protokol pro odesílání elektronické pošty
SNMP	Simple Network Management Protocol - asynchronní, transakčně orientovaný protokol založený na modelu klient/server
SPAM	nevyžádaná emailová zpráva většinou reklamního charakteru
SPF	Sender Policy Framework – jedna z ochran proti SPAMu
TCP	Transmission Control Protocol patří mezi základní komunikační protokoly internetu. Pomocí tohoto protokolu se mohou spojit dva nebo více počítačů a přenášet data
TPM	Trusted Platform Module
UAC	User Account Control – vrstva v OS Windows Vista umožňující používat účty, které nemají administrátorská práva
USB	Universal Serial Bus – univerzální sériová sběrnice pro připojení periférií k počítači