Zabezpečení systému Windows

Windows Security Protection

Filip Hujer

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Filip HUJER**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení systému Windows**

Zásady pro vypracování:

1. **Sestavte literární rešerši z oblasti zabezpečení systému Windows.**
2. **Formulujte současné bezpečností hrozby především směřující směrem z internetu.**
3. **Prozkoumejte možnosti standardního zabezpečení v současnosti nejpoužívanějších verzí operačního systému Windows.**
4. **Najděte vhodné programy, které by neměly chybět v počítači pro ochranu před vnějšími útoky uvedenými v bodu 2.**
5. **Navrhněte a otestujte nejvhodnější sadu programů především z oblasti freeware nebo open-source.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

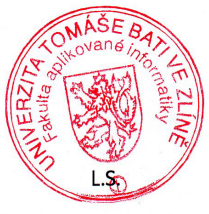
1. **O počítačích, IT a internetu -- Živě.cz [online]. Dostupné z URL: http://www.zive.cz**
2. **Technet.cz -- Technika kolem nás [online]. Dostupné z URL: http://www.technet.cz**
3. **Microsoft security [online]. Dostupné z URL: http://www.microsoft.com/security/**
4. **Microsoft [online]. Dostupné z URL: www.microsoft.com/CZE/**
5. **Bott, E., Siechert, C. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Computer Press. 2004. ISBN: 80-722-6878-3**
6. **Doseděl, T. Počítačová bezpečnost a ochrana dat. Computer Press. 2004. ISBN: 80-251-0106-1**

Vedoucí bakalářské práce: **Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010



prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tématem bakalářské práce je zabezpečení operačních systémů Windows XP a Vista. Výsledné poznatky mají za úkol poučit a posléze navést na stabilní řešení zabezpečení operačního systému, především z pohledu nepříliš zkušeného uživatele, který danou sadu nebude využívat pro komerční účely. Přínosem této práce bude doporučení nejvhodnějších kombinací bezpečnostních softwarových nástrojů, určených pro optimální zabezpečení operačního systémů. Hlavní kriteriem výběru softwarových bezpečnostních nástrojů je jejich licenční poskytnutí zdarma. V první kapitole se budu věnovat výchozí zabezpečení operačních systémů Windows XP a Vista bez programové výbavy jiných výrobců. Důraz bude kladen i na vývoj jednotlivých upgradů (service packy). Druhá kapitola bude zaměřena na definování hlavních hrozeb, pocházejících z vnějšího prostředí a šířených především pomocí sítě internet. Třetí kapitola bude obsahovat rešerší významných bezpečnostních programů. Tato rešerše bude vytvořena na základě kvality programů ohodnocených renomovanými bezpečnostními a počítačovými magazíny. Poslední kapitolu věnuji testování vybrané sady bezpečnostního softwaru na výše zmíněných hrozeb.

Klíčová slova: zabezpečení, firewall, antivirus, antispyware

ABSTRACT

The topic of bachelor thesis is Windows Security Protection. Resulting knowledge to the task of learning and then navigate to a stable operating system security solution, especially in view of not experienced users who will not use the suite for commercial purposes. Contribution of this work will be recommendations to the most appropriate combination of security software tools, designed for optimum security. The main selection criteria of security software tools is provided free of their license. In the first section, I shall discuss the initial security of Windows XP and Vista without additional program equipment from other manufacturers. Emphasis will be placed on the development of various upgrades (service packs). The second chapter will focus on defining the main threats to the external world (internet). The third chapter will include looking for major security programs. This research will be created based on the quality of programs ranked by renowned security and computer magazines. The last chapter is devoted to testing the selected set of security software for the above-mentioned threats.

Keywords: security, firewall, antivirus, antispyware

PODĚKOVÁNÍ

Chtěl bych s úctou poděkovat svému vedoucímu práce, panu ***Ing. Jiřímu Vojtěškovi, Ph. D.,*** za jeho cenné rady a připomínky, bez kterých by tato bakalářská práce nevznikla v podobě, jaké je.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Ve své bakalářské práci, psané na téma "Zabezpečení operačního systému Windows", se budu věnovat k vyhledání nejvhodnějších bezpečnostních softwarových nástrojů, určených pro optimální zabezpečení obou operačních systémů Windows XP a Windows Vista.

V první kapitole teoretické části rozeberu problém výchozího zabezpečení operačních systémů Windows XP a Windows Vista. Důraz budu přikládat vývoji bezpečnostního obsahu u jednotlivých servisních balíčků (service packs). Budu poukazovat na bezpečnostní slabiny operačních systému, na které v praktické části navrhnu vhodné bezpečnostní softwarové nástroje.

V druhé kapitole teoretické části se budu věnovat bezpečnostním hrozbám, ohrožující operační systémy Windows XP a Windows Vista. Zaměřím se především na hrozby nejčastěji dostupné z vnějších sítí (internet). Podrobně rozeberu druhy bezpečnostních hrozeb, mezi které patří viry, trojské koně a backdoor infiltrace.

Ve první kapitole praktické části zpracuji rešerši bezpečnostních nástrojů poskytovaných zdarma. Programy byly determinovány dle renomovaných počítačových periodik a dle hodnocení významných elektronických portálů. Souhrn bezpečnostních nástrojů poskytovaných zdarma jsem tematicky rozdělil na antivirovou, antispywarovou a firewallovou ochranu.

Ve druhé kapitole praktické části otestuji vybrané kombinace bezpečnostních nástrojů před reálnými hrozbami. Tyto programy budu testovat na jejich reakci vůči simulovaným hrozbám ve virtuálním prostředí.

Výsledné poznatky budou mít za úkol poučit a posléze navést na stabilní řešení zabezpečení operačního systému, především z pohledu nepříliš zkušeného uživatele, který danou sadu nebude využívat pro komerční účely. Přínosem této práce bude doporučení vhodného zabezpečení pro operační systém Windows pomocí softwarových nástrojů, určených pro optimální zabezpečení. Hlavní kriteriem výběru softwarových bezpečnostních nástrojů je jejich licenční poskytnutí zdarma.

I. TEORETICKÁ ČÁST

1 VÝCHOZÍ ZABEZPEČENÍ POUŽITÉ U OS WINDOWS

V této kapitola se věnuje krátkému shrnutí základních zabezpečovacích prvku operačních systému Windows. Kapitola se také zabývá politikou zabezpečení a to verzí Windows XP a Vista. Hlavním úkolem je uvedení do problematiky bezpečnosti operačních systémů Windows a její dostatečnosti.

1.1 Výchozí zabezpečení použitá u OS Windows XP

Windows XP patří mezi starší operační systémy, ale i v této době můžeme najít velký počet uživatelů, který je stále využívá. S vysokou pravděpodobností se tento systém bude stalé využívat ve vysoké míře, až do přechodu na nový operační systém Windows 7. Do této doby zabezpečení Windows XP bude stále aktuálním tématem. Microsoft vydal prohlášení, že vývoj aktualizací bezpečnosti systému bude aktivní do 8. dubna 2014.

Mezi prvními informacemi o významné bezpečnostní chybě v operačním systému Windows XP se objevuje nechráněná služba Universal Plug and Play. Její hlavní nedostatek spočívá ve snadném zneužití pro buffer overflow útok a pro více nebezpečné útoky DoS a Ddos. Tento problém Microsoft neodstranil v žádné aktualizaci a to ani v jednom ze tří Service Packů.[7]

Windows XP byl v minulosti také kritizován za jeho přecitlivost na malware, viry, trojské koně a červy. Tyto škodlivé kódy omezují rychlost operačního systému významnou měrou. Míra nebezpečí, které tyto hrozby způsobují, jsou umocněny implicitně nastaveným přístupem k administrátorskému účtu, který obdrží uživatel hned po instalaci. Tento účet umožňuje neomezený přístup do základů systému, které jiné účty nemají. Pokud má nezkušený uživatel přístup na tento účet, ve většině případů napomůže k ohrožení operačního systému.

Windows, díky svému vysokému podílu na trhu, je nejčastějším cílem pro tvůrce virů a jiných škodlivých kódů. Bezpečnostní díry často nejsou na první pohled zřejmé, ale ne zcela neviditelné a to hlavně do doby, dokud je někdo nezneužije. Microsoft uvedl, že každé uvolnění záplaty pro opravu výše zmíněných bezpečnostních děr, pomáhá tvůrcům škodlivého softwaru k identifikování těchto děr. Tito Hackeři zjišťují, jaké problémy záplaty opravují, a pak útočí proti systémům, které tyto opravy ještě neobsahují. Společnost Microsoft doporučuje, aby uživatelé zapnuli automatické aktualizace, aby se nestávali snadným cílem. Většina IT oddělení větších firem potřebují k testování

aktualizací před jejich vysláním napříč systémy předpovědět problémy s kompatibilitou softwaru a infrastruktury. Implementace oprav se prodlužuje a doba, kdy je systém ponechán nezajištěný zvyšuje úspěšnost napadení hackerem.

1.2 Windows XP Service Pack 1

Obsah Service Packu 1 nebyl příliš obsáhlý. Nyní je stažitelný jen jakou součást SP2. Samostatná podpora již byla ukončena, neobsahovala příliš razantní změny. Dle testu byla SP1 rychlejší jen o 0,5% než SP2. [7]

1.3 Windows XP Service Pack 2

Mezi výrazné změny obsaženy v Service Pack 2, se považuje:

- Vylepšené zabezpečení programu Internet Explorer
- Propracovanější implicitně zapnutý Firewall
- Vylepšené Centrum zabezpečení
- Lepší dohled nad a Antivirovým programem
- Windows Firewall

Service pack 2 se ovšem nevyvaroval řádce chyb:

- Zabezpečení Internet Explorer činilo velké potíže
- Blokace vysokého počtu bezpečných skriptů ve FTP protokolu
- Nutnost většího prostoru na Harddisku [7]

1.3.1 Centrum zabezpečení ve Windows XP SP 2

Centrum zabezpečení připravuje centrální správu klíčových prvků zabezpečení. Neustále kontroluje stav jednotlivých komponent a v případě zjištění nefunkčnosti některého ze subsystémů varuje uživatele. Tento prvek se u uživatelů nesetkal s přílišným ohlasem, uživatelům se zdál spíše otravným. Obsahuje i možnost vypnutí.

Je soustředěno (aktualizace SP 2) na tři základní okruhy:

- ochrana proti virům,
- automatické aktualizace
- brána firewall.

Neobsahuje implicitní antivirovou ochranu, kterou dokáže kontrolovat. Nicméně Centrum zabezpečení přítomnost antiviru vyžaduje. V okně Centra zabezpečení si Windows udává informaci o činnosti antiviru a o aktuálnosti virové databáze. Hlavním problémem je, že s vyšším počtem antivirových programů není kompatibilní a Centrum zabezpečení je nerozpozná.

Centrum zabezpečení zajišťuje propojení s automatickými aktualizacemi. Ve výchozím stavu jsou automatické aktualizace povoleny. V konfiguraci je možné nastavit frekvenci pravidelných kontrol nových aktualizací a hlavně režim fungování automatických aktualizací – od automatického stáhnutí na pozadí, přes pouhou notifikaci, až po úplné vypnutí, což samozřejmě Microsoft logicky tvrdě nedoporučuje.

1.3.2 Windows XP SP 2 Firewall

Je to aplikace, která z počátku nebyla příliš kvalitní. Vykonával funkci pouhého filtru, který příliš nezvládal kontrolovat odchozí provoz. U firewallu je kontrolována jeho aktivace na všechna aktivní síťová rozhraní, u automatických aktualizací je uživatel nucen nastavit pravidelnou kontrolu dostupnosti aktualizací a v sekci antivirů se kontroluje přítomnost antivirového řešení s čerstvou virovou databází.

Funkce firewall je zabránění útokům zevnitř i z venku. Jednodušší forma firewallu (dříve známá jako Internet Connection Firewall (ICF)) již existovala v předchozích verzích Windows. Service Pack 2 tento bezpečnostní prvek posiluje ve výbavě a hlavně zde zavádí jednu zásadní změnu – firewall je implicitně zapnutý. Zamezuje masivnějšímu útoku červů, kteří zneužívají otevřené porty sítě. Windows firewall je v SP2 podstatně propracovanější, samozřejmě spektrem nabízených služeb neútočí na pozici komerčních řešení třetích stran a pravděpodobně se o to ani nesnaží. Patří spíše do oblasti základní výbavy systému. Přístup do nastavení firewallu je možný z Centra zabezpečení. [12]

Samozřejmě Centrum zabezpečení není vázáno pouze na produkty Microsoftu, ale nabízí otevřené rozhraní pro produkty třetích stran, pomocí kterého se tyto produkty informačně propojí s Centrem zabezpečení. [12]

1.4 Windows XP Service Pack 3

Service Pack 3 je poslední service pack. Přes 10 % obsahu bylo věnováno převážně novým opravám. Tyto opravy se přímo podílely na bezpečnosti operačního systému. Mezi očekávané přínosy se počítá s upgradovaným generátorem náhodných čísel, který podléhal velké kritice uživatelů již od dob systému Windows 2000. Microsoft zvýšil rychlost a implementaci aktualizací. Service pack 3 obsahoval nové služby:

- Network Access Protection
- Microsoft Kernel Mode Cryptographic Module
- Detekce Black Hole Router [7]

1.4.1 Network Access Protection

Jak již název napovídá, tato služba provádí Ochranu síťového přístupu. Její hlavní funkcí je provádět inspekci všech systémů připojujících se do hlídané sítě. Zaměřuje se na kontrolu stavu klientova zabezpečení a na porovnání požadavky administrátora. Pokud tato kontrola nenachází očekávané hodnoty, NAP klientova práva omezí, popřípadě zcela mu zamítá přístup. Windows Vista službu NAP obsahuje ve výchozí verzi vydání.[18]

1.4.2 Microsoft Kernel Mode Cryptographic Module

Je to modul, ke kterému přistupují ovladače až na úrovni jádra a využívají jeho šifrovací algoritmy. Patří mezi vítané prvky vylepšení operačních systémů Windows XP SP3.Využívá se pro vyšší zabezpečení při implementaci druhé šifrované vrstvy nad službou NAP. Tato implementace přístupná jen na administrátorské úrovni. V této vrstvě probíhá nastavování pravidel pro šifrováním chráněnou komunikaci a interním ověřováním sítě. Šifrování probíhá pomocí algoritmu Triple-DES, které jsou přístupné skrze jádro operačního systému.[18]

1.4.3 Detekce Black Hole Routerů

Služba Detekce Black Hole Router obsahuje podobné chování jako Černé díry. Černé díry ve vesmíru stahují veškerou hmotu do svého středu, tak i ta to služba detekce Black Hole Router mizí síťové pakety. Tyto pakety se vymazávají a to bez zpětného návratu platného ICMP(Internet Control Message Protocol). Služba, která se v předchozích verzích nevyskytovala, pomáhá ochránit uživatele před vnějšími vlivy a zároveň příliš neomezovat detekci routerů. Dříve se k detekci routerů využíval příkaz ping se sekvenci ručně zadávaných příkazů a parametrů [18]

1.5 Výchozí zabezpečení použitá u OS Windows Vista

Windows Vista jsou považována za nejbezpečnější Windows v historii (v době před příchodem Windows 7). Microsoft vyvinul na bezpečnost velkou pozornost. Jedním z důvodů bylo bezpečnější obchodní transakce. Microsoft představil několik významných novinek v zabezpečení a provedl několik důležitých změn v architektuře. Zabezpečení počítačů v domácnosti a v podnikovém prostředí se v mnohém liší.

Operační systém Windows Vista se vyznačuje mnohem robustnějším zabezpečením, než předchozí operační systémy Windows. Některé funkce jsou nové, zatímco jiné rozšiřují ochrany, které již byly k dispozici v předchozích verzích systému Windows.

Mezi hlavní změny patří:

- Restriktivní instalace
- Integrovaná ochrana proti spywaru
- Vylepšená brána firewall
- Bezpečnější používání Internetu

1.5.1 Restriktivní instalace

V minulých verzích operačního systému Windows mohly nebezpečné programy provádět stahování a instalace bez vědomí uživatele. Při každém pokusu o instalaci softwaru v operačním systému Vista je uživatel vyzván, aby instalaci potvrdil. V některých případech je nutnost k zadání administrátorského hesla.

1.5.2 Integrovaná ochrana proti spywaru

Nástroj proti spywaru pro verzi operačního systému Microsoft XP byl dříve k dispozici ke stažení. Nicméně nyní je přímo integrován do operačního systému Vista.

1.5.3 Vylepšená brána firewall

Brány firewall předchozích verzí systémů Windows kontrolovaly pouze příchozí provoz, což byla vážná chyba. V operačním systému Vista je možnost nakonfigurovat bránu firewall tak, aby řídila také odchozí provoz, což nabízí možnost obrany, před interakcí kdy se nebezpečný kód tajně připojoval k Internetu z koncové stanice.

1.5.4 Bezpečnější používání Internetu

Díky uvedení verze prohlížeče Microsoft Internet Explorer 7 je používání Internetu s operačním systémem Vista bezpečnější. Hlavním pokrokem je že ovládací prvky ActiveX jsou ve výchozí konfiguraci operačního systému Vista zakázány. Prohlížeč Internet Explorer 7 zároveň obsahuje nástroje proti phishingu a spoofingu.

1.5.5 Uživatelské účty a šifrování

User Account Control (UAC) je často považováno za nejvýznamnější a nejkontroverznější vylepšení Windows Vista v bezpečnostním úhlu pohledu. Hlavním cílem je separovat od sebe jednoznačně uživatelská nastavení a citlivé části OS a to už jak v registrech nebo na Harddisku. V důsledku to znamená, že potřebuje-li aplikace spojení s oblastí operačního systému, muže tak vykonat jen se souhlasem uživatele.

Zjevná výhoda UAC je, že mnoho počítačových virů, spywaru a jiného škodlivého softwaru, takto proniká do systému jen u menšího počtu případů. Mezi nevýhody patří neustálá kontrola UAC bezpečné programy, jehož důsledkem je zpomalení systému. [8]

1.5.6 BitLocker

V operačním systému Vista, představuje uživatelský šifrovací program pro data uložená na Harddisku. Jeho klíčovou úlohou je chránit diskový oddíl s vlastním OS, k čemuž je dobře vybaven šifrou AES 128bit a Trusted Platform Module s PINem (modul na základní desce, sloužící jako úložiště pro ochranu šifrovacích klíčů). Klíč obdobně je možno uložit i na USB externí disk. Tuto funkci využijí i správci sítí a to s rozšířením Active Directory.

BitLocker se v mnoha směrech se projevuje jako velmi vítaný nástroj, který je rychlý, snadno ovladatelný, má příkazovou řádku a možnost obnovy dat. [8]

1.5.7 Vista Firewall

Vista Firewall obsahuje vylepšení v mnoha směrech, které byly dříve kritizovány v souvislosti s XP. Firewall monitoruje komunikaci oběma směry, stejně jako veškeré protokoly. Tento firewall je údajně odvozen od 64bitové verze Windows XP a umožňuje nastavení i s výjimkami programů nebo portů. Dokáže rozlišit různé sítě a všeobecně spojuje jednom místě velkou řadu komponentů, které nikdy dříve ve Windows propojeny nebyly. V praxi lze díky tomu nejen povolit vybraný komunikační kanál, ale současně určit, že tento kanál bude otevřený výhradně pro ověřená spojení a finálně na něm dosáhnout i šifrování.

Navzdory všem těmto výhodám byl Vista Firewall od počátku kritizován kvůli málo intuitivnímu ovládání a absenci funkce, ohlašující pokusy programů o odchozí komunikaci. Zejména uživatelé s nevelkými zkušenostmi tak měli značné problémy. Výše zmíněnou chybu se Microsoft pokusil napravit Vista Firewall Control, ale ani tento pokus nedopadl dle očekávání. Symantec brzy upozornil na to, že už samotná koncepce firewallu je chybná, neboť malware si může přístup k Internetu sám povolit a začít odesílat data (Symantec mimochodem snadno obešel i takový PatchGuard, který v 64bitové verzi Windows brání programům v upravování jádra). Další nevýhodou je, že v implicitně nastaveném firewallu, korigování odchozích spojení defaultně vypnuto, důsledkem čehož vysoké počty uživatelů tento program neaktivovalo.

Je tedy zřejmé, že i Vista Firewall je nástrojem problematickým, byť tomu vlastně tak vůbec být nemuselo. Microsoft si tak nějak jenom neuvědomil, že celá řada běžných uživatelů Windows si s ním zkrátka dost dobře neporadí. Dodávám ještě, že ve vlastním

Centru zabezpečení oproti Windows XP Service Pack 2 přibyla nová kategorie, která má na starost monitoring Internet Exploreru a řízení uživatelských účtu. [8]

1.5.8 Windows Defender

Microsoft vytvořil AntiSpyware program, který představuje poměrně účinnou pomoc v boji proti nežádoucímu spywaru. Spolupracuje i s programem Internet Explorerem 7, ale samo o sobě to rozhodně není důvodem další glorifikace programu Internet Explorer 7 a ani masy průměrných uživatelů to nepřesvědčilo o jeho využití. Nicméně jiné dovednosti už si pozornost zaslouží. Postaven je na bázi programu GIANT AntiSpyware a na rozdíl od jiných freeware aplikací obsahuje i nástroje pro aktivní monitorování a funkci ochrany v reálném čase. Automaticky stahuje aktualizace, scannuje na pozadí (což umožňuje naplánování systémového scannu na požadovaný čas) a zahrnuje rovněž Průzkumníka softwaru. Díky tomu není problém rychle zobrazit všechny programy, spouštěné bezprostředně po startu operačního systému. [8]

1.6 Windows Vista Service pack 1

První servisní balík je opětovným sloučením jádra systému v klientské i serverové vývojové větvi Windows. Windows Vista byla odvozena z jádra Windows Serveru 2003. Souběžně s Windows Vista, byl vyvíjen Windows Server 2008 (s vývojovým označením Windows Server Longhorn). Jeho vývoj tak byl o zhruba jeden rok delší než vývoj Windows Vista. Změna provedené v jádře právě za tento rok se do Windows Vista odrazí v podobě SP1. Ani u Windows XP nepřinesl první servisní balíček nijak zásadní změny viditelné uživatelem, natož pak nové funkce. Totéž se stalo i u Windows Vista. Microsoft se v této verzi soustředí na změny uvnitř systému - vylepšení stability, kompatibility, spolehlivosti a výkonu. O tom svědčí i několik v minulosti vydaných záplat soustředících se právě na vylepšení obdobného typu. [7]

Velké negativní zpětné vazby se Microsoftu dostává od uživatelů, kterým instalace narušila nejen operační systém, ale dokonce dala za vznik nekompatibility s dříve funkčním hardwarem či poškození. Vista v SP1 je nekompatibilní s vysokým počtem ovladačů zvukových karet, kodeky SoundMax a Connexant, integrovanými čipy Creative i HD kodeky Realtek. V SP1 se často vyskytují problémy s poškozováním systémových

souborů. Toto poškození může dospět do stádia, kdy se Vista z důvodu dané chyby nespustí.

1.6.1 Nedostatky operačního systému Vista

Microsoft při výrobě Windows Vista projevil snahu o vylepšení úrovně zabezpečení. Z důvodu inovace a předělání základů systému je většina novinek nedokonalá. Ochrana není kompletní a ani účinná bez vedlejších prostředků.

Mezi základní nedostatky operačního systému Windows Vista patří absence alespoň průměrné antivirové ochrany. V praxi je koncová stanice vybavená tím to systémem otevřena většině hrozeb z internetu typu viry, červy a trojské koně. Vyskytují se zde prvky systému, které napomáhají odstranění a zabraní škodlivým kódům v instalaci, ale ve srovnání s dnešními antivirovými programy jsou nedostačující. Z výše zmíněných důvodu je obranu proti hrozbám nutno hledat jinde.

Ve Vistách Microsoft přináší vylepšenou verzi brány firewallu, která v implicitním nastavení od výrobce není příliš vhodná pro nezkušené uživatele. V tomto nastavení neblokuje odchozí provoz, což v dnešní době je očekávaný standard firewallu, který je dostupný u většiny konkurence. Nezkušený uživatel nebude schopen rozpoznat, jen pomocí pop-up okna jestli dotazovaný program vhodný pro povolení či blokaci.

Microsoft poprvé přináší anispywarovou ochranu, která je integrována do operačního systému. Windows Defender neobsahuje dostatečné prvky k ochraně proti spywaru. Je potřeba, přidat nové funkce, aby byl tento program konkurence schopný. Předběžné testy společnosti Symantec objevili vysoký počet spywaru, který Windows Defender nezastavil. [17]

2 INTERNETOVÉ HROZBY OPERAČNÍCH SYSTÉMŮ WINDOWS

V druhé kapitole vymezuji nejčastější internetové hrozby, které ohrožují a omezují funkce Operačního Systému Windows nebo šíří soukromé informace o uživateli. Hlavním úkolem je uvést čtenáře do problematiky nejčastějších hrozeb internetu, které mohou ohrozit bezpečnost koncovou stanici uživatele.

2.1 Viry

Tento pojmenování tohoto typu malware bylo odvozeno od jeho chováni, které je nápadně podobné virům v biologické praxi. Biologický vir je nebezpečný pouze při kontaktu s hostitelskou buňkou, obdobně je tomu i u počítačových virů. Virus je škodlivý kód, který napadá jádro programu, přepíše, replikuje se a infikuje jiné soubory. Virus ovšem není schopen sebeaplikace bez hostitelského souboru. Při spuštění infikovaného souboru se zároveň spouští interakce viru, při které se snaží infikovat co nejvyšší počet vhodných hostitelů.

Hostiteli jsou nejčastěji:

- Spustitelné (executable) soubory.
- Systémové oblasti disku.
- Soubory při použití specifických aplikací (skripty).

Jsou známy případy, kdy novináři podávali informace o nových virech, které infikují jiné než výše zmíněné hostitele a to soubory typu JPEG a MP3. I když je virus součástí daného objektu, nemluví se o infikaci viru, ale připojení nepoužitelného kódu (tělo viru). Tělo viru má jinou strukturu kódu, než výše zmíněné typy formátů souboru. Při otevření či spuštění souboru tělo viru nevykonává žádnou nebezpečnou činnost a tato část považována za smetí. Z dalším důvodem, který potvrzuje danou hypotézu je, že datové formáty nejsou schopny pracovat s virem na binární úrovni.

Tím to se otevírá téma, jehož součástí je, diference mezi formátem souboru a jeho příponou. Formát je vnitřní struktura programu, která ovlivňuje kompatibilitu souboru se softwarem potřebným k jeho otevření. Přípona souboru slouží spíše informativnímu charakteru a nemusí odpovídat skutečnosti. Jsou známé případy, kdy je infikace proběhla u souboru s příponou „*.DAT“, která je zcela nezajímavá ze strany virů, ale to jen z důvodu,

že jeho vnitřní struktura odpovídá specifikaci formátu „*.EXE“ souboru. Podle typu hostitele a způsobů infekce lze viry rozdělovat do dalších skupin.

2.2 Makroviry

Jsou založené na podobné bázi replikace a připojení k souboru podobně jako viry, ale jsou mezi nimi diference. Makrovirus program nebo jen jeho část implantována do nějaké aplikace obdobného typu jako je Microsoft Word a je napsaný jeho vnitřním makrojazykem. Vyskytuje se vždy v rámci daného dokumentu. Pokud není jeho podporná aplikace ochráněna proti spuštění této hrozby, makrovirus nakazí veškeré dokumenty podpůrné aplikace. [1]

2.3 Trojské koně (Trojan)

Oproti virům tento škodlivý kód není schopen sebe-replikace a infekce souborů. Není to ovšem jeho účel. Trojský kůň byl v minulosti dar Řeků pro obyvatele města Tróji. Tento dar obsahoval jednotku vojáků, kteří otevřeli brány Tróje, poté město vyplenily. Funkce Trojského koně v počítačovém světě je stejná. Trojský kůň na první pohled působí dojmem obyčejného spustitelného souboru typu „*.EXE“, který v reálu obsahuje jen tělo tohoto škodlivého kódu. Odtud společně se skutečností, že Trojan (časté označení trojského koně) není připojen k žádnému hostiteli, plyne, že jedinou formou dezinfekce je odmazání dotyčného souboru. Starší definice říkají, že Trojan je program, vizuálně vypadající jako užitečný, ve skutečnosti však škodlivý.

Z historie této hrozby je znám případ, kdy se objevil trojský kůň, který se vydával za antivirový program McAfee VirusScan a který ve skutečnosti poškozoval veškeré datové vybavení hard disku. Na obdobné fázi byl založen Trojan pojmenovaný „Telefoon“, který se vydával za novou verzi oblíbeného komprimačního programu RAR 3.0, ještě před jeho skutečným uvedením na trh.

V současnosti se tak můžeme setkat nejčastěji s následující formou trojských koní:

2.3.1 Trojské koně typu Password-stealing (PWS)

Trojani tohoto typu obsahují funkci podobnou keyloggerů. Tedy zaznamenávají stisky kláves, které ukládají a posléze odesílají na požadované e-mailové schránky. Tento typ infiltrace je možné klasifikovat i jako spyware. Tyto trojské koně byli, často využívány ke konkurenčnímu zpravodajství.

2.3.2 Destruktivní trojské koně

Chování těchto druhů Trojanů je identické k výše zmíněnému starořeckému přirovnání. Tyto formy daného kódu při svém spuštění likvidují dostupné soubory na pevném disku nebo naplánuje a uskuteční kompletní formátování. Tito Trojani ve vysoké míře obsahují příponu „*.BAT“, které bývají složitě naprogramovány a jejich pravá funkce je dobře skryta i před zkušenými uživateli.

2.3.3 Dropper

Škodlivý kód, se vyskytuje nejčastěji jako spustitelný program s příponou EXE, který při svém spouštění umožňuje vstup do koncové stanice jiné součásti, které jsou vněm skryty před identifikací.

2.3.4 Downloader (TrojanDownloader)

Trojan downloader je na obdobné bázi jako jeho předchůdce, ale neobsahuje další škodlivý kód, který by vypustil do koncové stanice, nýbrž další malware stahuje z dostupných vnějších sítí. Pomocí pevně definovaných internetových adres (URL). Praxi nastávala situace, kdy různé skripty na straně serveru stahování upravily, že v nastávající situaci Trojani stahovali rozdílný software a při horší variantě stáhli více druhů škodlivého kódu. V důsledku to znamená, že v jeden nevinně vypadající soubor muže být branou pro vlnu vysokého počtu škodlivého kódu, který zpomalí koncovou stanici

2.4 Backdoor

Jde o aplikace typu klient-server, které umožňují obdobné činnosti, které moho zprostředkovat komerční produkty jako pcAnyWhere, VNC či Remote Administrator. Hlavním rozdílem mezi nimi je, že tyto aplikace působí anonymně a snaží se skrýt před běžnou ochranou operačního systému, která by uživatele před ním upozornila. Snaží se vyhnout detekci. Jedná se tedy o neautorizovaný vstup. Základní funkcí aplikace typu Backdoor je umožnění vzdáleného přístupu ke koncové stanici a aplikace sama osobě nemusí poškozovat běh operačního systému. Backdoor nebývá původce škody, ale umožňuje přístup jinému uživateli a je pouze na něm, jestli daného přístupu zneužije.

2.4.1 Princip Backooru

Pokud půjde o činnost škodlivou, pak tuto osobu nazýváme vzdáleným útočníkem. Princip fungování backdooru závisí na tom, že klientská část vysílá požadavky útočníkovi na jeho serverovou část, jež následovně tyto požadavky plní a popřípadě odesílá zpět klientu požadované informace. Z předchozího je zřejmé, že klientskou část aplikace by měl vlastnit útočník a serverová by měla být umístěna na počítači, kde lze očekávat kupříkladu důležitá data. Pokud je serverová část backdooru vypouštěna úspěšně se šířícím virem, má vzdálený útočník k dispozici tisíce počítačů, ke kterým může vzdáleně přistupovat. Celá komunikace probíhá ve většině případů na bázi TCP/IP, která ve spojení s celosvětovou sítí Internet umožňuje, aby útočník byl vzdálen tisíce kilometrů od serverové části backdooru. [1]

2.5 Červy

Červi jsou aplikace, které neprovádějí infikaci pomocí spustitelných souborů podobně jako viry, ale infikují systém přes síť kopírováním na připojené prvky sítě. Z tohoto důvodu způsobuje nevítané zatížení daných sítí a zahlcením pevného disku koncové stanice. Mezi další diferenci oproti virům patří skutečnost, že červ ke svému působení nevyžaduje další soubory (hostitele). Na platformách internetového protokolu TCP/IP a sítí WAN může uživatel nejčastěji narazit na hrozbu tohoto charakteru.

Červům podobné infiltrační škodlivé kódy jsou tzv. **bakterie** (bacterium) a **králíci** (rabbit). Oba tyto typy se shodují svým následným okopírováním po jejich spuštění. Baktérie

odesílá své kopie pouze do jiných systémů, které ještě nenakazila. Pohyb králíka představuje větší hrozbu. Králík nemá omezené cíle jako bakteria, ale napadá dostupné systémy. Těmto napadeným systémům pak odebírá čas procesoru a zabírá volný diskový prostor. [2]

2.6 Spyware

Aplikace typu Spyware využívá Internet k odesílání všech dat z koncové stanice uživatele, na které je naprogramován a to bez vědomí jeho uživatele. Tyto aplikace nenarušují chod operačního systému, ale záleží na útočníkovi, jak s těmito daty naloží. Od aplikací typu backdoor, který umožňuje přístup, spyware kopíruje po většinou jen informace a jiné se snaží vnutit. Phising a hoax jsem zde zařadil z důvodu snahy vylákat informace nebo zmást uživatele k jeho škodě.

2.6.1 Adware

Za aplikaci typu Adware jsou považovány druhy softwaru podporujícího nevyžádanou reklamní činnost. Aplikace přehrávají, zobrazují nebo stahují reklamy, bez chtěného vlivu uživatele, na koncovou stanici. Adware je považován za druh spywaru vzhledem k jeho tendencím narušovat soukromí uživatele.

2.6.2 Hijacker

Hijacker je označení pro škodlivý kód, který upravuje nastavení internetového prohlížeče. Mezi jeho známé nevítané funkce patří například změna domovské stránky dle nastavení útočníka. V horších případech může ovlivnit cookies.

2.6.3 Dialer

Spyware program Dialer ohrožuje jen některé typy uživatelů a to hlavně ty, kteří jsou vlastníky starších internetových připojení. Ohroženi jsou majitelé vytáčeného internetové připojení. Dialer totiž změní telefonní číslo, které vytáčí modem a pohyb uživatele po internetu muže být mnohem nákladnější.

2.6.4 Keylogger

Keyloggery jsou záznamová zařízení a mohou byt jak hardwarového tak i softwarového charakteru. Tyto aplikace zaznamenávají veškeré úhozy do klávesnice. Keyloggery se

využívají hlavně při konkurenčním zpravodajství, kdy mohou zaznamenat citlivé údaje. U běžných uživatelů je obzvláště nebezpečný při využívání internetového bankovnictví.

2.6.5 Hoax

Hoax je nevyžádaná zpráva, která uživatele varuje před určitou hrozbou, prosí o pomoc, informuje o nebezpečí nebo se snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele. Různé řetězové e-mail jsou příkladem hoaxu.

2.6.6 Phishing

Phising je technika sociálního inženýrství, která má za úkol vylákat od uživatelů citlivá data.

2.7 Spam

Slovem SPAM se označuje nevyžádaná reklamní pošta. Jsou to každý den miliardy zpráv, které rozesílá několik málo lidí, a které vám nabízejí služby nebo neexistující produkty. Dále se takto šíří nabídky různého nelegálního kopírovaného obsahu, např. Windows XP za 50USD. Za tuto cenu jde samozřejmě o nelegální kopii.

Tyto zprávy jsou škodlivé jednak tím, že zbytečně zahlcují síť a brzdí provoz, a také důvodem, že zahlcují jejich adresáty, kteří je musí mazat a ztrácí tím čas. Obrana proti SPAMu je dvojí. Preventivními kroky a metodou filtrování.

II. PRAKTICKÁ ČÁST

3 SOFTWAROVÉ ZABEZPEČENÍ PROTI VNĚJŠÍM HROZBÁM

Ve své praktické části se věnuji výběru vhodného softwarového řešení ochrany proti hrozbám, jímž jsem se věnoval v teoretické části. Tyto programy jsem selektoval na základě jejich snadné dostupnosti z internetu a jako další kritérium výběru jsem použil syntézu z velkých testů významných renomovaných webových portálů. Na základě studia testů jsem pečlivě vybral nejvhodnější kombinace softwarových řešení.

3.1 Druhy licencí softwaru

Nejprve se zaměřím na hlavní typy licencí softwaru, se kterými se běžný uživatel setká nejen na poli problematiky zabezpečení ale i na poli veškerého softwaru obecně.

3.1.1 Shareware

Programy typu shareware jsou zkušební verzi placeného softwaru. Obsahuje pouze omezené funkce a to jen po 30dní.

3.1.2 Trial

Trial verze nemají omezené funkce ale jen čas pro užívání daného softwaru. Zpravidla to bývá 30 dní. Po uplynutí této doby obvykle přestane fungovat. Pokud je uživatel spokojen, je mu nabídnuta možnost pro znovu aktivování programu, ale jen po zaplacení plné verze.

3.1.3 Public domain

Public domain jsou softwary, u kterého se jeho tvůrci dobrovolně vzdali svých autorských práv. Tyto programy lze legálně upravovat nebo volně šířit.

3.1.4 Demo

Funkčně omezená verze programu, nejčastěji se vyskytuje ve zkušební verzi her.

3.1.5 GPL

Jde o jinak pojmenovanou obdobu Public domain.

3.1.6 Opensource

Opensource programy jsou k dispozici většinou zdarma a díky přístupným zdrojovým kódům se vyskytuje možnost je dále upravovat.

3.1.7 Freeware

Používání těchto programů, které jsou k dostání zdarma, je v jiném znění než GPL nebo Public domain. Freeware se nemůže legálně využívat ke komerčním účelům.

3.1.8 Plná verze zdarma

Software je plné verzi zcela funkční a časově neomezený, nelze ho ovšem volně šířit. Veškeré komerční využití musí být v souladu s výrobcem. [20]

3.2 Antivirová ochrana

Tato část je věnována přehledu, který zprostředkovává elitu světově uznávaných antivirových řešení ochrany, které brání koncovou stanici před nebezpečím.

Internet je nevětší zdroj informací a škodlivých kódů současnosti. Pohyb po internetu se v dnešní době neobejde bez patřičné ochrany. Windows XP ani Vista tuto ochranu neobsahují, z tohoto důvodu vzniká potřeba se proti hrozbám chránit cestou antivirové ochrany. Podle statistik se každý den objeví průměrně deset nových počítačových virů anebo jiných škodlivých kódů. Škody, které tyto útoky způsobují, jsou vyčísleny často ve velmi vysokých částkách a jistotu před nimi nemůže mít žádná skupina uživatelů.

Mezi potřebné standardy kvalitního antiviru patří:

- jednoduchá instalace a použití,
- rezidentní štít
- ochrana počítače proti počítačovým virům a červům
- jednoduché uživatelské rozhraní
- virová truhla
- kontrola e-mailů
- rychlá ochrana proti virovým epidemiím
- automatická aktualizace virových definic

Nyní se zaměřím na konkrétní software poskytované zdarma.

3.2.1 Avast! 4.7 Home – freeware

Jeden ze dvou předních českých antivirových systémů, který je ve verzi pro domácí užívání zcela zdarma. Umožňuje hledat známé počítačové viry, trojské koně, vytvářet a kontrolovat databázi integrity, spouštěné i ukládané programy, otevírané dokumenty a elektronickou poštu. Produkt je pro domácí nekomerční použití zdarma. Po instalaci nebo do několika dnů je nutné pro trvalé použití zdarma provést registraci.

Hlavní funkce:

- Rezidentní ochrana - kontrola emailového klienta, sledování scriptů v prohlížečích (verze Pro), kontrola používaných souborů
- Antivirová kontrola před plným nastartováním systému
- Seznam známých virů
- Automatická aktualizace virové databáze

3.2.2 AVG 7.5 – freeware

AVG je kompletní antivirový systém vytvořený českou firmou Grisoft. Daný software umožňuje scan virů na vyžádání, rezidentní štít aplikací v běhu a uložených programů, souborů a také scan došlé i odesílané elektronické pošty. Minimální systémové požadavky CPU Intel Pentium, 300 MHz, 70 MB volného místa na HDD, 64 MB RAM. Neobsahuje možnost aktualizace a stahování virových definic neoplývá vysokou rychlostí a neobsahuje českou lokalizaci.

3.2.3 ESET NOD32 Antivirus 4.0.474 - trial

Pokud jde o reputaci, ESET NOD32 je prakticky nenapadnutelný. Verze 4 je efektivní antivirová a antispywarová ochrana s důrazem na funkci ThreatSense, která útoky odhaluje dříve, než dojde k větší infikaci. Obsahuje úhledné rozhraní a eden z nejlépe hodnocených testů věnovaným detekci. NOD32 netrpí detekcí falešných poplachů. Bohužel se vyskytuje pouze v časově omezené verzi

3.2.4 TrustPort Workstation 1.4 - trial

Další český zástupce antivirové ochrany TrustPort Workstation, má ve svém obsahu dokonce firewallovou, antispamovou a antispywarovou ochranu. Celkový balík aplikací řešící výše zmíněné hrozby. Určen jen pro použití na koncové stanice. Novátorskou a vítanou funkcí je také elektronická skartovačka dat. Vítaná je také možnost výběru využívat jeden nebo více antivirových motorů. Tento program obsahuje vysoký počet funkcí, které neobsahují chyby, ale s porovnáním s ostatními jejich kvalit není příliš vysoká.

3.2.5 AntiVir PersonalEdition Classic 7.06 - freeware

Německý software AntiVir patří antivirou ochranu, která si již vypracoval vysokou oblibu. Prokazatelně již dosahuje kvalitních výsledků na poli řešení ochrany počítačů s operačními systémy Windows před viry, červy, trojskými koni a jiným nebezpečím. Hned nainstalování provádí scan počítače na možnost detekce škodlivého kódu. Obsahuje také žádanou rezidentní ochranu, která kontroluje chod operačním systémem. Bohužel chybí česká lokalizace.

3.2.6 ClamAV For Windows 0.9 – open source

Open source antivirový systém pro Windows. Daný program využívá ke svému ovládání příkazový řádek. Jeho funkce jsou rychlé a výkonné a jednoduše se integruje do aplikací na serverech. Z důvodu typu jeho ovládání není příliš vhodný pro nezkušené uživatele.

3.2.7 BitDefender Free Edition 10 – freeware

BitDefender Free Edition přináší šanci používat jeden z antivirových motorů zdarma. Umožňuje spokojeně užít základní ochranu proti virům a to bez dodatečných nákladů. Tato verze bohužel neobsahuje rezidentní štít. Pro nepřetržité připojeni k internetu, se doporučuje spíše zvážit více komplexní antivirové řešení. Avšak placená verze nabízí nejen tuto funkci, ale ještě daleko více.

3.2.8 PC Tools AntiVirus Free Edition 3.6 - freeware

Je to balíček bezpečnostního řešení, který obsahuje definice virů, červů a trojských koňů. Neobsahuje však nutnou rezidentní ochranu. Umožňuje provádět scan operačního systému a následné léčení souborů infikovaných škodlivým kódem.

3.2.9 ClamWin Portable 0.91 - freeware

Tento nástroj je nejen zdarma dostupný, ale jeho hlavní výhodou je jeho portable řešení kdy ho lze používat na přenosovém mediu. ClamWin Portable je verze výše zmíněného, stejnojmenného, antivirového řešení ochrany, které nevyžaduje přímou instalaci do operačního systému Windows. [6]

3.3 Firewall

Firewall je aplikace, jejímž úkolem kontrolovat komunikaci mezi lokální sítí (LAN) a externími sítěmi (WAN). Jedná se o síťové zařízení, které má za úkol zabezpečit chod řízení mezi síťové komunikace udržením různé úrovně důvěryhodnosti. Firewall definuje soubor pravidel, která slouží jako místo mezi sítěmi ovlivňující blokaci či povolení aplikace s vnějším světem a odděluje je. Také podává informace o legálních procesech, vznikajících při použití uživatelské aplikace a měl by tyto činnosti povolit či zakázat a dané rozhodnutí uložit pro stejné případy. Firewall v historii zahrnoval identifikaci zdroje a místo určení dat (zdrojovou a cílovou IP adresu), ale v dnešní době je tato funkce nedostatečná. Bez znalostí protokolů o spojení a prvků IDS firewall není možné považovat za kvalitní. [4]

3.3.1 ZoneAlarm freeware

ZoneAlarm freeware je základní verze známého firewallu.Tato bezplatná verze nabízí kvalitní a spolehlivou ochranu a řízení síťových procesů. ZoneAlarm nabízí možnost upravení pravidel, která si uživatel může upravit průběhu jiných interakcí mezi sítěmi.

V plné verzi ZoneAlarm nabízí balík bezpečnostních ochrany, které obsahují například i antispamový filtr e-mailů, rodičovský zámek (filtrování stránek otevíraných na internetu),

antivir nebo ochranu před odcizením identity uživatele, což patří do nečasto viděným funkcím.

3.3.2 Outpost Firewall freeware

Outpost Firewall patří mezi oblíbené freeware firewally. Tato aplikace je známá svoji snadnou ovladatelností i pro méně zkušené uživatele, která spolehlivě udržuje potřebnou míru bezpečnosti pro koncovou stanici, před útočníky, nebezpečnými programy a únikem soukromích dat. Outpost Firewall také umožňuje webovou filtraci prohlížených stránek.

Obdobně je zde možnost upgradování na plnou verzí komerčního programu, který obsahuje mnoho dalších funkcí pro zabezpečení koncové stanice.

3.3.3 Jetico Personal Firewall

Jetico Personal Firewall poskytuje koncové stanic, až třístupňovou ochranu před nebezpečným chováním programů z dostupných sítí. Firewall umožňuje udržovat koncovou stanici ve stealth módu, při kterém se u připojení k potenciálně nebezpečným sítím stává koncová stanice neviditelnou. Obsahuje i klasické funkce kontroly komunikace a instalace programů spojenou internetem. Dokáže a ochránit před trojskými koňmi a obdobným nechtěným softwarem.

Také v případě Jetico Personal Firewallu je možnost zakoupit plnou placená verzi s přidanými funkcemi, které rozšiřují daný produkt.

3.3.4 SoftPerfect Personal Firewall

Podrobné definice pravidel pro síťové komunikace zprostředkovává firewall SoftPerfect Personal Firewall. Poskytuje také možnost nastavení samostatné konfigurace pro variabilní síťové adaptéry. Obsahuje soubor přednastavených pravidel filtrování a i tento soubor se dá upravit nastavením uživatele. Aplikace tuto úpravu řeší pomocí pop-up oken při adekvátní situaci.Není ovšem příliš vhodný pro začátečníky.

3.3.5 Comodo Firewall Pro

Firewall nabízí detailní nastavení a informace o aplikacích přistupujících k síti. Program umožňuje definovat nastavení ke každé aplikaci zvlášť, obvykle pomocí pop-up okna v okamžiku, kdy se aplikace pokouší připojit k internetu. Zvolit lze i takzvaný „mód pro učení“, kdy se firewall „učí“, které aplikace má považovat za bezpečné nebo které má zakázat. Comodo Firewall dále chrání počítač nejen před napadením hackery, ale i před Trojany, spywarem a dalšími nebezpečnými programy i kódy. Součástí programu je i rozsáhlá databáze aplikací sloužící k analýze bezpečnostních rizik.

Comodo Firewall Pro je k použití zdarma, po instalaci jej stačí bezplatně zaregistrovat. [13] [14] [15]

3.4 Antispyware

Antispyware software je navržen pro ochranu koncové stanice a jejího obsahu proti hrozbám typu spyware a adware. Nevědomky do systému nainstalovaných škodlivých kódů, které zobrazují nevyžádané reklamy, shromažďují osobní údaje, nebo dokonce přebírající kontrolu systému pro nelegální účely se vyskytuje celá řada. Existuje mnoho antispyware dostupných aplikací, některé jsou zdarma.

3.4.1 Ad-Aware Anniversary Edition 8

Tento program je dostupný v licenci freeware a umožňuje odhalovat nejčastější spyware programy. Ad-Aware je populární lovec reklamy a spywaru. Ve své výroční edici, která oslavuje deset let výrobce v této branži, nabízí nový vzhled, ovládání i řadu nových funkcí:

- Behavior-based heuristical detection
- Ad-Watch Live!
- Integrace s bezpečnostními prvky Windows.

Nová verze 2008 přináší znatelné zrychlení kontroly disku a menší spotřebu systémových prostředků u komponenty Ad-watch.

3.4.2 IObit Security 360

Daný software odstraňuje z koncové stanice hrozby v typu spyware, adware, trojanů, keyloggerů, červů atd. Obsahuje jedinečný dvou jádrový snímač a heuristickou detekcí malware. IObit Security 360 se dokáže vypořádat s většinu komplikovaných spywarů a malwarů a nedlouhou dobu.

IObit Security 360 obsahuje ochranu v reálném čase a rychlou automatickou aktualizaci pro udžení připravenosti proti aktuálním bezpečnostním hrozbám. Program je dostupný ve dvou kvalitativně i cenově rozdílných verzích. Pro tuto práci zajímavá zdarma freeware verze pro nekomerční užití, která neobsahuje automatické aktualizace a ani technickou podporu.

3.4.3 Malwarebytes Anti-Malware

Tento program je určen zejména pro scannování obsahu koncové stanice. Jedná se o účinný nástroj na vyhledávání (rychlé i kompletní), a při případné detekci a odstranění malwaru z koncové stanice.

Program se specialně zaměřuje na jednotlivé procesy, které probíhají v systému a v momentě detekce podezřelých souborů okamžitě proces zastaví. Snadná obsluha spolu s pěkně zpracovaným grafickým rozhraním znamená plus pro začátečníky.

Malwarebytes Anti-Malware vám ji poskytuje adekvátně sebevědomou detekci.

3.4.4 Spybot - Search & Destroy

Program kontroluje systém proti komplexní databázi adware a jiným systémovým útočníkům. Je zde také několik vylepšení, včetně několika skinů pro jeho vzhled. Výsledky testů se zobrazí uspořádané skupiny ve stromové struktuře a umožňuje okamžité zobrazení informací o vybrané položce, které pomohou se rozhodnout, zda nález odstranit nebo ne. Mezi další užitečné nástroje, včetně zabezpečení Shredder, patří funkce absolutní odstranění souboru. Vedle této základní skupiny funkcí Spybot chrání i proti dialerům, přesměrovávajícím modemové připojení přes drahé linky, trojským koním, keyloggerům a mnoha dalším nebezpečím.

Samozřejmostí je možnost aktualizace přes Internet. Program obsahuje i českou lokalizaci základního menu a ovládání. Neobsahuje rezidentní štít.

3.4.5 SpywareBlaster

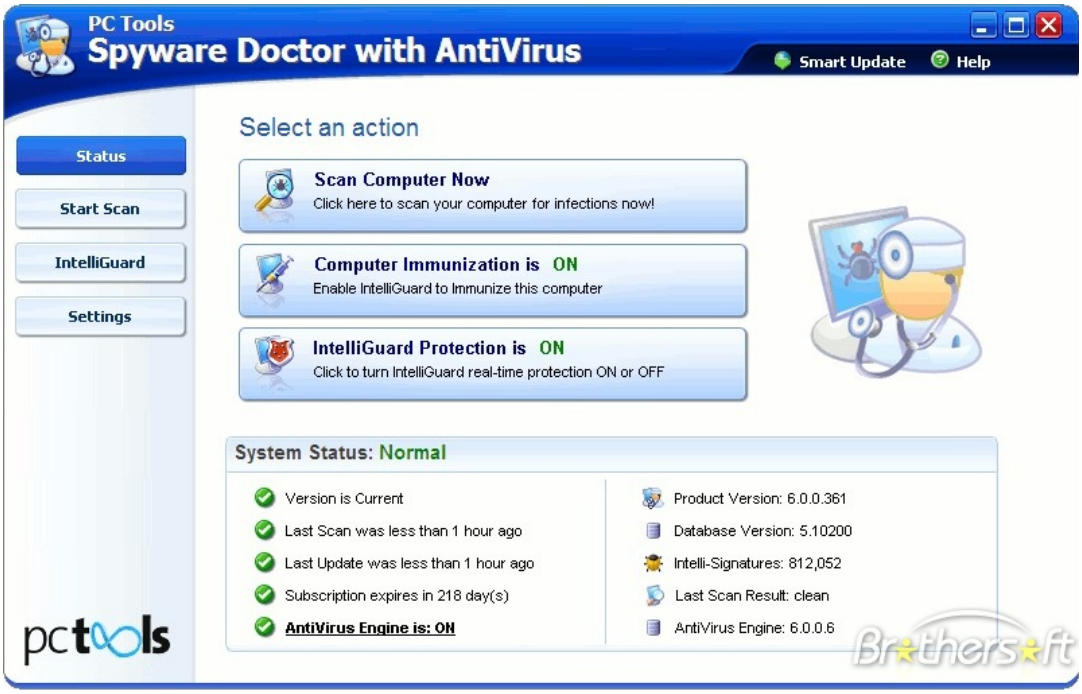
SpywareBlaster nepatří mezi klasické anti-spyware programy. Jeho hlavní funkce není založena na scannu koncové stanice a následném odstranění nalezeného spywaru. SpywareBlaster zabraňuje nežádoucím programům v instalaci na váš počítač. Daný software obsahuje i možnost nastavení, před jakou hrozbou typu spyware se uživatel potřebuje chránit.

Užitečnou funkcí je tzv. „System Snapshot“, která vytvoří bod obnovy v čistém stavu. Samozřejmostí je i automatická aktualizace, která udržuje SpywareBlaster v připravené podobě.

3.4.6 Spyware Doctor Starter Edition

Účinný nástroj určený pro hledání a odstraňování škodlivých kódů, jakými jsou spyware, adware, trojské koně, keyloggery, viry typu hijacker, či další škodlivé a jinak nebezpečné hrozby, mezi něž patří phishing, popup okna, apod. Aplikace pochází od společnosti PC Tools.

Spyware Doctor disponuje trojcestnou ochranu před spywarem, dokáže systém imunizovat a chrání jej v reálném čase. Neregistrovaná verze programu, oproti plné variantě, nedisponuje možností online aktualizací bezpečnostních databází. Placená verze naopak nabízí všechny update a opravy po dobu jednoho roku v ceně. Spyware Doctor je zdarma dostupný také ve verzi Starter Edition jako součást softwarového balíku Google Pack. Spyware Doctor získal v minulosti řadu prestižních ocenění v mnoha zemích světa. Z nich lze jmenovat vítězství v People's Choice Award v letech 2005, 2006 a 2007.



Obrázek 1 Ukázka uživatelského prostředí [10]

3.4.7 Spyware Terminator

Spyware Terminator je jedním z velmi oblíbených programů tohoto typu.

Aplikace dokáže kvalitně reagovat na hrozby typu spyware, hijacker, trojský kůň či keylogger. Kontrola běhu procesů je zde prováděna rezidentním štítem. Tato funkce je doplněna Různě nastavitelným scannem koncové stanice

Rozsáhlá databáze škůdců je obsahem dané aplikace a umožňuje uživateli podrobnější informace než u konkurence. Nalezené škudce aplikace může přesunout do ignorovaných, smazat anebo odsunout do karantény

V případě potíží můžete využít možnosti zálohy, před odstraněním nebezpečného softwaru.

3.4.8 SuperAntiSpyware Free Edition

SUPERAntiSpyware umožnuje scan koncové stanice a reaguje na výskyt známých a nebezpečných aplikací typu Spyware, Adware, Malware, Trojans, Dialers, Worms, KeyLoggers, HiJacker atd. Vytváří možnosti práce se těmito hrozbami podobně jako Spyware Terminator. Obsahuje zabezpečení domovské stránky.

Nastavitelné parametry scanu ovlivní velkou vahou rychlost a účinnost daného scannování Aplikace disponuje i opravnými funkcemi, do kterých patří funkce oprava vytvořené škody, které byla způsobená nebezpečné aplikace.

Free verze postrádá rezidentní štít, který vás chrání v reálném čase a pár dalších pokročilých funkcí. [3]

4 TESTOVÁNÍ NEJVHODNĚJŠÍ SADY PROGRAMŮ

V této kapitole jsem se věnoval testování vybrané sady, s odůvodněním daného výběru, bezpečnostního software na výše zmíněné hrozby. Zaměřím se na detailní popis jejich funkcí a následně tyto funkce otestuji ve virtuální prostředí Sun VirtualBox.

Výběr bezpečnostního softwaru:

- Antivir **Avast 4.7 Home**
    - Tento program jsem vybral, z důvodů požadavků této práce. Měl nejlepší webové reference mezi freeware antiviry. Antivir NOD32 obsahuje lepší kvality, ale je k dostání pouze jako trial vision,což se pro mou práci nehodí.
- Firewall **Comodo Internet Security 4.0**
    - Firewall Comodo jsem vybral na základě webových testů.[13]
- **Spyware Terminator**
    - Vybral jsem tento program na základě šíře jeho poskytovaných služeb a možností, které ostatní programy ve verzi freeware nepodporovaly.[14]

4.1 Testovací souprava

Pro otestování dané sady programů jsem použil virtuální prostředí Sun VirtualBox 3.1 a v něm jsem danou sadu otestoval na operačních systémech Windows XP SP3. [16]

Windows XP jsem vybral místo Windows Vista, z důvodů nepříliš doladěných prvků chodu systému a ochrany. V době kdy jsem měl zvolit jednu ze dvou zmíněných variant, byl dostupný pro Visty jen Service pack 1. Ten vykazoval problémy s kompatibilitou Hardwaru a nemalí počet dalších chyb. Ve výsledku Windows XP SP3 je stabilnější proto jsem ho zvolil pro dané testování.

Hardwarová sestava byla ovlivněna nastavením virtuálního prostředí. Vybrané nastavení virtuálního prostředí je:

Tabulka 1: Popis hardwarového prostředí

Operačního sytému	**Windows XP SP3**
Operační paměť	512MB
Procesor	1.6 Ghz
Video paměť	16 MB
3D/2D Akcelerace	vypnuta
Síťová karta	PCnet-FAST III (NAT)

4.2 Test Avast 4.5 Home

Program obsahuje možnost jednouché instalace pro začátečníky s možností implicitní nastavení ochrany od Alwil Softwaru (výrobce), kterou jsem použil testu. [11]

Avast v této verzi nabízí funkce:

- **Testování Počítače:**
  - obsahuje možnosti scannů, které jsou rozdělené dle poměru důkladnosti a časové náročnosti.
- **Rezidentní štít**
  - Obsahuje 7 typů rezidentních štítů, u kterých lze pozorovat pomocí grafů jejich chování a reakce.
- **Údržba programu**
  - Obsahuje možnosti aktualizace programu jádra s virovou databází, virovou truhlu.

V testu sem jsem se zaměřil na ochranu tvořenou rezidentními štíty. Testoval jsem je pomoci virů z webové adresy http://biohazard.xz.cz/biohazard.html.

4.2.1 Průběh testu:

1. Stáhl jsem z daného zdroje soubor, který byl zabalen ve formátu .ZIP a obsahoval 130 virů.
2. Webový rezidentní štít zareagoval na tento soubor již v zabaleném stádiu. Pro možnost dalšího testu jsem byl nucen tento štít vypnout.

Obrázek 2: Ukázka webového štítu Avast

3. Soubor jsem rozbalil pomocí implicitních nástrojů Windows XP.
4. Při procesu rozbalování Antivirus zareagoval na škodlivý obsah a přesunul ho virového trezoru.

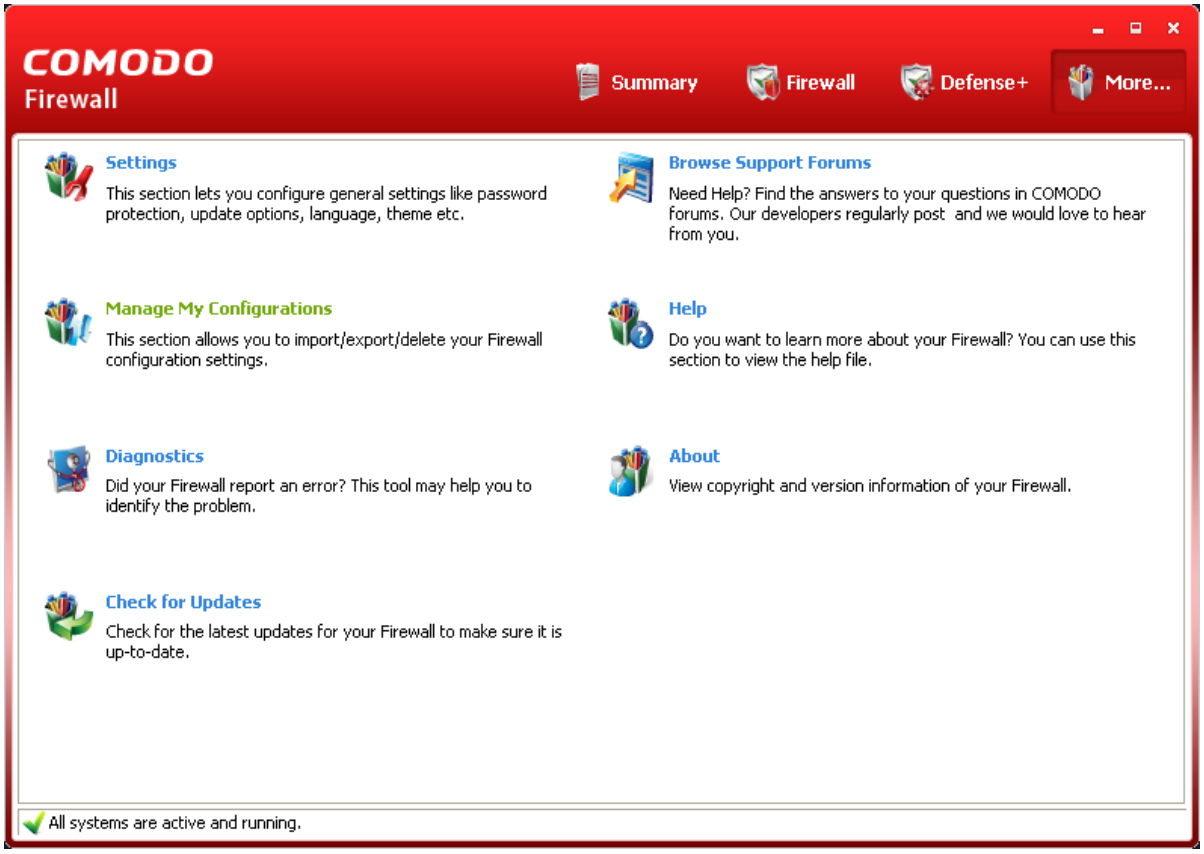
Obrázek 3: Ukázka Souborového štítu Avast

5. Následné scannování prokázalo, že systém nebyl napaden škodlivým kódem.

Obrázek 4: Výsledný scan Avast

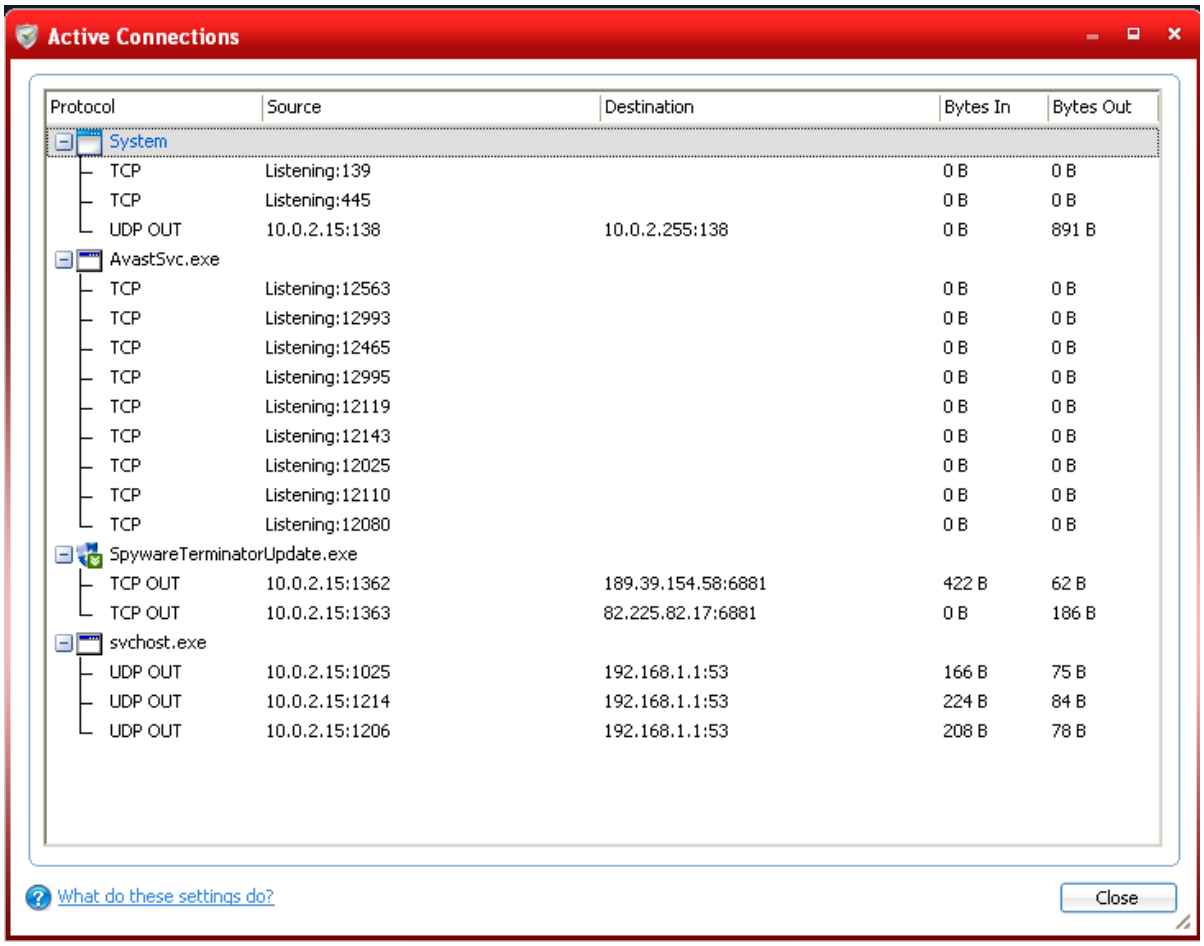
4.3 Comodo internet security 4.0

Firewall comodo jsem vybral na základě webových referencí. Tento program si zajistil velkou oblibu za dobu svého působení. [13]



Obrázek 5: Uživatelské rozhraní Comodo

Volil jsem jednoduchou instalaci, která vychází z implicitního nastavení výrobce. Vyskytuje se zde dále možnost doladění nastavení pravidel firewallu. Při každé interakci s vnější sítí jsem obdržel výzvu, v podobě pop-up okna, povolit či zakázat komunikaci daného programu s jiným prvkem z jiné sítě. Mezi zajímavé funkce patří aktivních spojení. Mezi nevýhody patří snad jen nečeská lokalizace.



Obrázek 6: Výčet aktivních připojení

4.4 Spyware Terminator

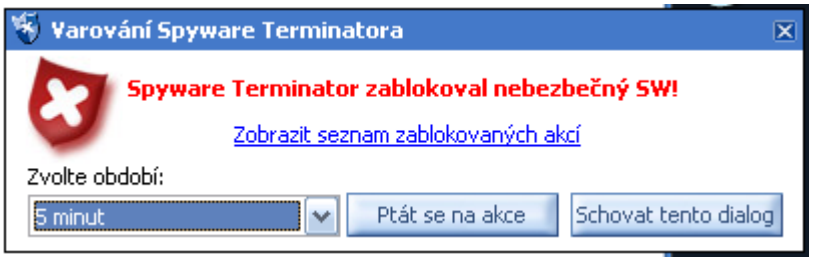
Tento program patří ke špičce v oblasti freeware pro detekci spywaru. Spyware Terminator v sobě obsahuje detekční modul a rezidentní štít, který chrání počítač na pozadí, a tím online zamezuje infiltraci škodlivého kódu. Jeho test je založen na obdobném základu, jako předchozí test antiviru. Pro škodlivý kód jsem použil testovací spyware ze zdroje „http://spycar.org/Spycar.html“.

Spyware terminator obsahuje:

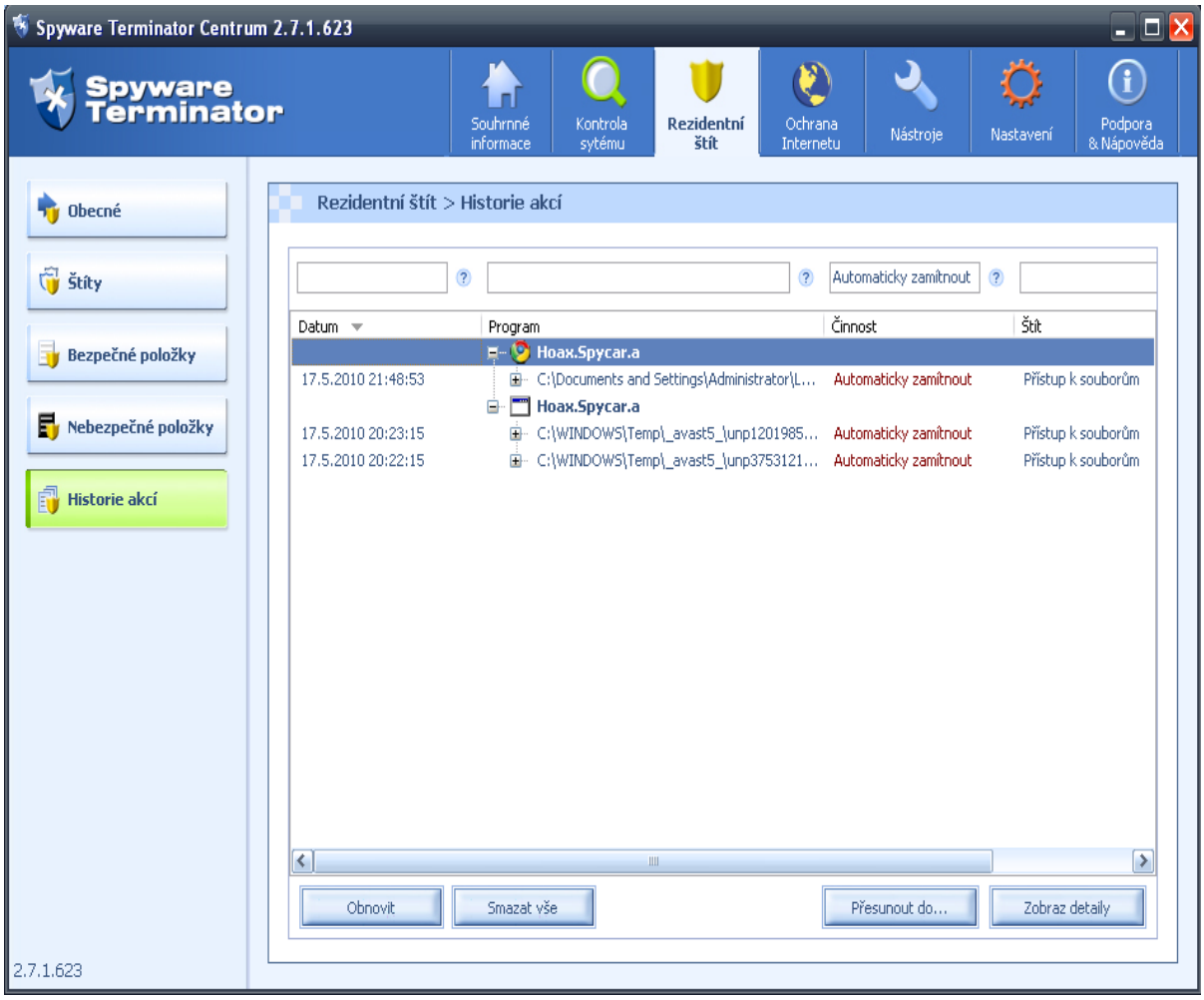
- **Kontrola systému:**
  - Nabízí rychlou, kompletní a nastavitelnou kontrolu
- **Rezidentní štít**
  - V jeho obsahu se nachází 8 typů obranných štítů a historii jejich akcí na nalezené soubory.
- **Ochrana internetu**
  - Kontrolu cookies a oblíbených webů v internetovém prohlížeči
- **Nástroje**
  - Tato položka obsahuje systémové nastavení, obnovu systému, analýzu souboru a odstranění souborů s jeho registry

4.4.1 Průběh testu:

1. Stáhl jsem z výše zmíněné stránky spyware
2. Rezidentní štít zastavil stahování. V pop-up oknu se nabízely možnosti pro řešení a odkaz na seznam nalezeného spywaru. Pro otestování scannu jsem rezidentní štít vypnul.

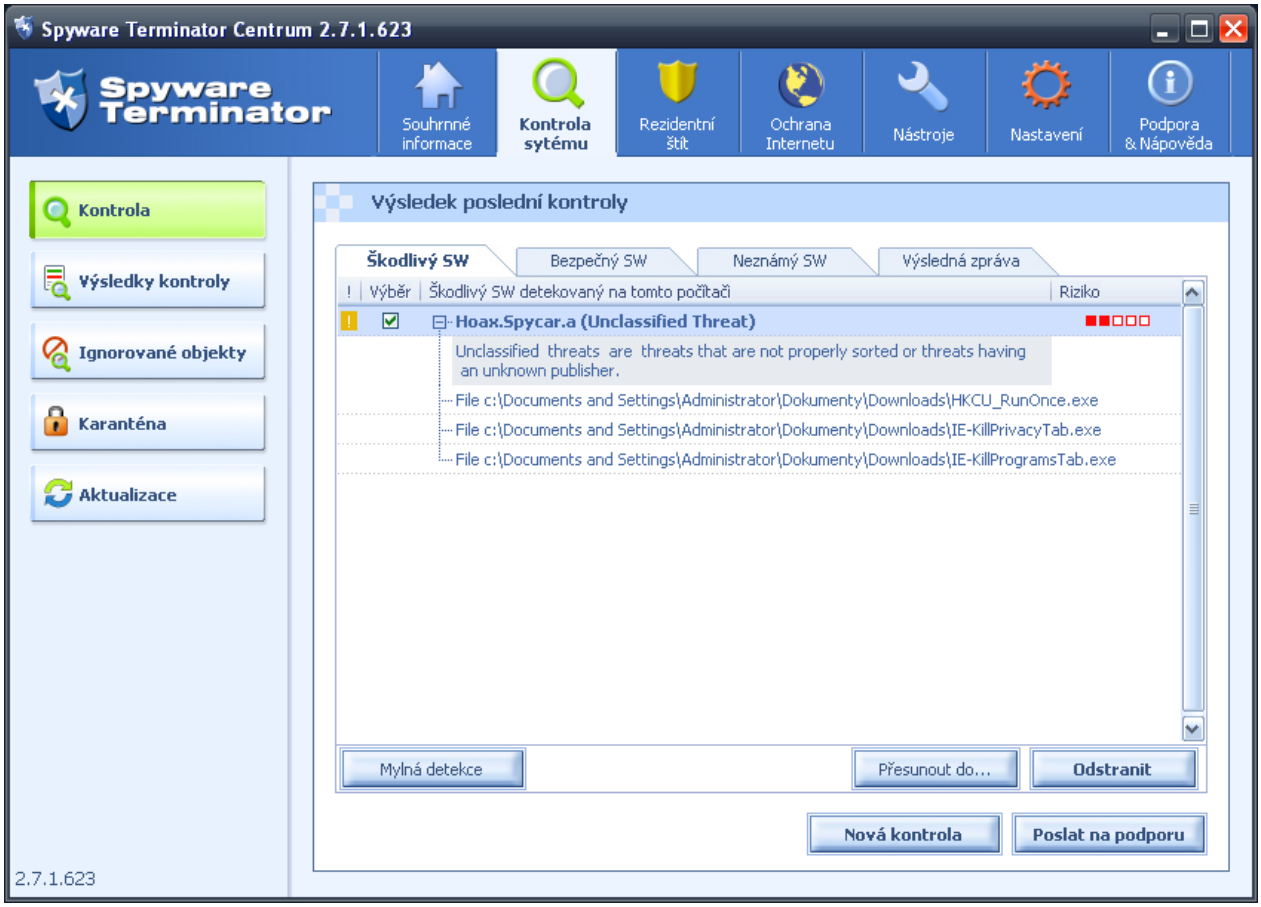


Obrázek 7: Pop-up okno Spyware terminator



Obrázek 8: Historie zaznamenané hrozby

3. Rychlá kontrola prohledávala pouze cookies a hrozbu nenašla.
4. Kompletní scan hrozbu vyhledal a nabídl její vymazání.



Obrázek 9: Výsledek scannu Spyware terminator

ZÁVĚR

Ve své bakalářské práci, psané na téma "Zabezpečení operačního systému Windows", jsem se věnoval rozboru nejvhodnějších bezpečnostních softwarových nástrojů, určených pro optimální zabezpečení vhodné pro operační systémy Windows XP a Windows Vista.

V první kapitole teoretické části jsem rozebral problematiku výchozího zabezpečení operačních systémů Windows XP a Windows Vista. Důraz jsem přikládal na vývoj bezpečnostního obsahu u jednotlivých servisních balíčků (service packs). Poukázal jsem na bezpečnostní slabiny operačních systému, které je třeba řešit vhodným výběrem bezpečnostních nástrojů a to z důvodu, že Windows postrádají konkurence-schopné vlastní nástroje ochrany proti dnešním hrozbám internetu.

V druhé kapitole teoretické části jsem se věnoval bezpečnostním hrozbám, ohrožující operační systémy Windows XP a Windows Vista. Zaměřil jsem se zejména na hrozby nejčastěji dostupné z vnějších sítí (internet). Tyto hrozby jsem rozdělil podle druhů a popsal, v čem spočívá jejich největší nebezpečí pro systém a uživatele.

V první kapitole praktické části jsem zpracoval rešerši bezpečnostních nástrojů, která obsahovala bezpečnostní programy poskytované zdarma, a jež byly v renomovaných počítačových periodikách a internetových portálech nejlépe hodnoceny. Souhrn bezpečnostních nástrojů poskytovaných zdarma jsem tematicky rozdělil na antivirovou, antispywarovou a firewallovou ochranu.

Ve druhé kapitole praktické části jsem otestoval vybrané kombinace bezpečnostních nástrojů před reálnými hrozbami. Testování jsem prováděl ve virtuálním prostředí VirtualBox. Z operačních systémů jsem si vybral Windows XP Service Pack 3, který byl lépe ohodnocen než novější operační systém Windows Vista SP1 a to jak z hlediska bezpečnosti, tak z hlediska stability systému.

Pro antivirové řešení problému jsem vybral Avast 4.5 Home a to především z důvodů, že žádný program, který by splňoval licenční požadavky, nedosahoval takové kvality a funkce. Dále jsem tento program podrobil testování na jeho reakci vůči různým škodlivých kódů, které jsem ziskal z webových stránek Biohazard. Otestoval jsem všechny jeho funkce. Test ukázal, že program odhalí korektně všechny testované viry a zabrání jejich dalšímu šíření včas.

Obdobný postup jsem zvolil u testování antispywarové ochrany Spyware terminátor. Tento program také jako jediný splňoval dané požadavky na kvalitu a typ licence. Test probíhal pomocí infikace spyware z webových stránek Spycar. Reakce programu splnily bezpečnostní požadavky. Aplikace hrozbu označila a zabránila ji v činnosti, která by ohrožovala uživatele. Spyware terminator splnil očekávané požadavky.

Poslední ze třetice ochranných prvků je program Comodo internet security. Daný firewall jsem doporučil na základě nejlepších výsledku v testu webového portálu Matousec, který hodnotil víc jak 18 známých firewallů.

Jako vhodnou kombinaci bezpečnostních nástrojů poskytovaných uživateli zdarma pro zabezpečení na testovaném operačním systému Windows XP Service Pack 3, doporučuji antivirovou ochranou Avast.4.5 Home, firewall Comodo internet security 4.0 a antispyware ochranu Spyware terminátor

Výsledné poznatky mají za úkol poučit a posléze navést na stabilní řešení zabezpečení operačního systému, především z pohledu nepříliš zkušeného uživatele, který danou sadu nebude využívat pro komerční účely ale pro účely soukromého použití.

Přínosem této práce je výše doporučená sada programů poskytovaných uživateli zcela zdarma a poskytujících komplexní ochranu proti počítačovým hrozbám.

ZÁVĚR V ANGLIČTINĚ

In his thesis, written on the theme Windows Security Protection, I worked to find the best security software tools, designed for optimum security suitable for Windows XP and Windows Vista.

In chapter one, I disassembled the security problems starting Windows XP and Windows Vista. The emphasis was attributed to the development of the security content of individual service packages (service packs). I pointed out security weaknesses in operating systems, which are not capable or do not have enough protection level against Internet threats today.

In the second chapter one I worked on security threats, threatening operating systems Windows XP and Windows Vista. I focused in particular on the most common threats available from the external network (internet). These threats are divided into types I and described in what is their biggest threat to the system and users.

In the third chapter of the practical part I have compiled a search of security tools, which include security software available free of charge, which was renowned in the computer magazines and portals of the best studied. Summary of the security tools provided for free, I thematically divided into antivirus, antispyware and firewall protection.

The fourth chapter the practical part will include testing of a chosen combination of security tools against real threats. I was doing testing in a virtual environment VirtualBox. The operating system I chose Windows XP SP3, which was rated as better in the field of security and stability in the field of system than the newer Windows Vista SP1.

For anti-virus solution to the problem I chose Avast Home 4.5, and for reasons that no program that would meet the licensing requirements did not reach such quality and function. Then I tested the program's response to various packages of malicious codes, which I got from Biohazard website. I tested all its functions. The test showed how the program responds to the challenges and threats to reveal all the time.

I chose a similar approach in testing antispyware protection Spyware Terminator. This program is the only meet the requirements for the quality and type of license. The test was carried out with the infection of spyware websites Spycar. Response program meet safety requirements, applications and threats were called in by avoiding activities that would compromise the user. Spyware Terminator has fulfilled the expected requirements.

Thirdly, the last of the security features of the program is Comodo Internet Security. The firewall, I recommend the best test scores Matousec web portal, which reviewed more than 18 well-known firewalls.

Providing a definitive solution includes Windows XP Service Pack 3 with all available updates, antivirus home Avast.4.5, firewall, Comodo Internet Security 4.0 Spyware Terminator antispyware.

Resulting knowledge to the task of learning and then navigate to a stable operating system security solution, especially in view of very experienced users who will use the suite for commercial purposes. In this regard, this freeware licenses do not support the contribution of this work is a set of recommended programs.

SEZNAM POUŽITÉ LITERATURY

Monografie

[1] BOTT, Ed; SIECHERT, Carl. *Zabezpečení Microsoft Windows 2000 a XP*. 28. dubna 48, 635 00, Brno : Computer Press , 2004. Ochrana vašeho osobního počítače, s. 310. ISBN 80-722-6878-3.

[2] HEINIGE, Karel. *PCWorld Edition – Viry a počítače*. Jundrovská 33, 624 00 Brno: UNIS Publishing, s.r.o., 2001. Červi podrobněji, s. 15-18. ISBN 80-86097-74-9.

Elektronické zdroje

[3] *Antivir Info* [online]. 30. 7. 2009 [cit. 2010-05-13]. Antispywary. Dostupné z WWW: <http://antivir.czweb.org/antispywary.html>.

[4] *A plus KB* [online]. 3. 3. 2010 [cit. 2010-05-13]. How to choose a Firewall. Dostupné z WWW: <http://www.apluskb.com/scripts/How_to_choose_a_Firewall_answer187.html>.

[5] *Biohazard.xz* [online]. 2009 [cit. 2010-05-17]. Cryogenic room. Dostupné z WWW: <http://biohazard.xz.cz/biohazard.html>

[6] DVOŘÁK, Jakub. Technet.cz [online]. 6. 11. 2007 [cit. 2010-04-26]. Vybrali jsme pro vás 10 antivirových programů zdarma. Dostupné z WWW: <http://technet.idnes.cz/vybrali-jsme-pro-vas-10-antivirovych-programu-zdarma-f9d-/software.asp?c=A071015_203549_software_dvr>.

[7] ČERNÝ, Jiří. Bezpečnost: XP vs. Vista (1). *Svět Hardware* [online]. 5. 5. 2009, [cit. 2010-04-03]. Dostupný z WWW: <http://www.svethardware.cz/art_doc-3074ABA1B7108B46C12575A4005B707C.html>.

[8] ČERNÝ, Jiří. Bezpečnost: XP vs. Vista (2). *Svět Hardware* [online]. 24. 6. 2009, [cit. 2010-04-06]. Dostupný z WWW: <http://www.svethardware.cz/art_doc-B608BE750336C031C12575DC003B998B.html>.

[9] HÁK, Igor. Moderní počítačové viry.[online]. 15.9.2005, [cit. 2010-05-18]. Dostupný z WWW: <http://viry.cz/viry.cz/kniha/kniha.pdf>.

[10] Dostupné z WWW: <http://www.brothersoft.com/spyware-doctor-starter-edition-166039.html&usg=__6Hnhxbms0iTC0UI9X-JZ6AaD-9M=&h=509&w=800&sz=130&hl=cs&start=1&um=1&itbs=1&tbnid=68dy0CQw_rJClM:&tbnh=91&tbnw=143&prev=/images%3Fq%3DSpyware%2BDoctor%2BStarter%2BEdition%26um%3D1%26hl%3Dcs%26sa%3DN%26tbs%3Disch:1>

[11] Dostupné z WWW:<http://www.filehippo.com/download_avast_antivirus/27/>

[12] JURÁSEK, Vít. Novinky v zabezpečení Windows XP Service Pack 2, 2. část. *Živě.cz* [online]. 11. 8. 2004, 1, [cit. 2010-04-21]. Dostupný z WWW: http://www.zive.cz/clanky/novinky-v-zabezpeceni-windows-xp-service-pack-2-2-cast/sc-3-a-118933/default.aspx

[13] *Matousec.com* [online]. 2008 [cit. 2010-05-14]. Proactive Security Challenge. Dostupné z WWW: <http://www.matousec.com/projects/proactive-security-challenge/results.php>.

[14] Mylovelyapps [online]. 2009 [cit. 2010-05-17]. Antispyware test 2009. Dostupné z WWW: <http://www.mylovelyapps.com/comp/antispyware-test2009.htm>.

[15] KUBEŠ, Radek. Technet [online]. 4. 3. 2007 [cit. 2010-05-13].Firewall – další krok k ochraně počítače. Dostupné z WWW: <http://technet.idnes.cz/firewall-dalsi-krok-k-ochrane-pocitace-dx7-/software.asp?c=A070301_135341_software_vse >.

[16] *Slunečnice* [online]. 2009 [cit. 2010-05-19]. VirtualBox 3.1.4.57640. Dostupné z WWW: <http://www.slunecnice.cz/sw/virtualbox/>.

[17] Symantec.com [online]. 1. březen 2007 [cit. 2010-04-18]. Zabezpečení operačního systému Windows Vista. Dostupné z WWW: <http://www.symantec.com/cs/cz/norton/library/article.jsp?aid=article1_03_07>.

[18] WAIC, Vlastimil. Windows XP nejsou na odpis: SP3 přináší novou bezpečnost. *Živě.cz* [online]. 15. 10. 2007, [cit. 2010-05-04]. Dostupný z WWW: http://www.zive.cz/clanky/windows-xp-nejsou-na-odpis-sp3-prinasi-novou-bezpecnost/sc-3-a-138525/default.aspx.

[19] WAIC, Vlastimil. Pod poklicí Windows Vista SP1. *Živě.cz* [online]. 5. 11. 2007, [cit. 2010-05-04]. Dostupný z WWW: <http://www.zive.cz/clanky/pod-poklici-windows-vista-sp1/sc-3-a-138813/default.aspx>.

[20] Živě.cz [online]. 15. 8. 2008 [cit. 2010-04-25]. Druhy licencí softwaru. Dostupné z WWW: <http://beruska55.blog.zive.cz/2008/08/druhy-licenci-softwaru/>.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK