ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA

V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

Ochranný SW pro operační systémy

Diplomová práce

Praha 2010 ©

Vedoucí práce: Ing. Pavel Šimek, Ph.D.

Autor práce: Marek Veverka

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma „*Ochranný software pro operační systémy*“ vypracoval samostatně, pouze za odborného vedení vedoucího diplomové práce.

Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury.

V Praze, dne 5.4.2010 Podpis: .....

Poděkování

Rád bych tímto vyjádřil poděkování Ing. Pavlu Šimkovi, Ph.D. za jeho cenné připomínky, odborné vedení a ochotu při tvorbě této diplomové práce.

Název

Ochranný software pro operační systémy

Souhrn

Diplomová práce se zabývá ochranným softwarem pro operační systémy, to znamená antivirovými programy, firewally a antispyware programy. Hlavním úkolem práce je provést porovnání vybraných zástupců volně dostupných ochranných programů a vybrat z nich ty nejvhodnější pro zajištění ochrany počítače před škodlivým softwarem. Vybrané programy jsou testovány a jsou popsány jejich funkce a možnosti. Testování těchto programů a jejich popis tvoří základ pro jejich další hodnocení podle vybraných kritérií. Zjištěné výsledky tohoto hodnocení jsou porovnány a na jejich základě jsou vybrány ty nejvhodnější ze zkoušených programů, které lze doporučit k zajištění ochrany počítače.

Klíčová slova

Škodlivý software, Vir, Červ, Trojský kůň, Spyware, Antivirus, Firewall, Antispyware

Title

Security software for Operating systems

Summary

The diploma thesis deals with security software for operating systems, it means antivirus programs, firewalls and antispyware programs. Primary objective of thesis is to make comparison of selected representatives of freely accessible security programs and choose the most optimal of them for securing safety of computer against malicious software. Selected programs are tested and their functions and options are described. Testing procedure of these programs and their description make base for their additional evaluation according to selected criterias. Discovered events of this evaluation are compared and in accordance with them, the most optimal of tested programs are selected and recommended for securing safety of the computer.

Key words

Malware, Virus, Worm, Trojan horse, Spyware, Antivirus, Firewall, Antispyware

Obsah:

1. Úvod

Příchod počítačů znamenal revoluci v životě lidstva. Tyto ze začátku obrovské stroje byly nejdříve používány pro usnadnění zpracování rozsáhlých výpočtů a umožnily tak například sestrojit atomovou bombu, nebo doletět člověku na Měsíc. Postupem času se počítače zmenšovaly a nacházely si cestu do dalších a dalších oblastí lidského života. Dnes je jejich prostřednictvím řízena doprava, zajišťovány obchodní transakce, vyráběno široké spektrum produktů atd. V moderním světě si tak již každodenní život bez počítačů, nebo připojení k internetu nelze představit. Díky tomu jsou dnešní počítače, laptopy a kapesní počítače zaplňovány obrovským n množstvím nejrůznějších dat, například dokumenty, aplikacemi, hudbou, videem apod. Některá z těchto dat jsou postradatelná, jiná však nenahraditelná. V každém případě bude ať firemní, nebo soukromý počítač vždy obsahovat data, která je třeba chránit.

S rychlým rozvojem počítačů šel předvídatelně ruku v ruce i rozvoj potencionálního nebezpečí pro jejich uživatele. Dnešní počítače jsou tak ohrožovány širokou škálou nebezpečí a hrozeb, do kterých jsou zařazovány nejrůznější formy počítačových virů, červů a trojských koní, dialerů, hoaxů a také spyware a adware. Vliv tohoto ohrožení na napadený počítač je různý. Dojít může mimo jiné ke zpomalení výkonu počítače, ztrátě nebo odcizení dat, zpomalení komunikace v síti, zaplavení mailové schránky nevyžádanou poštou apod. Doby, kdy veškerou bezpečnost počítače zajišťoval antivirový program aktualizovaný jednou za čas disketou zaslanou výrobcem, jsou však bohužel nenávratně pryč.

Existuje několik způsobů jak zajistit ochranu počítače před výše zmíněnými hrozbami. Naprostý základ představuje používání zdravého rozumu. Uživatel, který nebude při práci s počítačem zbytečně riskovat, tak nemusí mít důvod k vážným obavám. Další a neméně důležitou součást ochrany počítače představuje specializovaný ochranný software. Jeho dnešní nabídka je skutečně široká, antivirovými programy počínaje, přes firewally, programy na detekci a odstranění spywaru a dalšími bezpečnostními utilitami konče. Kombinace těchto způsobů pak umožňuje nejen spolehlivou ochranu počítače a jeho operačního systému před přístupem škodlivého softwaru, ale i odstranění již nalezených hrozeb.

2. Cíl a metodika práce

2.1. Cíl práce

Cílem diplomové práce je provést porovnání vybraných zástupců volně dostupných ochranných programů, používaných pro zajištění ochrany počítačů pracujících pod operačními systémy před škodlivým softwarem. Výkony testovaných programů, jejich nároky na systémové zdroje a další vlastnosti budou posouzeny podle stanovených hodnotících kritérií a na základě tohoto hodnocení budou vybrány programy nejvhodnější pro zajištění ochrany počítače.

2.2. Metodika

Nejprve bude uvedeno rozdělení škodlivého softwaru na jednotlivé druhy, zmíněna bude také jejich historie a vývoj do současnosti. Následující kapitoly se budou věnovat podrobnějšímu popisu jednotlivých druhů škodlivých programů. Popsány tak budou jejich funkce, způsob činnosti a možné způsoby šíření. Pozornost bude věnována také škodám, které mohou škodlivé programy v počítači způsobit.

Další část práce bude zaměřena na ochranu počítače. Přiblíženy budou základní způsoby zajištění jeho bezpečnosti, nastíněna bude i problematika antivirových firem a testování ochranného softwaru. Následující kapitoly se budou věnovat jednotlivým typům ochranného softwaru. Proveden tak bude podrobnější popis funkce a způsobů činnosti antivirů, antispywarových programům a firewallů.

Závěr práce bude obsahovat popis vybraných zástupců tří hlavních typů ochranných programů, které jsou použitelné pro zajištění ochrany počítače. Tyto vybrané programy budou prozkoumány, otestovány a ohodnoceny podle stanovených kritérií, např. podle rychlosti kontroly počítače, kvality uživatelského rozhraní, nebo vytížení systémových zdrojů. Výsledné hodnocení pak poslouží jako podklad pro výběr programu nejvhodnějšího pro zajištění ochrany počítače uživatele, který disponuje minimálními, nebo žádnými znalostmi z oblasti zabezpečení počítače proti škodlivému softwaru.

3. Hrozby pro počítač

S tím jak se svět stále více stává propojený prostřednictvím nejrůznějších komunikačních sítí, je kyberprostor navzdory uplatňování mnoha opatření vystaven nejrůznějším druhům počítačové infiltrace. Pod tímto pojmem si lze představit jakýkoli neautorizovaný vstup do operačního systému počítače, jeho programů nebo paměti, kde je následně prováděna jejich modifikace, poškození, nebo znepřístupnění. Mezi nejrozšířenější způsoby infiltrace patří šíření a zneužívání vlastností škodlivého software, tzv. malware (z angl. MALicious softWARE) a útoky hackerů, spojené často se zneužíváním specializovaného malware. Někdy se infiltrace používá i zúženě ve spojení s viry – virová infiltrace.[6]

Malware je zastřešující pojem pro počítačové červy, viry, trojské koně, špionážní software, zadní vrátka aj. Šíření škodlivého software je však většinou uživatelů spojováno pouze s termínem virus, bez ohledu na to, zda se jedná o virus, nebo jiný druh škodlivého software.

Starší uživatelé počítačů tak už jen se slzou v oku vzpomínají na doby, kdy byl malware představován viry rozšiřovanými prostřednictvím kopírování souborů z diskety na pevný disk a kdy s trochou opatrnosti bylo těžké počítač zavirovat.[3]

3.1. Klasifikace škodlivého SW

Jednoznačné dělení škodlivého softwaru je velmi obtížné, protože:

- Vlastnosti malwaru jsou někdy velmi podobné
- Infiltrace škodlivým software je často kombinací několika jeho druhů
- Různí odborníci používají poněkud nejednotnou terminologii

Následující rozdělení tedy představuje jednu z mnoha variant.

- Počítačové viry (angl. Viruses)
- Červy (angl. Worms)
- Trojské koně (angl. Trojan horse)
- Zadní vrátka (angl. Backdoor)
- Dialer

- Adware
- Špionážní software (angl. Spyware)

3.2. Historie malwaru

Zcela jistě se dnes nenajde uživatel počítače, který by se někdy nesetkal s jeho napadením virem, nebo jinou formou malwaru. I když by se mohlo zdát, že se tak děje zejména v poslední době, není to pravda. V minulosti byl škodlivý software tvořen z různých důvodů, častokrát dokonce v zájmu vědy a poznání. Mnoho dřívějších nakažlivých programů, mezi které patří internetoví červi a velký počet virů, vzniklo jako experiment nebo žert a většinou se záměrem vůbec neškodit nebo pouze obtěžovat. Mladí programátoři, kteří studovali možnosti virů a techniky jejich psaní, vytvářeli takové programy, aby ukázali, že to dovedou, nebo aby viděli, jak dalece se mohou jejich výtvory rozšířit.

Za vůbec první volně se šířící je považován virus Joe, který se objevil na počítačích Apple Macintosh v roce 1981.[6] Teoreticky byly viry předpovězeny až za dva roky F. Cohenem. Na počítačích IBM PC získaly v roce 1986 prvenství viry Burger a VirDem. Prvním boot virem se pak ve stejném roce stal virus Brain, napsaný dvojicí bratrů z Pákistánu. Tento virus byl šířen pomocí disket s nelegálním software zakoupených cizinci v jejich obchodě. V těle viru byla zanechána textová zpráva s jejich jmény, adresou a telefonním číslem.

V roce 1987 se objevily další, tentokrát souborové viry Leligh a první z rodiny virů Jerusalem. Během několika let začaly viry způsobovat škody za stamiliony dolarů a staly se postrachem nezabezpečených počítačových sítí. V této době se navíc do počítačů ukládala jen velmi důležitá data, proto viry představovaly velké nebezpečí.

V roce 1988 došlo k rozšíření jednoho z prvních počítačových červů. Tzv. Morrisův červ infikoval více než 6000 počítačů a zcela ochromil tehdejší sítě. Vytvořen byl tehdy 23letým studentem Robertem Morrisem.

obrázek č. 1 - Disketa obsahující zdrojový kód červa Morris uložená v Bostonském vědeckém muzeu [http://www.flickr.com/photos/87242149@N00/1802318014/]

Průběžně vznikly i první firmy specializované na vývoj antivirových programů, např. společnost McAfee, která na trh uvedla po dlouhou dobu legendární program VirusScan.

V dalších letech pokračoval vývoj virů, a to jak kvantitativní, tak i kvalitativní. Na konci roku 1990 se objevil první polymorfní virus a v roce 1992 s objevil první Windows vir, napadající spustitelné soubory pro Windows. Populace počítačových virů dosáhla několika stovek jedinců. Tvůrci virů změnili taktiku a viry se tak začaly šířit i do domácích počítačů. Ty tehdy ještě nebyly propojeny sítěmi, ale mezi uživateli panovala čilá výměna dat a zejména nelegálního software na disketách a později i na CD discích.

S rozšířením Internetu hrozba virové nákazy počítače značně stoupla. Začaly se šířit makroviry a skriptovací viry. Kromě virů se však začaly šířit i další formy malwaru – spyware, spam, trojské koně a dialery. Spyware a adware se stává stále větším problémem. Navíc se tento škodlivý software v řadě případů prolíná s trojany. Typicky trojan – downloader stáhne do počítače adware. V poslední době se pak fenoménem stává zejména nevyžádaná pošta, tzv. spam. Dochází rovněž k návratu klasických červů.

Mohlo by se zdát, že s koncem používání disket je konec i se šířením virů, červů a jiné "havěti", ale opak je pravdou. S nástupem USB flash disků a jejich masivním rozšířením dochází k přenosu škodlivého softwaru právě jejich prostřednictvím. Využívá se přitom vlastností souboru autorun.inf. Na základě informací z tohoto souboru operační

systém Windows rozhodne o další činnosti s vloženým USB diskem. Za normálních okolností dojde například ke spuštění nějakého EXE souboru, který je v souboru autorun.inf uveden. Pokud je flash disk napaden virem a tento ovládl autorun.inf, může dojít ke spuštění infikovaného EXE souboru a následně k infekci samotného počítače.

3.3. Viry

Počítačové viry představují po trojských koních nejstarší skupinu malwaru. Počítačový virus lze definovat jako škodlivý program, který využívá slabin operačního systému počítače a bez vědomí uživatele se samovolně replikuje a dále šíří. Virus ke své replikaci a dalšímu šíření potřebuje hostitele, ke kterému je připojen. Vhodnými hostiteli viru mohou být spustitelné soubory, systémové oblasti disku, nebo soubory, k jejichž použití je třeba specifická aplikace, např. dokumenty MS Word, Excel apod. V okamžiku spuštění hostitele je proveden i kód viru a jeho následná replikace. Virus dále zkoumá aktivity systému a čeká na naprogramovaný signál pro zahájení své škodlivé činnosti.

Nejvíce virů je v dnešní době napsáno pro operační systém Windows, uvádí se více jak 60 000. Je to dáno jednak jeho obrovským rozšířením, ale také dalšími důvody, např. standardní používání administrátorského typu účtu u většiny počítačů se systémem Windows. Dalším důvodem šíření virů ve Windows jsou skrývané přípony souborů, takže pokud uživatel místo dopis.doc.exe vidí pouze dopis.doc, může v dobrém víře spustit místo neškodného dokumentu něco zcela jiného. Tyto viry na Linuxu nefungují, s výjimkou některých emulátorů, protože Linux není binárně kompatibilní s Windows a nemohou tedy způsobit žádnou škodu.

Přímo pro Linux několik málo virů existuje, ale skoro vůbec se nešíří, stejně tak u operačního systému Mac OS X. Je to dáno jednak malým rozšířením Linuxu a na jeho základě založených operačních systémů, kdy se pro ně nevyplatí nějaký virus vyvíjet, a jednak architekturou systému a systémem oprávnění.

Uživatelé a oprávnění jsou v Linuxu nastaveny tak, že běžné úkony uživatel provádí pouze s omezenými oprávněními, běžný uživatel tak nemůže měnit programy, k nimž nemá právo zápisu, a instalovat nové aplikace do systémových adresářů. Programy pro Linux jsou vytvářeny tak, že spustitelná část programu a globální konfigurační soubory jsou uloženy na místě, kam není běžným uživatelům umožněn zápis. Uživatel má ve svém

domovském adresáři uloženy vlastní konfigurační soubory, které ostatní uživatelé nevidí a nevyužívají. Toto uspořádání efektivně brání jak šíření virů, tak nezkušeným uživatelům v poškozování systému. Pokud uživatel do systému přece jen virus dostane, virus může napadnout pouze spustitelné soubory, ve kterých má uživatel právo zápisu.

Svou roli hraje také způsob šíření programů v Linuxu, u opensourcových aplikací nejsou téměř nikdy přenášeny spustitelné, virem napadnutelné soubory, ale jen jejich zdrojový kód, který je teprve na cílovém stroji přeložen do spustitelného tvaru.[10]

Pokud tedy správce systému dodržuje několik základních pravidel, je šíření virů v Linuxu prakticky nemožné.

3.4. Klasifikace počítačových virů

Počítačové viry lze rozlišovat z několika hledisek, např. podle rychlosti šíření, podle typu napadaných objektů, nebo způsobu činnosti.

3.4.1. Klasifikace virů podle rychlosti šíření:

Podle rychlosti šíření lze viry dělit na:

- Rychlé viry – jakmile jsou v paměti aktivovány, napadají všechny otevřené programy. Při prohledávání pevného disku, např. při spuštění antivirového programu, může dojít i k napadení všech spustitelných souborů na disku. Tyto viry také mohou aktivně vyhledávat soubory vhodné k napadení.
- Pomalé viry – i když jsou v paměti aktivovány, se svou replikaci čekají na dobu, kdy se s daným spustitelným souborem normálně pracuje, např. vytváření, kopírování, resp. modifikace souboru. Virus se tak pozvolna nepozorovaně množí a napadá všechna dostupná paměťová média.
- Vzácně napadající viry – jsou charakteristické tím, že napadají spustitelné soubory pouze při splnění specifických podmínek. Dochází tak k napadení např. každého desátého souboru, souboru s velikostí v určitém rozmezí apod., rychlost šíření na další paměťová média je však nízká. Podobně jako pomalé viry tak snižují pravděpodobnost svého odhalení.

3.4.2. Klasifikace virů podle typu napadených hostitelských objektů:

Podle typu infikovaných hostitelských souborů lze viry dělit na:

- Boot viry
- Souborové viry
- Multiparitní viry
- Makroviry

3.4.2.1. Boot viry

Představují nejstarší a nejčastěji se vyskytující skupinu virů, se kterou se uživatel může setkat. Boot viry infikují určité systémové oblasti disku. Těmito oblastmi mohou být boot sektory disket a MBR (Master Boot Record) pevného disku. Napadením některé z těchto oblastí si boot virus zajistí svoje spuštění hned po startu počítače, kdy se startovací rutina pokouší zavést operační systém z prvního dostupného zařízení podle pořadí určeného nastavením v BIOSu. Virus zde uložený v těchto oblastech je tak aktivován a zahájí svou činnost. Boot viry se chovají tak, že obvykle přepíší svým vlastním kódem boot sektor, a původní přepsanou část boot sektoru uschovají na jiné, bezpečné místo disku. Jedná se například o:

- nevyužité clustery
- použité clustery (hrozí poškození původního obsahu)
- systémové oblasti
- oblasti nacházející se mimo aktivní oblast disku

Pokud dojde k tomu, že virus zapíše původní boot sektor do kritické oblasti disku či diskety, jako je např. sektor obsahující část tabulky FAT, nebo hlavní diskový adresář, mohou být data na disku navždy ztracena.

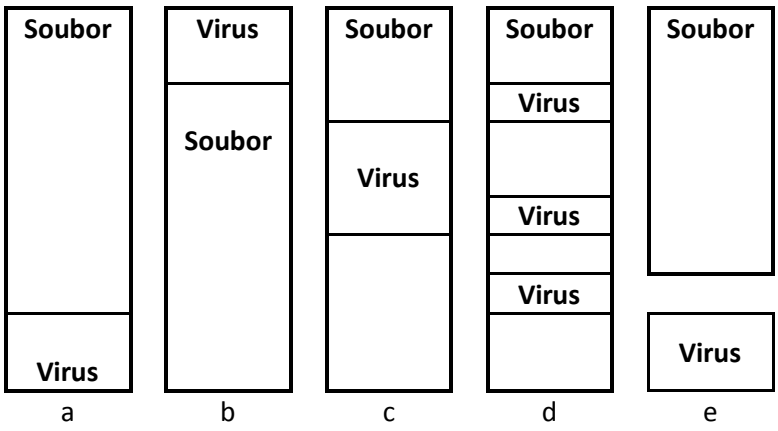
Typickým příznakem přítomnosti infekce způsobené boot virem, který lze zaznamenat i u neznámých boot virů je skutečnost, že kapacita systémové paměti, zobrazená programem chkdsk či mem, je většinou nejméně o 1024 bytů menší, než jaká je skutečná paměť instalovaná v systému.

3.4.2.2. Souborové viry

Představují druhou a svého času nejrozšířenější skupinu virů, hostitelem přenášejícím virus jsou spustitelné soubory. Souborové viry v napadeném programu přepíší část kódu svým vlastním, nebo vlastní kód k programu připojí a tím změní jeho velikost a chování.

Podle metody infekce lze souborové viry rozdělit na několik skupin:

- Přepisující viry – přepisují a tím ničí části původního kódu programu. Původní část programu je tak ztracena a opětovným spuštěním souboru dojde pouze k aktivaci samotného viru snažícího se o další replikaci a nikoliv původního programu.
- Parazitické viry – za parazitické jsou označovány viry, které se připojí k proveditelnému hostiteli bez toho, aby ho nějak trvale poškodily. Tuto skupinu lze dále rozdělit na viry typu *prepend (před)*, *insert (v)* a *append (za)*, a to podle toho, kam je tělo viru z pohledu původního souboru umístěno. Posledně jmenovaný způsob je nejčastější. Původní soubor je při nakažení upraven tak, aby po jeho opětovném spuštění došlo jak k aktivaci původního programu, tak i viru.



obrázek č. 2 - Možné umístění viru v souboru [6]

- Doprovodné viry - nemění soubory, ani systémové oblasti disku, ale infikují soubory s příponou EXE tak, že vytvoří nový soubor s tělem viru, a to se stejným názvem, ale s příponou COM, např. u souboru COD.EXE virus vytvoří soubor COD.COM. Na základě priorit dojde při volání tohoto souboru bez uvedení přípony nejprve k aktivaci toho s příponou COM a tím i k aktivaci viru. Po

provedení vlastní zadané činnosti může virus nechat provést původní soubor s příponou EXE.

Jinou metodou infikování je přejmenování původního EXE souboru změnou jeho přípony a vytvoření souboru s tělem viru pod původním názvem (například přejmenováním COD.EXE na COD.EXD a posléze vytvořením infikovaného souboru COD.EXE).

3.4.2.3. Multiparitní viry

Napadají soubory i systémové oblasti disku, výhodně kombinují možnosti boot virů i souborových virů. Hlavní výhodou boot virů představuje to, že se dostanou do paměti jako úplně první spustitelný kód zaváděný z disku nebo diskety, to je ale současně i jejich nevýhodou. V danou chvíli totiž ještě nemají k dispozici služby operačního systému a jsou tak odkázány na nejnižší úroveň systémových služeb BIOSu, nemohou tedy infikovat soubory a možnosti jejich rychlého šíření jsou proto omezené.

Souborové viry naproti tomu mohou využívat služby operačního systému a napadají soubory, je tedy mnohem pravděpodobnější, že bude spuštěn napadený soubor, než že bude systém spuštěn z infikovaného média.

Multipartitní viry tak využívají výhod obou výše zmíněných postupů. Mohou napadnout nejen zaváděcí oblast disku nebo diskety, ale i spustitelné soubory. Při útoku na soubor mohou multipartitní viry vyžívat libovolný postup napadení souboru a napadení systémové oblasti je shodné s technikami používanými běžnými boot viry.

3.4.2.4. Makroviry

Napadají dokumenty vytvořené v některých kancelářských aplikacích, především dokumenty aplikací MS Office, vyjímečně i dokumenty jiných aplikací. Výměnou těchto dokumentů mezi uživateli tak dochází k jednoduchému a rychlému šíření. Využívají toho, že tyto soubory neobsahují pouze data, ale i makra, která viry využívají ke svému šíření. Např. virus W97M Melissa při své aktivaci použije dokument, na němž uživatel zrovna pracuje, infikuje jej a rozešle elektronickou poštou na 50 náhodně vybraných adres z adresáře uživatele. Takováto akce zřejmě nebude mít hrozivé následky, ale podobný

makrovirus může z uživatelova počítače vykrádat důvěrné informace, pracovat s jeho soubory, spouštět aplikace apod.

3.4.3. Klasifikace virů podle způsobu činnosti:

Podle způsobu činnosti lze viry dělit na:

- Rezidentní viry – tento typ viru se po spuštění hostitelského souboru (souborový virus), nebo při prvním zavedení systému z napadeného boot sektoru (boot virus), usídlí v operační paměti a zde dále provádí škodlivou činnost. Soubory, se kterými uživatel pracuje, napadá až dokud není systém vypnut.
- Nerezidentní viry – jakmile je spuštěn hostitelský soubor, virus provede svou škodlivou činnost a je ukončen. Napadá nalezené dostupné nenakažené soubory. Nezůstává v paměti.
- Stealth viry – snaží se skrýt svou přítomnost v systému pomocí tzv. stealth technik. Pokud virus usazený v paměti zachytí požadavek na čtení ze souboru, zkontroluje si, jestli se požadavek týká i napadeného souboru. V takovém případě pak vrací hodnoty původního neinfikovaného souboru.
- Polymorfní viry – svým chováním se podobají stealth virům, své odhalení se snaží znesnadnit tak, že při své replikaci tvoří kopie, které jsou odlišné od původního viru. V napadených souborech tak není možné najít typické sekvence stejného kódu.

3.5. Červi

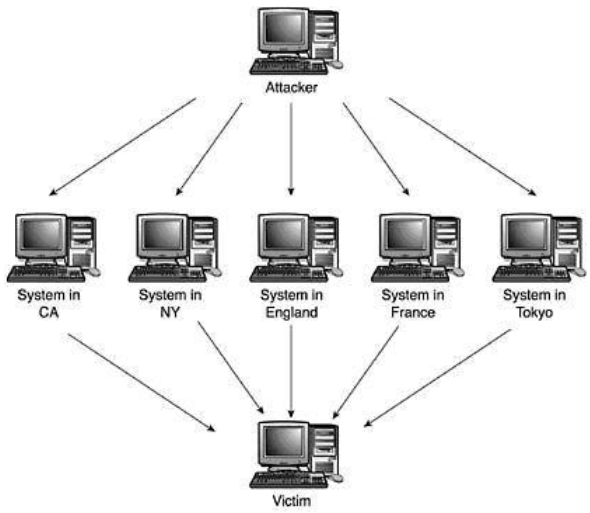
Poprvé byl počítačový červ (worm) popsán Johnem Brunnerem r. 1975 v románu The Shockwave Rider jako spustitelný kód replikující sebe sama v síti. Na začátku 80. let byli červi simulováni ve výzkumném středisku firmy Xerox v Palo Alto. V roce 1989 pak tzv. Morrisův červ dokázal zahltit většinu tehdejší sítě, ze které později vznikla síť s velkým S, tedy Internet. V poslední době jsou "populární" červi Code Red, SQL Slammer, Lovsan / Blaster, Sasser nebo Conficker.

Červ je speciální program schopný rozesílat svoje kopie na jiné počítače, a ty v případě příznivých okolností infikovat. Mnoha uživateli jsou červi často nesprávně považováni za podskupinu počítačových virů. Stejně jako viry se šíří bez vědomí uživatele,

ke svému šíření však červ nepoužívá infikované soubory, ale síťové pakety. Ty jsou směrovány od již infikovaného počítače na další počítače připojené k Internetu, a to buď náhodně, nebo podle zadaného klíče. Pokud takový infikovaný paket dorazí k počítači a zjistí v jeho zabezpečení specifickou trhlinu, může dojít k infikování tohoto počítače a následné další reprodukci červa prostřednictvím dalších paketů. Šíření červa je tedy založeno na využívání, či spíše zneužívání specifických bezpečnostních děr operačního systému nebo aplikací počítače napojeného na Internet.

Stejně jako počítačových virů, i počítačových červů existuje několik druhů. Rozlišovány jsou podle způsobu šíření na:

- E-mailové červy - ke svému šíření využívají elektronickou poštu. Po infikování počítače se začnou rozesílat na e-mailové adresy z jeho adresáře, nebo prohledáváním obsahu uložených souborů a extrahováním řetězců, které vyhovují tvaru e-mailové adresy. Zvláštním případem jsou sítě botnet, složené z počítačů infikovaných speciálním červem, kdy infikované počítače na příkaz autora červa hromadně zasílají SPAM, nebo provádějí útoky typu DDoS na jiné počítače.



obrázek č. 3 - Schema útoku typu DDoS [11]

Obsah infikované zprávy zaslané e-mailovým červem obvykle obsahuje vlastní škodlivý program jako přílohu, případně odkazuje na webové stránky, které jsou schopny infikovat počítač příjemce. Výhodou tohoto přístupu je možnost využít e-mailového účtu oběti a v kombinaci s použitím adres dostupných v adresáři e-mailových adres působit jako věrohodná korespondence.

- Internetoví červi – využívají všechny dostupné síťové prostředky počítače ke skenování ostatních počítačů připojených k síti. Pokud najde počítač, který je zranitelný a umí-li této zranitelnosti využít, provede na takový počítač útok a (v závislosti na závažnosti této zranitelnosti) je v ideálním případě schopen spuštění škodlivého kódu a vlastní instalace do systému.
  Výhodou tohoto přístupu je fakt, že v případě efektivního využití zranitelnosti počítače je možno jej infikovat bez vědomí nebo přičinění uživatele.
- IM a IRC červy - ke svému šíření využívají sítě pro komunikaci v reálném čase. IM červy obvykle rozesílají odkazy na webové stránky schopné infikovat příjemcův počítač, IRC červi pak zasílají svůj program jako spustitelný soubor. Z toho vyplývá jejich menší nebezpečnost, neboť aby mohlo dojít k infekci, musí uživatel soubor přijmout, uložit a následně spustit.
  Výhodou tohoto přístupu je, stejně jako v případě e-mailových červů, možnost zasílání odkazů a souborů jménem uživatele napadeného systému a působit věrohodně.

3.6. Trojské koně

Za trojského koně neboli trojana může být označen jakýkoli atraktivní nebo užitečný program, který kromě své primární úlohy provádí nějakou formu škodlivé činnosti. V daleké minulosti se tak několikrát objevil trojský kůň vydávající se za antivirový program McAfee VirusScan, ve skutečnosti však likvidoval soubory na pevném disku. Jedním z posledních, dodržujících tuto tradici, byl trojan Telefoon, který se vydával za komprimační program RAR 3.0, jehož oficiální verze 3.0 ale vyšla až za několik let.[6] V současnosti se mohou trojské koně šířit ve spojení s počítačovými viry nebo červy, případně mohou být nainstalovány při využívání aktivních skriptů na WWW stránkách, k jejich šíření tak již nemusí být potřeba výše zmíněná kamufláž.

Trojský kůň není na rozdíl od virů a červů schopen vlastní replikace a infikování souborů. Trojský kůň se nejčastěji šíří jako spustitelný soubor typu.EXE, který obsahuje tělo trojského koně. Uživatelé bývají zlákáni ke spuštění takovéhoto souboru, neboť se domnívají, že pochází z důvěryhodného zdroje. Nejsnadnějším způsobem ozdravení napadeného systému počítače pak je jednoduché smazání příslušného souboru, vzhledem k tomu, že trojský kůň není připojen k žádnému hostiteli.

V současnosti se lze setkat s několika formami trojských koňů:

- Password sterling trojani (PWS) – skupina trojských koní, která většinou sleduje stisky jednotlivých kláves (key-loggers), tyto ukládá a následně odesílá na zadanou e-mailovou adresu. Tímto způsobem tak lze získat i velmi důležitá hesla, např. k elektronickému bankovnictví uživatele počítače, k chráněným složkám apod. Tento typ trojanů lze klasifikovat také jako spyware.
- Destruktivní trojani – klasická forma, pokud je takovýto trojský kůň spuštěn, ničí soubory na pevném disku, případně ho celý rovnou kompletně zformátuje. Do této kategorie lze zařadit i většinu tzv. BAT trojanů, tedy škodlivých dávkových souborů s příponou BAT.
- Trojský kůň typu "dropper" – jedná se o tzv. vypouštěče, neboť ve svém těle přenáší jiný škodlivý kód, který je po aktivaci trojského koně vypuštěn do systému.
- Zadní vrátka, tzv. Backdoor – jde o aplikace typu client-server sloužící pro vzdálenou správu počítače a sama o sobě nemusí být škodlivá. Záleží na poctivosti a aktivitách osoby, která tuto vzdálenou správu vykonává.
  Zadní vrátka pak fungují následovně. Klientská část aplikace, vlastněná útočníkem, vysílá jeho požadavky serverové části, umístěné např. na počítači s cennými a důležitými daty, serverová část tyto požadavky plní a případně odesílá zpět ke klientovi požadované informace. Pokud je serverová část zadních vrátek vypuštěna např. spolu s úspěšně se šířícím virem, může mít útočník k dispozici obrovské množství počítačů, ke kterým má přístup. Komunikace mezi oběma částmi je většinou založena na protokolech TCP/IP, z čehož vyplývá, že útočník může být vzdálen tisíce km od serverové části zadních vrátek.
- Downloader (TrojanDownloader) - význam tohoto škodlivého programu je podobný jako v případě dropperu – vypustit „škodnou" do počítače. Downloader si ovšem další škodlivé programy nenese s sebou, ale snaží se je stáhnout z předem definovaných adres na Internetu.

3.7. Hoax

Hoax je označení pro zprávu, která svým kladným nebo záporným obsahem motivuje jejího příjemce k dalšímu rozesílání jeho známým. Motivace k jejímu dalšímu rozesílání je výhradně dána jejím kladným (např. nabídka určitého produktu zdarma), nebo záporným (např. varování před neseriózní firmou, nebo jiná poplašná zpráva) vlivem na příjemce Hoaxu. Šíření Hoaxu tak zcela závisí na uživatelích, kteří takovouto zprávu e-mailem obdrží a její přeposílání pak způsobuje její lavinovité šíření.

Hoaxy lze typicky dělit na:

- Falešný poplach – takováto zpráva manipuluje s informacemi a snaží se uživatele přimět k dalšímu šíření zprávy (např. Pozor ICQ vir, pošlete to všem) nebo dokonce k nějakému destruktivnímu zásahu (Smažte jbdmgr.exe z instalace Windows, je to virus.). Tento typ zprávy přesně vystihuje původní význam pojmu hoax
- Zábavné – dříve se řetězové dopisy šířily pomocí klasické pošty, dnes je za stejným účelem využíván internet. Zábavné hoaxy využívají uživatelovy touhy být vtipný nebo jeho pověrčivosti a vyhrožují, že pokud danou zprávu nepošle dál, bude mít v dalším životě smůlu. Poslušnému uživateli naopak slibují všechno možné.
- Prosby – hoax většinou působí na city a prosí příjemce o darování krve, hledání ztracené osoby, případně přímo vylákává peníze. Některé z těchto zpráv byly původně opravdu rozeslány lidmi ve svízelné životní situaci, ale hoaxy často přežívají mnohem déle, než měl autor v úmyslu.

Mezi nejčastější Hoaxy patří varování před počítačovým virem. Pokud uživatel takovouto podezřelou zprávu obdrží, nejlépe udělá, pokud ji jednoduše smaže. Také je možné se přesvědčit, zda je již tato zpráva zveřejněna na serveru www.hoax.cz, a pokud ne, odeslat ji tvůrcům tohoto serveru.

Příklady některých hoaxů:

Únos dětí v obchodním domě

Dávejte si pozor na své děti!
Upozorňuji na případ, který se stal nedávno mé známé při nakupování v obch.domě IKEA.

Rodiče šli nakupovat se svou desetiletou dcerou do obch.domu IKEA. Najednou zjistili, že dcera s nimi není. Chvíli čekali, jestli se neobjeví. Pak se rozhodli nechat ji vyhlásit. Obchodní dům hned uzavřel všechny východy a začal ji hledat. Holčička byla objevena na toaletě, ostříhaná a převlečená do jiných šatů.
Asi to nebyl první případ, co se tam stal.
Proto pozor při předvánočních nákupech!!!!!!!!!!

Oficiálně z banky:
Oficiálně z banky: Jakmile se ocitnete v kritické situaci a musíte pod nátlakem vybrat peníze z bankovního automatu na požádání/přinuceni násilníkem, zadejte svůj PIN opačně: to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policii, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli.

Přepošlete toto co nejvíce lidem.

3.8. Dialer

Dialer je program, který změní způsob přístupu počítače na internet prostřednictvím modemu. Místo běžného tel. čísla pro připojení na Internet, přesměruje vytáčení na čísla se zvláště vysokým tarifem za minutu spojení. Stejnou změnu může dialer provést i u připojení přes mobil pomocí GPRS.

Dialer je možné získat dvěma způsoby. Nejčastěji se do počítače dostane tak, že si jej uživatel sám stáhne, jakmile navštíví stránky, nabízející ke stažení nelegální hudbu, filmy, software nebo s pornografickým obsahem. Dialer je také možné získat prostřednictvím sítí pro sdílení dat, např. Direct Connect, Kazaa apod. Mnoho takto postižených uživatelů si ale dialer stáhne a spustí sama a dobrovolně. Důvodem je to, že na příslušných stránkách je uvedeno, že jinak se k požadovanému obsahu nelze dostat.

Druhý způsob získání dialeru je zákeřnější, někdy se totiž dialer stáhne a spustí zcela bez vědomí uživatele. V takovém případě ho může do počítače prostřednictvím e-mailu umístit nějaký virus, nebo si ho oběť může nechtěně stáhnout, pokud používá špatně nastavený internetový prohlížeč.

Ne vždy může být dialer považován za škodlivý program, může totiž sloužit jako zpoplatnění určité služby (například přístup na speciální www stránky) s plným vědomím uživatele.

S rozšiřováním připojení počítače k internetu prostřednictvím ADSL, Wi-Fi nebo jiných technologií však tento druh malwaru pomalu ustupuje.

3.9. SPAM

Spam je nevyžádaná emailová zpráva, zpravidla obsahující obchodní sdělení či nějakou „lukrativní“ nabídku. Tyto zprávy jsou v mnoha kopiích rozesílány po celém internetu ve snaze vnutit lidem pochybné výrobky či je jinak podvést.[9] Spam nemusí být primárně považován za malware, ale různé formy malwaru mohou být ke spamu připojeny, například v podobě trojského koně.

Vzhledem k nárůstu počtu zasílaných nevyžádaných emailů, se ze spamu stává problém, který je již v některých státech trestně postihován. Rozesílání spamu je skvělý obchod, na kterém se podílí organizované skupiny na celém světě. Stačí pouze, aby uživatel zadal svoji správnou emailovou adresu v některé z mnoha diskuzí probíhajících na internetu. Jinak jsou e-mailové adresy do spamových databází získávány mj. také pomocí robotů a virů. Roboti, kteří procházejí webové stránky a sbírají e-mailové adresy, se však zpravidla nezatěžují hlubší analýzou zdrojového kódu a sbírají všechno, co jenom trochu vypadá jako e-mailová adresa, tedy jakoukoli posloupnost písmen, číslic, pomlček a teček, která obsahuje zavináč. S rozesíláním spamu je navíc spojeno i falšování adres odesílatele, kdy jsou často zneužívány reálné a důvěryhodné e-mailové adresy a spam tak není včas odhalen.

Spam lze dělit do následujících kategorií:

- Reklamní spam (nejčastější, „pravý“ spam)
- Hoax
- Funkční nebo modifikované e-maily, generované viry, červy
- Odezva spamových filtrů, e-mailových klientů a antivirových programů o pokusu zaslat na určitou adresu spam

Existují i dvě kategorie spamu, které nemají za cíl získat peníze za pomoci reklamy, ale skutečným podvodem.[3]

Takovýmto spamem je:

- Phishing – tento spam se tváří jako dopis od uživatelovy banky nebo jiné důvěryhodné společnosti, vyzívající jej k zaslání důležitých informací. Zpravidla se jedná o údaje o kreditní kartě, tedy číslo kreditní karty a PIN, se záminkou jejich ověření. Ve spamu je také uveden odkaz na elektronický formulář, do něhož důvěřivý uživatel zadá příslušné údaje, které podvodník většinou ihned zneužije.
- Nigerijský dopis – jde o dopis, ve kterém odesílatel sděluje, že disponuje velkým množstvím peněz, bohužel zablokovaných v nějaké nepřístupné oblasti. V minulosti to byla občanskou válkou sužovaná Nigérie, odtud tedy název Nigerijský dopis. Odesílatel dopisu žádá, aby mu příjemce dopisu poskytl svůj bankovní účet k uložení této obrovské sumy peněz, dokud si nezařídí svůj bankovní účet v nějaké bezpečné zemi Evropy, nebo v USA. Za to slibuje odměnu. Pokud důvěřivý příjemce dopisu souhlasí, je většinou ještě požádán o určitou sumu peněz na údajné poplatky, či úplatky nutné k převodu peněz. Takovýto požadavek může příjemce obdržet i několikrát, jakmile ale podvodníkovi pošle dost peněz, už se neozve a jakoby se po něm slehne zem.

3.10. Adware

Adware (z angl. Advertising-supported software) je označení pro produkty znepříjemňující práci s nějakou aplikací prostřednictvím reklamy. Tyto reklamní programy bývají na cílový počítač nainstalovány současně s instalací různých freewarových aplikací. Adware pak uživateli předkládá různé reklamy v podobě reklamních bannerů, vyskakujících pop-up oken, nebo ikon v oznamovací oblasti, které ho vybízejí ke koupi jistého zboží. Další nepříjemností způsobenou adwarem může být přesměrování uživatelovi domovské stránky na jiné, reklamní stránky. Adware také může sledovat uživatelovy aktivity na Internetu a tomu přizpůsobit nabízené reklamy. Pokud jsou tyto informace dále odesílány nebo je s nimi obchodováno s třetími osobami, jedná se už spíše o spyware.

3.11. Spyware

Spyware je počítačový program, nainstalovaný na uživatelův počítač bez jeho souhlasu za účelem shromažďování informací o uživateli a jeho počítači. Spyware tajně sleduje uživatelovo chování a shromažďuje různé typy osobních údajů, v podobě praktik procházení na internetu, historie navštívených stránek nebo přehled nainstalovaných programů. Tato činnost je zdůvodňována snahou o zjištění potřeb či zájmů uživatele počítače a následné využití zjištěných informací pro cílenou reklamu. Technologie spywaru by však jeho tvůrci mohla být zneužita k odcizení podstatně důležitějších dat, např. přístupových hesel, přihlašovacích jmen apod. Stírá se tak hranice mezi spywarem a trojským koněm typu backdoor. Spyware také může ztěžovat uživateli ovládání počítače instalací dalšího software, změnou nastavení počítače vedoucí ke zpomalení připojení, otevírání různých domovských stránek, ztrátu připojení k Internetu nebo funkcionality programu.

Spyware se do uživatelova počítače nejčastěji dostává spolu s instalací jiného softwaru, nejčastěji programů pro sdílení hudby či videa. Většinou se jedná o ne zcela legální programy, které umožňují dostat se k jinak nepřístupnému softwaru.[3] Instalace spywaru někdy bývá zapsána jako jedna z licenčních podmínek, drtivá většina uživatelů se však neobtěžuje s jejich čtením a rovnou kliká na tlačítko Yes. Dalším trikem tvůrců spywaru je zobrazení dialogového okna s tím, že pokud uživatel klepne na tlačítko No, nebude moci stáhnout daný program.

3.12. Škody způsobované malwarem

Nakažení počítače některou z forem malwaru může uživateli způsobit škody různého rozsahu. Tyto škody se značně liší, a to podle toho, jakou formou malwaru byl počítač nakažen a jaký účinek má na operační systém, resp. na počítač.

3.12.1. Škody způsobené viry

Napadení počítače virem se projevuje jeho zhoršenou funkcí. Virus může způsobit:

- Zpomalení načítání programu – to z důvodu, že nejdříve dojde ke spuštění viru a teprve poté ke spuštění požadovaného programu. Zpomalení může být způsobeno i přímo činností viru, pokud probíhá současně s načítáním programu

- Snížení výkonu počítače – v důsledku činnosti prováděné virem souběžně s jinou činností počítače, nebo jako součást škodlivé činnosti viru
- Úbytek volného prostoru na pevném disku – v důsledku prodlužování souborů činností souborových virů, vytvářením nových souborů případně uchováváním mnoha kopií viru
- Úbytek operační paměti – z důvodu výskytu rezidentních virů v paměti. K projevům patří hlášení o nedostatku paměti při spouštění programů
- Poruchy programů – dříve zcela funkční program nepracuje vůbec, nebo pouze částečně
- Nečekaná hlášení na monitoru a jiné speciální projevy - mnoho tvůrců virů cítí potřebu dát najevo přítomnost viru prostřednictvím různých výpisů zpráv na monitor, žertovných grafických projevů (houkající sanitka přejíždějící přes monitor, padání písmenek) nebo akustických projevů v podobě melodií.

Virus však může způsobit i jiné škody než poškození systému. Obecně lze škody způsobené virem, případně jinou formou malwaru, rozdělit na škody přímé a nepřímé.

Přímé škody jsou zřejmější a patří sem:

- Náklady vynaložené na odstranění viru
- Náklady vynaložené na kontrolu, opravu a reinstalaci poškozených dat a softwaru
- Náklady vzniklé v důsledku výpadku výroby, problémů v řízení firmy, chybně provedených finančních transakcích (banky, burza, platební příkazy)
- Následky havárie jako důsledek chybného řízení technologického procesu (chemické továrny, jaderné elektrárny)
- Poškození zdraví v důsledku poškozeného programu

Nepřímé škody mohou být svojí výší porovnatelné se škodami přímými, uživatel si je ale mnohdy neuvědomuje tak, jako škody přímé a mohou být i obtížněji vyčíslitelné.

Mezi nepřímé škody patří:

- Náklady na nákup a provoz ochranného software a na s tím spojená organizační opatření a školení
- Náklady z omezení činností daná opatřeními antivirové ochrany

Způsobené škody lze také klasifikovat podle vlastností škodlivých částí viru a doby uplynulé od přítomnosti viru v počítači do jeho detekce a odstranění. Škody pak lze dělit na:

- Triviální – minuty nutné k odstranění viru, virus nemá destrukční část a není přepisující
- Malé – obnovení některých nebo všech spustitelných souborů ze záložních kopií, resp. reinstalace programů, desítky minut nutných k odstranění viru
- Střední – kódování disku, zničení FAT tabulky, formátování pevného disku. Data je nutné obnovit ze záloh, ztracena práce cca za půl dne
- Velké – postupné ničení nebo modifikace dat, virus je objeven až po několika dnech. Data je nutné obnovit ze starších záloh, pokud tyto existují, reinstalace softwaru, ztracena práce za několik dní
- Kruté – virus provádí postupné ničení dat, objeven s velkým zpožděním, obtížná obnova ze záložních kopií

3.12.2. Škody způsobené červy

Škody, které způsobuje počítačový červ, souvisejí zejména s procesem jeho šíření. Jedná se o snižování rychlosti průtoku dat mezi jednotlivými počítači v síti. Pokud má červ pro své šíření dobré podmínky, může dojít až k zahlcení počítačové sítě.

Kromě vlastního šíření červ v počítači velmi často provádí i nějakou sekundární činnost, která je červem nesena jako náklad. Typicky se jedná o:

- zneprovoznění počítače, nebo jeho součástí
- odstraňování souborů uložených v počítači
- zašifrování souborů uživatele kryptovirálním útokem jako nátlak k zaplacení poplatku, po kterém je přislíbena jejich opětovné dešifrování
- prohledávání počítače za účelem získání osobních dat, která mohou pro autora programu znamenat nějaký profit
- jako důsledek jiné činnosti způsobují nestandardní chování systému.
- A další činnosti

3.12.3. Škody způsobené dialerem

Vzhledem k charakteristice dialeru tento může kromě nepřímých škod způsobit i poměrně masivní škody přímé. V důsledku změny tarifu pro připojení k Internetu pomocí modemu za mnohem dražší může být uživateli doručen účet za telefon mnohonásobně překračující běžnou částku. A přestože uživatel počítače dialer většinou získal nevědomky, je zpravidla nucen účet zaplatit. Výše způsobených škod záleží pouze na rychlosti odhalení.

3.12.4. Škody způsobené spamem

Spam jako takový nemusí být primárně považován za malware. Problémem není ani tak zasílaná reklama, jako její obrovské množství. Spam škodí především tím, že:

- zabírá místo ve schránce a prodlužuje dobu stahování pošty (zvyšuje cenu placenou za připojení k Internetu)
- je třeba věnovat čas na rozlišování co je a co není spam a mazání spamu
- mezi spamem lze přehlédnout důležitý "normální" mail
- zbytečně zatěžuje počítačové linky a poštovní servery
- náklady na ochranu před spamem jsou větší než náklady na provoz e-mailu jako takového
- při automatické detekci spamu dochází k omylům, smazání chtěného e-mailu a k záhadným ztrátám e-mailů - snižuje se spolehlivost e-mailu jako takového
- antispamová opatření mohou způsobit zpoždění e-mailu - řádově v hodinách

Kromě toho mohou být různé formy malwaru ke spamu připojeny, například v podobě trojského koně.

3.12.4. Škody způsobené spywarem a adwarem

Spyware a adware způsobuje jak přímé, tak nepřímé škody. Jedná se zejména o získávání různých informací o uživateli, např. praktiky při procházení internetu, historie navštívených stránek nebo přehled nainstalovaných programů. Tyto informace jsou potom bez vědomí uživatele odesílány tvůrcům spywaru a využity k zasílání reklamy v podobě vyskakujících pop-up oken. Jejich zobrazování a následné zavírání uživatele obtěžuje a obírá o čas. Reklamy také mohou zobrazovat obsah, který se uživateli může zdát

nevhodný. Kromě toho může spyware a adware způsobit změny v nastavení počítače, způsobit přesměrovávání prohlížeče, problémy s internetovým připojením nebo může instalovat a spouštět různé další programy. Spyware také může způsobit znatelné snížení výkonu počítače, pokud je ho v pozadí operačního systému nainstalováno příliš velké množství. V takovém případě je potom nutné nainstalovat specializovaný software a spyware odstranit.

4. Ochrana počítače

Zajištění ochrany počítače před jeho infikováním některou z forem malwaru nevěnuje mnoho uživatelů žádnou pozornost. Žijí v blahém domnění, že jim se přece nemůže nic stát, ale opak je pravdou. Vzhledem k množství výše zmíněných hrozeb ohrožujících počítač, je jen otázkou času, než dojde k jeho napadení.

Účinná ochrana počítače před napadením malwarem se skládá z několika částí. Základní část ochrany představuje prevence. Je totiž mnohonásobně snazší a levnější malwaru zabránit v přístupu do počítače, než ho potom pracně a zpravidla s velkými nervy odstraňovat. Neplatí tedy, že pokud má uživatel nainstalovaný antivirový, nebo jiný specializovaný ochranný software, tak se počítači nemůže nic stát, to není dostatečná prevence.

Základní formou prevence je používání zdravého rozumu. Metoda je to nejúčinnější, velice jednoduchá, levná a spočívá v přemýšlení a neklikání myší na každou "blbost". Přesto je tato metoda pro mnoho uživatelů složitá a zcela nepochopitelná.

Důležité jsou také pravidelné aktualizace alespoň těch programů, které jsou nějak spojeny s používáním počítačové sítě nebo Internetu. Tyto programy mohou obsahovat chyby - bezpečnostní díry a pokud se objeví zrovna v části, která např. zajišťuje přístup do Internetu, může se najít vzdálený útočník - hacker, který chybu využije k získání kontroly nad počítačem uživatele.

Existují dvě cesty jak zajistit pravidelnou aktualizaci příslušného softwaru:

- povolit pravidelnou aktualizaci operačního systému Windows a jeho součástí (nabídka Start / Ovládací panely / Automatické aktualizace)
- pravidelně aktualizovat i další, běžně používané produkty, které by mohly být z Internetu zneužity (Mozilla Firefox, ICQ, DC++ apod.), nebo. v nich také přímo povolit automatickou aktualizaci.

Vhodné je také používat jiný internetový prohlížeč, než internet Explorer. Prohlížeče jako Mozilla Firefox nebo Opera jsou totiž více imunní. Hlavním důvodem je skutečnost, že Internet Explorer stále používá většina uživatelů a tak je havěť zaměřena právě proti Internet Exploreru.

Poslední součástí ochrany počítače je instalace specializovaného ochranného softwaru. Vzhledem k tomu, že až do nedávna představovaly nejvýznamnější hrozbu viry, představuje instalace antivirového programu základ. V poslední době však dochází k rozvoji i jiných forem malwaru v podobě spywaru, adwaru, spamu apod. Je tedy vhodné doplnit antivir také dalším ochranným softwarem v podobě firewallu, antispywaru apod.

4.1. Antivirové firmy

Hlavní náplní těchto specializovaných firem je vývoj a distribuce ochranného softwaru, technická podpora uživatelů jejich produktů a pomoc při odstraňování infekce způsobené škodlivým software. Kvalitní vývoj a testování ochranných programů je značně časově i organizačně náročný. Zejména udržování kvalitní databáze hrozeb, kde je důraz kladen na získávání nových druhů virů, červů, trojanů, spywaru apod. Existuje více způsobů, jak nové druhy malwaru získat, např. od uživatelů, nebo prostřednictvím technické spolupráce mezi firmami. Spolupráce mezi firmami se však neomezuje jen na výměnu vzorků možného malwaru, týká se i získávání dalších aktuálních informací, případně společného vývoje programového vybavení. Ukázalo se, že bez této spolupráce není efektivní vývoj antivirových programů možný.

Kromě vývoje nových produktů se firmy zabývají také jinými činnostmi. Mimo jiné zajišťují aktualizaci svých produktů a také sledují nové trendy v dané oblasti, snaží se předvídat budoucí kroky jak tvůrců virů, tak tvůrců konkurenčního ochranného software. Firmy zabývající se vývojem a produkcí ochranného softwaru jsou v dnešní době značně vytíženy a pod velkým tlakem, proto se jejich počet snižuje. Z těch, které na dnešním trhu fungují, lze jmenovat společnosti:

- Symantec – antivir Norton
- Lavasoft – antispyware Ad-Aware
- Crawler – antispyware Spyware Terminator
- Alwil – antivir Avast!
- AVG Technologies CZ – antivir AVG
- ESET – antivir NOD32

4.2. Testování ochranného software

Situace programů chránících počítač před některou z forem malwaru je velice specifická. Na rozdíl od jiných musí tento typ programů průběžně reagovat na aktuální výskyt nových forem malwaru a požadavky na něj jsou tak hůře definovatelné. Testování ochranného softwaru je tedy náročná a zdlouhavá činnost, při které se může vyskytnout několik problémů:

- Kvalita databáze hrozeb – její vytvoření, údržba, aktualizace, oddělení od ostatních souborů.
- Původ databáze hrozeb – jestliže je databáze nějak spojena určitým ochranným softwarem, může být ohrožena objektivita testu
- Zajištění srovnatelných podmínek testu pro různé programy
- Finanční náročnost testování
- A další

Za účelem dosažení objektivního výsledku testu by měl být proveden zápis. V něm by mělo být uvedeno:

- Konfigurace počítače, na kterém bylo testování prováděno
- Podrobná charakteristika testovací databáze hrozeb
- Popis způsobu vyhodnocení nejlepšího programu
- Přesná specifikace, základní charakteristika a stáří testované verze ochranného programu

Při testování programu jsou posuzovány jeho různé parametry. Zejména se jedná o úspěšnost při odhalování malwaru, rychlost kontroly počítače, množství falešných poplachů, ale také kvalita uživatelského rozhraní a snadnost používání. Na základě výsledků, které program v těchto parametrech dosáhl, je nakonec provedeno vyhodnocení.

4.3. Antivirové programy

Antivirový program, zkráceně antivir, je specializovaný program chránící počítač před hrozbou virů. Představuje jeden ze základních prvků ochranného software počítače. Antivir dokáže prohledat paměť i všechny soubory na pevném disku a najít přítomné viry.

Ty pak většinou dokáže odstranit bez poškození infikovaného souboru, v nejhorším případě je celý napadený soubor bezpečně a spolehlivě smazán.

Řada antivirových programů je rozšiřována bezplatně a lze si je za jistých podmínek stáhnout z Internetu, a to na stránkách výrobce, nebo na jiných odkazech (www.stahuj.cz, www.slunečnice.cz apod.).

4.3.1. Dělení antivirových programů

Antivirové programy lze dělit do několika skupin:

- Jednoúčelové antiviry - jedná se o antivirové programy, které jsou zaměřeny na detekci, popřípadě i dezinfekci jednoho konkrétního viru, popřípadě menší skupiny virů. Jednoúčelové antiviry rozhodně nelze použít jako plnohodnotnou antivirovou ochranu, jedná se o pouze o jakousi krabičku poslední záchrany. Pokud uživatel zjistí, že je jeho počítač infikován určitým virem, je nejjednodušší, pokud využije právě schopností jednoúčelového antiviru. Jednoúčelové antiviry jsou obvykle k dispozici zdarma a slouží k likvidaci pouze rozšířeného viru v dané době.
- On-demand skenery – většinou bývají jednou ze součástí antivirového systému, on-demand skener nicméně bývá nabízen některými AV společnostmi zdarma, popřípadě jako shareware. Obvykle jde o jednoduché verze pro OS DOS ovládané přes příkazový řádek. Tato kategorie antivirových programů se uplatní především při dezinfekci počítačů, kdy např. operační systém MS Windows není schopen provozu. Zajímavou alternativou jsou i on-line skenery dostupné na Internetu, které někteří výrobci antivirových programů nabízejí na svých stránkách. Obvykle jde o skript, který ve spojení s internetovým prohlížečem dokáže plnohodnotně prohledat pevný disk uživatele na výskyt virů, bez toho, aby tento antivirus získal fyzicky natrvalo.
- Antivirové systémy – v současnosti se jedná o nejčastější formu antivirových programů. Antivirový systém se skládá s částí, které sledují všechny nejpodstatnější vstupní/výstupní místa, kterými by případná infiltrace mohla do počítačového systému proniknout. Mezi tyto vstupní/výstupní místa může patřit například elektronická pošta (červi šířící se poštou), www stránky (škodlivé skripty, download infikovaných souborů), média (CD, diskety apod.). Nedílnou součástí

dnešních antivirových systémů je aktualizace prostřednictvím Internetu. Antivirové systémy představují komplexní antivirové řešení v některých případech doplněné i o osobní firewall. Do této kategorie patří takové produkty, jakými jsou: Avast!, AVG, Norton Antivirus, Kaspersky Antivirus, NOD32, McAfee ViruScan atd.

4.3.2. Techniky kontrol antivirových programů

Antivirový program využívá při kontrole počítače k odhalení viru několik technik využívajících různých principů kontroly:

- Skenování - při kontrole souboru antivirový program zjišťuje, zda se kód některé jeho části neshoduje s kódem některého ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má antivir následující možnosti:
  - pokusit se opravit nebo vyléčit soubor odstraněním viru ze souboru pokud je to technicky možné
  - umístit soubor do karantény kde se virus nemůže dále šířit, protože ho nelze dále používat
  - smazat infikovaný soubor i s virem

  Antivirové programy fungující na základě databáze virů kontrolují soubory v momentě, kdy je operační systém počítače vytvoří, otevře, zavře nebo je zasílá či přijímá e-mailem. V takovém případě je virus možné zjistit ihned po přijmutí souboru.
- Heuristická analýza – tato metoda kontroly souborů v nich nevyhledává typický kód viru a neporovnává ho s databází, ale provádí logickou analýzu kódu souboru vyhodnocováním jednotlivých instrukcí a posuzuje jejich praktický význam. Heuristická analýza zachycuje podezřelé činnosti programu, např. pokus o otevření a zápis do jiného spustitelného souboru. Každá taková podezřelá činnost může být charakterizována tzv. příznakem. Každý příznak je ohodnocen určitou vahou, a pokud kontrolovaný soubor součtem vah všech příznaků překročí určitou hranici, je tento soubor označen jako možná napadený virem. Heuristická analýza tedy vyhledává viry na základě činností souvisejících s reprodukcí či instalací viru, nebo jeho destrukční činností.

Výhodou této metody je možnost detekovat i dosud neznámý typ viru. Tato metoda hledání virů dokáže odhalit nejnovější a dosud neznámý vir, tedy i takový, který ještě není v databázi antivirového programu.
Nevýhodou heuristické analýzy je její nižší rychlost vzhledem k provádění mnohem složitějších operací. Další nevýhodou je vzhledem k jejímu principu i možnost mylného hlášení, neboť existují korektní programy, které jsou však napsány téměř stejně, jako počítačové viry. Takové programy mohou být heuristickou analýzou označeny jako napadené virem.

- Test integrity/kontrola změn – tato metoda využívá informace o souboru získané porovnáním s databází virů a heuristickou analýzou. Tyto informace jsou uloženy do databáze integrity. Pokud je u souboru při dalším testu zjištěna změna např. velikosti souboru, aniž by došlo k jeho aktualizaci, lze předpokládat, že může být infikován virem. Jedním ze způsobů využití této metody antivirem je, že zkontroluje soubory a všechny změněné soubory následně zkontroluje skenováním.
- Rezidentní štít – tato technika chrání počítač pře viry v reálném čase. Při startu počítače se automaticky do operační paměti počítače RAM umístí rezidentní štít antiviru a sleduje probíhající činnost. V případě pokusu o např. zápis do systémové oblasti disku, nebo modifikaci souborů s příponou EXE, COM antivirový program uživatele na tuto skutečnost upozorní.
- Sandbox - neboli pískovištěm je metoda která napodobuje operační systém a spouští .exe soubory v jakési simulaci. Po ukončení testovaného programu antivirový program analyzuje sandbox, pro zjištění případných změn, které by mohly ukázat možnou přítomnost virů.

Dnešní antivirové programy využívají kombinaci několika výše uvedených metod hledání virů. Jediná metoda není stoprocentně účinná, ale využití kombinace těchto metod minimalizuje riziko napadení uživatelova počítače virem.

4.3.3. Aktualizace antivirového systému

Aby antivirový program správně fungoval, jsou potřeba jeho pravidelné aktualizace. Šíření nových virů, červů a ostatní havěti je dnes díky Internetu natolik rychlé, že antivirový systém nemůže klasickou metodou detekce pomocí vyhledávání známé infiltrace zareagovat včas.

Pro zajištění efektivní aktualizace je potřeba zajistit:

- rychlá reakce ze strany AV společnosti
- správné nastavení části antivirového programu, stahující aktualizace na straně uživatele.

Antivirové společnosti se snaží zajistit co možná nejrychlejší proces stahování aktualizace. Rychlost ovlivňuje nepochybně velikost aktualizace.

Metodou, jak snížit velikost aktualizace je její rozdělení na dvě nezávislé části:

- aktualizace programové části antivirového systému. Tato aktualizace odstraňuje nedostatky v programové části antiviru, popřípadě tuto část rozšiřuje o nové funkce.
- aktualizace virové databáze. Tato aktualizace zajišťuje detekci nových virů, popřípadě upravuje detekci těch stávajících.

To jakým způsobem se virové databáze aktualizují, je závislé na konkrétním antiviru.

Obecně existují dva způsoby:

- Plná aktualizace, kdy se pokaždé stahuje celá virová databáze znovu. Tento typ aktualizace je časově více náročný s rostoucím množstvím známých virů. Velikost každé takové aktualizace lze obvykle měřit na MB. AV společnosti se tak snaží tomuto způsobu aktualizace vyhnout
- Přírůstkové aktualizace, kdy se stahují pouze ty části virové databáze, které na serveru výrobce přibyly od poslední aktualizace provedené uživatelem. Dochází tak ke stáhnutí pouze těch informací, které se v uživatelově počítači dosud nevyskytují. Pozitivem je zároveň i rychlost a velikost aktualizací.

4.3.4. Virová databáze

Virová databáze představuje klíčovou součást antivirového programu, obsahuje informace nutné k detekci známých virů antivirovým skenerem. Virová databáze se obvykle označuje datem vydání. Na základě informací z virové databáze dokáže antivirový skener detekovat většinu známých virů, které vznikly před datem vydání virové databáze.

Pravidelnou aktualizací lze zajistit, že rozdíl mezi současným datem a datem vydání bude co nejmenší a budou tak detekovány i nejnovější přírůstky mezi viry.

4.3.5. Antivirové skenery

Antivirové skenery jsou nejstarší součástí každého antiviru. Umožňují provádět proces skenování, během kterého jsou vyhledávány počítačové viry na základě informací z virové databáze. Pokud virová databáze informace o daném viru neobsahuje, „obyčejný“ skener ho nedokáže detekovat. Proto postupem času vznikly metody detekce, které dokážou odhalit i doposud neznámé viry a tohoto nedostatku se tak částečně zbavit.

Skenery lze rozdělit na dvě hlavní skupiny:

- on-demand - viry vyhledává až po vydání požadavku uživatelem (proto on-demand). Požadavek je často vydáván manuálně, obvykle vybráním požadované oblasti pro test (adresáře, pevný disk, disketa atd.) a stiskem tlačítka *start* v antivirovém programu. Některé on-demand skenery je možné aktivovat na základě plánovače (scheduler) v časovém období, které předem definuje uživatel, např. každý den v 14:00.
- on-access - zcela automaticky a neustále vyhledává viry v datech, nejčastěji v souborech, se kterými přichází uživatel do styku.

Kromě skenerů se antivirové systémy skládají z dalších více či méně běžných částí:

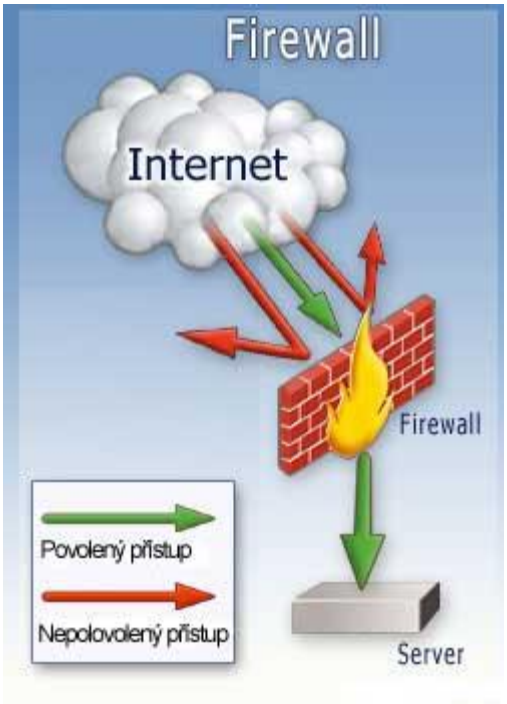
- udržujících antivirový systém v aktuální podobě. Zajišťují stahování aktualizací antivirového systému z Internetu.
- vykonávajících automatickou antivirovou kontrolu příchozí a odchozí elektronické pošty.
- plánovače událostí (scheduleru), který umožňuje ve zvoleném termínu automaticky vyvolat naplánovanou úlohu, např. antivirovou kontrolu důležitých dokumentů.
- karantény
- monitorovacích programů
- antivirový spořič obrazovky
- osobního firewallu nebo antispamu - takový produkt je nazýván jako bezpečnostní balík “Internet Security” apod.

Nutným minimem, kterým by měl disponovat každý antivirový systém, je on-access skener a část udržující antivirový systém v aktuální podobě Pokud antivirový systém tyto části neobsahuje, je bezpečnější takovýto antivirový program nepoužívat.

4.4. Firewall

Firewall představuje další prvek ochranného software počítače připojeného k počítačové síti. Úkolem firewallu je řízení, kontrola a filtrování komunikace mezi vlastním počítačem a vnější počítačovou sítí, především Internetem. Vlastní komunikace probíhá na základě přenosu síťových paketů.

Činnost firewallu je založena na souboru pravidel, která řídí komunikaci z počítače směrem ven, soustřeďuje ji do jednoho uzlu, odfiltrovává nebezpečné služby, blokuje nepřátelské monitorování sítě apod. Prostřednictvím firewallu tak lze přesně určit, co má do počítače přístup a co ne a ochránit tak počítač před útokem hackerů, před viry a červy. Moderní firewally také umožňují sledovat odchozí komunikaci a chrání tak počítač před trojskými koňmi a aplikacemi, které odesílají získaná data zpět svým tvůrcům.



obrázek č. 4 - Schéma funkce firewallu [12]

Komunikace mezi počítačem a vnější sítí probíhá přes porty. Celkem je k dispozici 65535 portů, přes které je možné vést útok. Jednou z možností, jak se může osoba, počítačový virus nebo jiný počítač, nabourat do uživatelova počítače, je najít odpovídající port, který bude při útoku a případné pozdější komunikaci využívat. Pomocí skenování portů pak zjišťuje, jaké služby na nich běží a pokud najde nějakou službu s bezpečnostní dírou, může útok provést.

Čísla některých portů a služby, které je standardně využívají:

- FTP (přenos souborů): 20, 21
- HTTP (www stránky): 80
- POP (elektronická pošta): 110
- IMAP3 (elektronická pošta): 220
- ICQ: 4000

Takovýmto pokusům o skenování portů a o průnik bývá počítač vystaven zpravidla okamžitě po připojení k síti. Firewall má proto za úkol kontrolovat všechny porty a komunikaci na nich probíhající. Tu vyhodnocuje podle pravidel, jež má nastaveny a rozhoduje, zda je komunikace vyhovující či nevyhovující. Tato pravidla vždy zahrnovala minimálně identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port. Pokud firewall narazí na nějaké pokusy o proniknutí, pokouší se je odrazit a nepustit je dovnitř počítače.

Současné firewally však nemusí plnit jen základní funkci ochrany před únikem dat či napadením počítače. Moderní firewall představuje komplexní řešení v oblastech připojení k Internetu, antivirové ochrany, optimalizace připojení, problémů s IP, přístupových práv uživatelů, zabezpečené komunikace, sdílení přístupu k internetu apod.

4.4.1. Kategorie firewallů

Firewally se během svého vývoje řadily zhruba do následujících kategorií:

- Paketové filtry - nejjednodušší a nejstarší forma firewallu. Jejich činnost spočívá v tom, že vyhodnocují jednotlivé pakety podle informací obsažených v hlavičce (IP adresa odesílatele i příjemce, zdrojový i cílový port a další informace). Firewall

tyto informace vyhodnotí a na základě přesně stanovených pravidel rozhodne, zda přenos paketu bude povolen, nebo naopak zamítnut. Pravidla uvádějí z jaké adresy a portu a na jakou adresu a port může být procházející paket doručen. Výhodou tohoto řešení je vysoká rychlost zpracování, proto se ještě i dnes používají na místech, kde není potřebná přesnost nebo důkladnější analýza procházejících dat, ale spíš jde o vysokorychlostní přenosy velkých množství dat. Nevýhodou je nemožnost kontroly obsahu přenášených paketů.

obrázek č. 5 - Schéma funkce paketového filtru [13]

- Aplikační brány - poněkud mladší forma firewallu, na rozdíl od paketových filtrů zcela oddělují sítě, mezi které byly postaveny. Někdy jsou také označovány jako Proxy firewally. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Vedlejším efektem použití aplikační brány je, že server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT). Výhodou aplikačních bran je poměrně vysoká míra zabezpečení známých protokolů. Naopak nevýhodou je zejména vysoká náročnost na použitý HW – aplikační brány jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti, než paketové filtry.

- Stavové paketové filtry - **s**tavové paketové filtry kontrolují komunikaci stejně jako normální paketové filtry, navíc si však ukládají informace o povolených spojeních. Ty jsou následně použity při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody – urychluje se tak zpracování paketů již povolených spojení, případně lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá.

  Výhodou stavových paketových filtrů je jejich vysoká rychlost, poměrně slušná úroveň zabezpečení a ve srovnání s aplikačními branami a jednoduchými paketovými filtry i mnohonásobně snazší konfigurace. Z jednodušší konfigurace vyplývá i nižší pravděpodobnost chybného nastavení pravidel obsluhou. Nevýhodou je poněkud nižší bezpečnost, než jakou poskytují aplikační brány.

- Stavové paketové filtry s kontrolou protokolů a IDS - moderní stavové paketové filtry jsou schopny kontrolovat procházející spojení a korektnost přenášených dat známých protokolů i aplikací. Pokud objeví známky toho, že se nejedná o požadavek na WWW server, mohou takové spojení. Kromě toho se do moderních firewallů integrují funkce tzv. in-line IDS (Intrusion Detection Systems – systémy pro detekci útoků). Tyto systémy jsou podobně jako antiviry za pomocí databáze signatur a heuristické analýzy schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

  Výhodou tohoto typu firewallů je vysoká úroveň bezpečnosti kontroly procházejících protokolů, snadná konfigurace a poměrně vysoká rychlost kontroly ve srovnání s aplikačními branami. Proti stavovým paketovým filtrům jsou však stále zhruba o třetinu až polovinu pomalejší.

  Nevýhodou je zejména možnost výskytu zneužitelné chyby v kódu firewallu vzhledem k jeho složitosti.

4.5. Antispyware

Antispyware je specializovaný program, jehož úkolem je odstraňovat či blokovat spyware, který se bez uživatelova vědomí natáhl do jeho počítače. Protože se však nejedná přímo o viry, přítomnost spywaru v počítači antivirový program zpravidla neodhalí. Dřívější verze antispyware programů se soustředily pouze na detekci a odstraňování současné verze však kromě toho umí odstraňovat i jiné formy malwaru, např. viry.

Se spywarem lze bojovat dvěma způsoby:

- Antispyware programy mohou poskytovat ochranu proti instalaci spywaru do počítače v reálném čase. Tento typ antispywarové ochrany pracuje na stejném způsobu jako realtime ochrana v antivirovém programu - antispyware prohlíží všechna data příchozí ze sítě a v případě objevení podezřelých dat je zablokuje a nepustí do počítače.
- Antispyware programy mohou být použity výhradně pro detekci a odstranění spywaru, který již byl do počítače nainstalován. Tento typ antispywarové ochrany je mnohem jednodušší na použití a také více populární. Program zkontroluje registr a složky operačního systému a nainstalované programy a po provedení kontroly poskytne seznam všech hrozeb, které nalezl. Uživatel si tak může zvolit, které nalezené objekty si chce nechat a které chce naopak smazat.

Jako většina antivirového softwaru, mnoho antispyware programů pro svou správnou a kvalitní funkci vyžaduje často aktualizovanou databázi hrozeb. Tak jak je nový spyware vypouštěn do světa, jsou výrobci antispyware programů tyto hrozby zkoumány a jsou vytvářeny jejich signatury. Na jejich základě je potom spyware antispywarovými programy odhalován a odstraňován. Ve výsledku je tedy antispyware program bez pravidelných aktualizací k ničemu. Někteří tvůrci těchto programů poskytují jejich aktualizace pouze registrovaným uživatelům, někteří je však poskytují zdarma. Aktualizace mohou být prováděny automaticky na základě naplánovaného rozvrhu před provedením kontroly, nebo mohou být provedeny uživatelem ručně.

Ne všechny antispyware programy se spoléhají na aktualizace, některé programy částečně nebo zcela spoléhají na minulá pozorování. Sledují současné konfigurační parametry počítače, a pokud je provedena jakákoliv změna, ohlásí ji uživateli. Protože tyto

programy nejsou závislé na aktualizacích, které by jim umožnily všimnout si nového spywaru, nemohou zároveň poskytnout žádnou radu, co s možným spywarem provést. Uživateli je tak ponecháno rozhodnutí, jestli to co udělal je správné a změna konfigurace PC vhodná.

5. Ochrana počítače pod OS

V této práci bylo hodnoceno několik vybraných zástupců programů používaných k zajištění ochrany počítače před hrozbou malwaru. Hodnoceny byly antivirové programy, antispywarové programy a firewally.

Pro testování byl použit počítač pracující pod operačním systémem Windows XP Professional service pack 2, s procesorem AMD Athlon 64 X2 Dual Core na frekvenci 1,58 GHz. Počítač dále pracoval s operační pamětí 2 GB RAM, pevný disk o kapacitě 160 GB obsahoval 90 GB dat.

5.1. Antivirové programy

Z antivirů byly testovány programy:

- AVG 9 Free Edition
- AVAST! Free antivirus
- ESET NOD32

5.1.1. AVG 9 Free Edition

AVG 9 Free Edition je softwarový nástroj na ochranu počítače před viry, červy, trojskými koni a spywarem. Umí však také kontrolovat příchozí elektronickou poštu.

Tvůrcem programu je společnost AVG Technologies CZ. Pro nekomerční využití je AVG Free Edition distribuován jako freeware, v domácnosti a pro nekomerční využití ho tedy uživatel může používat zcela zdarma. Velikost stahovaného souboru je cca 85 MB. Free verzi AVG 9 je možno stáhnout buď přímo na stránkách free.avg.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 9.0.800.

AVG 9 Free Edition lze využívat pod operačními systémy Windows Vista 32bit a 64bit, Windows XP, Windows 2000 a Windows 7.[14] Existuje i veze pro operační systém Linux.

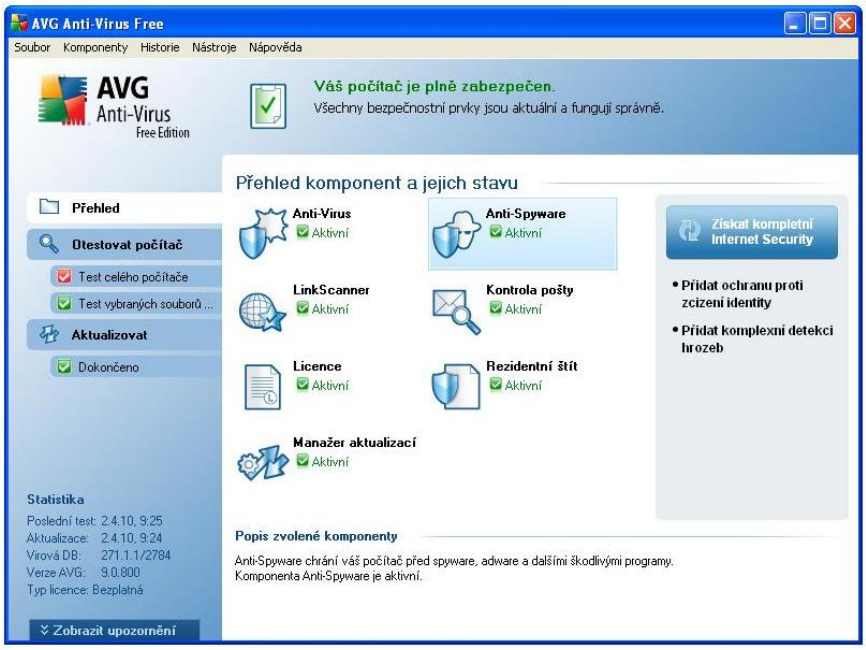
Přestože se jedná o free, a tedy poněkud „okleštěnou“ verzi, program obsahuje rezidentní štít, kontrolu pošty a antispyware. Stěžejní je však podle výrobce funkce LinkScanner. Tato funkce se skládá ze dvou částí:

- AVG Active Surf-Shield – zajišťuje kontrolu všech webových stránek na škodlivý obsah dříve, než jsou uživatelem navštíveny
- AVG Search-Shield - testuje každý jednotlivý odkaz vygenerovaný u vyhledavačů Google, MSN a Yahoo! a zobrazuje jejich bezpečnostní hodnocení, funguje jako doplněk prohlížečů Internet Explorer a Mozilla Firefox

Funkce *Kontrola pošty* potom hlídá poštovního klienta před nebezpečnými přílohami a odkazy v příchozí poště. Nechybí samozřejmě rezidentní štít, který testuje všechny otevírané, kopírované a ukládané soubory a kontroluje systémové oblasti počítače na přítomnost různých druhů nebezpečného kódu.

Instalace programu trvá poněkud déle, probíhá ale bez problému. AVG dokonce uživatele upozorní, pokud již má nějaký antivir nainstalovaný, čímž by mohly vzniknout konflikty. Jakmile je instalace hotová, program se při prvním spuštění uživatele zeptá, zda chce provést optimalizaci rychlosti testů. Vytváří se tak databáze známých důvěryhodných souborů, kterou program při kontrole počítače používá a rychlost kontroly počítače by se tak měla výrazně zvýšit.

Uživatelské rozhraní programu je jednoduché a přehledné, graficky dobře zpracované. Vzhledem k tomu, že pochází od české firmy, je celý program plně lokalizován do češtiny. S jeho ovládáním by neměli mít problém ani uživatelé-začátečníci. Hlavní okno programu v záložce *Přehled* obsahuje informace o aktivních funkcích programu, v dalších záložkách uživatel může provést kontrolu počítače nebo aktualizaci programu.



obrázek č. 6 - Úvodní okno AVG antiviru

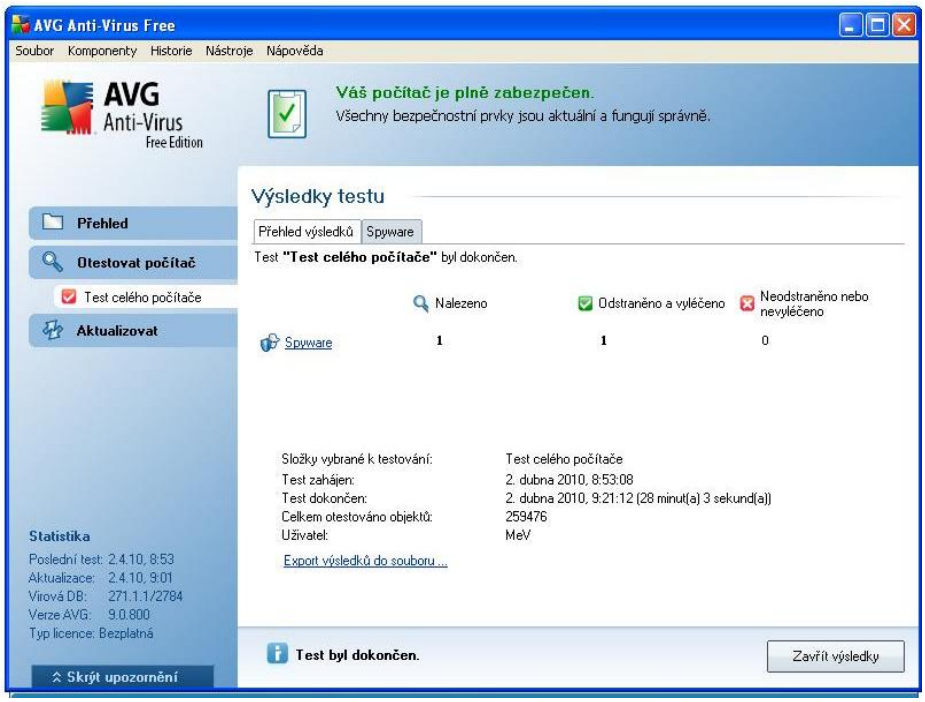
Záložka *Kontrola* nabízí na výběr dva možné typy kontroly:

- Test celého počítače – kontroluje všechny infikovatelné soubory ve všech složkách a souborech na všech místních discích, systémové oblasti a paměť počítače a na přítomnost virů, spywaru, červů apod.
- Test vybraných souborů či složek – kontroluje infikovatelné soubory a archivy na vybraných discích, případně složkách na přítomnost virů, spywaru, červů apod.

U obou typů testů lze dále nastavit, zda má být proveden *Pomalý*, *Automatický* nebo *Rychlý* test. Jednotlivé možnosti se liší podle úrovně vytížení systémových prostředků počítače a z toho vyplývající rychlosti provedení.

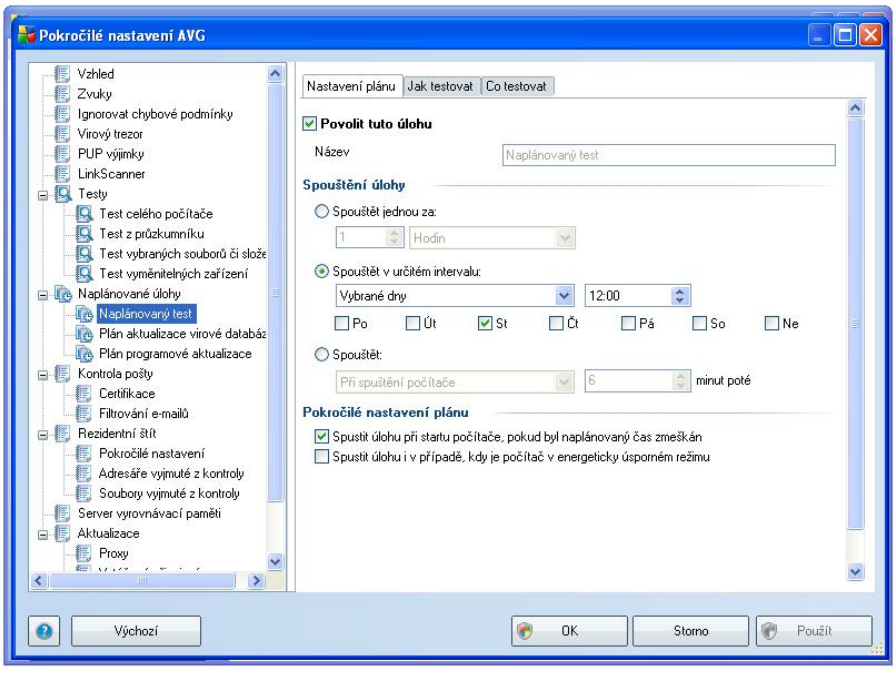
Test celého testovaného počítače v případě jeho automatické varianty trval 28min 3s a procesor byl vytížen v průměru na 70%.

Po skončení kontroly AVG zobrazí přehlednou statistiku. Napadený soubor se AVG automaticky pokusí vyléčit, případně odstranit, pokud se mu to však nepovede, přesune napadený soubor do karantény-virového trezoru.



obrázek č. 7 - Výsledek antivirového testu počítače

AVG 9 Free Edition také umožňuje široké možnosti přizpůsobení programu podle požadavků uživatele. Nastavení je celé v češtině a přehledné. Umožňuje přizpůsobit např. nastavení kontroly počítače a kontroly pošty, naplánování budoucích kontrol počítače nebo nastavení rezidentního štítu a jiná nastavení.



obrázek č. 8 - Nastavení plánu kontrol

5.1.2. ESET NOD 32

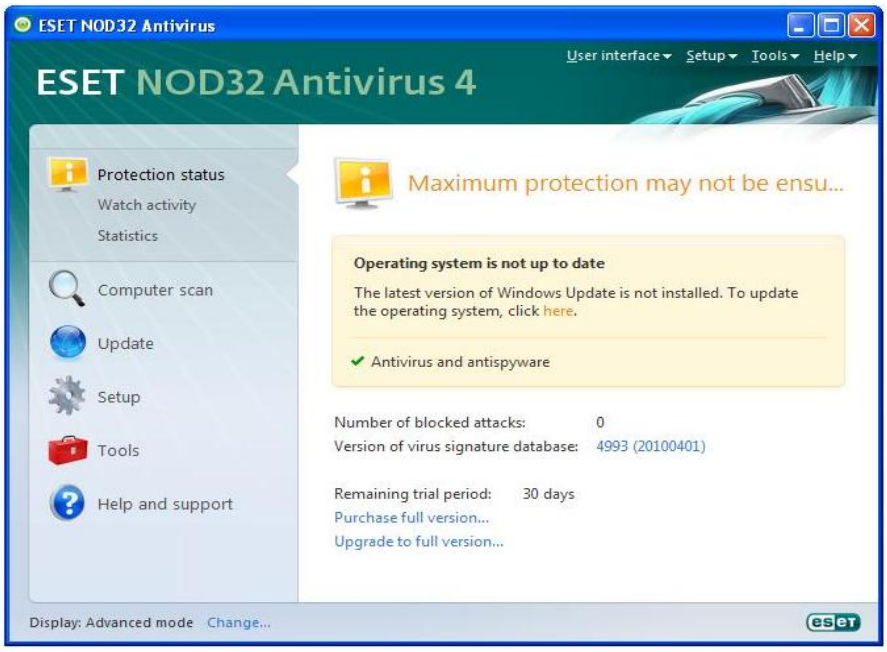
ESET NOD32 Antivirus, také známý jednoduše jako NOD32, je antivirový program zajišťující ochranu počítače před viry, trojskými koňmi a červy. Kromě toho však počítač chrání i před spyware a adware.

Tvůrcem NODu je slovenská společnost ESET. Uživatel si musí NOD 32 koupit, není to freeware. Program je ale možné na 30 dnů bezplatně vyzkoušet, poté je ho potřeba upgradovat na plnou verzi, nebo přestat používat. Velikost stahovaného souboru je cca 35 MB. Zkušební verzi NOD32 je možno stáhnout buď přímo na stránkách www.eset.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 4.0.468.

ESET NOD32 Antivirus lze využívat pod operačními systémy Windows Vista 32bit, Windows XP, Windows 2000 a Windows 7.[15]

Instalace probíhá rychle, neměl by se vyskytnout žádný problém, program uživatele dokonce upozorní, pokud již má nějaký antivir nainstalovaný, čímž by mohly vzniknout konflikty.

Uživatelské rozhraní programu je jednoduché a přehledné, graficky dobře zpracované. K dispozici je i česká lokalizace, přepnout program do češtiny se mi však přes veškerou snahu nepodařilo. Záložka *Stav ochrany* uživatele informuje o aktivních typech ochran, množství zachycených hrozeb, verzi nainstalované virové databáze a v případě testovací verze i zbývající době bezplatného zkušebního provozu.



obrázek č. 9 - Úvodní okno ESET NOD 32

Záložka *Kontrola počítače* nabízí dva možné typy kontroly počítače:

- Chytrá kontrola – provádí hloubkovou kontrolu počítače, s výjimkou e-mailů a archivů kontroluje všechny soubory na pevném disku, automaticky léčí nebo maže odhalený škodlivý software
- Volitelná kontrola – uživatel si může zvolit cíl a typ prováděné kontroly

Vlastní kontrola počítače trvala poměrně dlouho, u testovaného počítače to byla 1h a 23min, procesor byl vytížen v průměru na 50%.

Na konci kontroly se objeví okno se zobrazenými výsledky – s počtem zkontrolovaných, napadených a odstraněných objektů. Napadené objekty odstraňuje NOD32 sám, uživateli dá na výběr z možných operací, pouze pokud se mu nepodaří provést standardní akci.

obrázek č. 10 - Výsledek volitelné kontroly

Kromě on-demand scanneru obsahuje NOD32 i několik rezidentních štítů, z nichž každý chrání počítač před infekcí jiným typem viru:

- AMON - Antivirus MONitor, kontroluje soubory tak, jak jsou zpřístupněná systémem, provádí ochranu systému před viry
- DMON - Document MONitor, prohlíží dokumenty kancelářského balíku Microsoft Office a další soubory proti makrovirům
- IMON - Internet MONitor, přeruší průběh výměny dat se serverem u běžných protokolů pošty a internetu jako jsou POP3 a HTTP, dříve než je zjištěný a zachycený virus uložen na disk.
- EMON - E-mail MONitor, pomocný modul pro kontrolu příchozích/odchozích e-mailů přes MAPI rozhraní používané Microsoft Outlook a Microsoft Exchange Client
- XMON - MS eXchange MONitor, skenuje příchozí a odchozí poštu v momentě, kdy NOD32 běží pro licencovaný Microsoft Exchange Server - ie, ale funguje pouze v serverovém prostředí. Tento modul není součástí edice pro samostatné pracovní stanice.

NOD 32 umožňuje i několik možnosti nastavení, mj. nastavit automatické provádění dalších kontrol, odpojení rezidentních štítů apod.

5.1.3. Avast! Free Antivirus

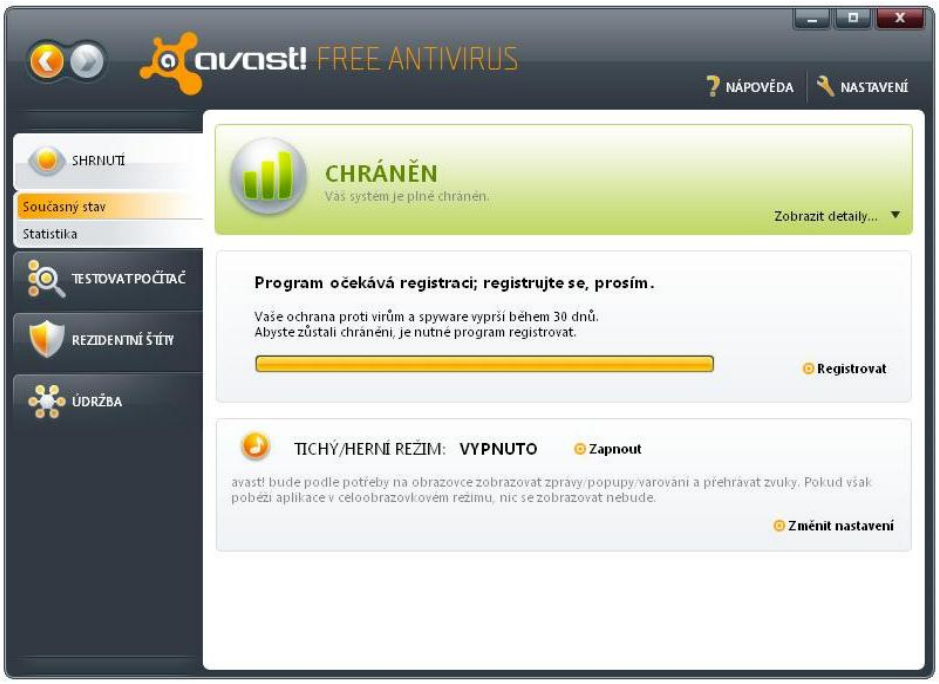
Avast! Free Antivirus je specializovaný nástroj na ochranu počítače virovou, spywarovou nebo jinou malware nákazou.

Tvůrcem programu je společnost ALWIL Software. Pro nekomerční využití je Avast! distribuován jako freeware, uživatel ho tedy doma a pro nekomerční využití může bezplatně používat 30 dnů. Během této doby by se měl uživatel zdarma zaregistrovat na stránkách výrobce, odkud e-mailem obdrží aktivační kód s platností 1 roku. Po uplynutí této doby si uživatel nechá vygenerovat nový kód a může opět pokračovat v legálním užívání programu. Registrace také zajistí, že program bude stahovat aktualizace virových definic, a bude Vás tak chránit proti nejnovějším hrozbám. Velikost stahovaného souboru je cca 40 MB. Avast! Free Antivirus je možno stáhnout buď přímo na stránkách www.awast.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 5.0.462.[16]

Avast! Free Antivirus lze využívat pod operačními systémy Windows Vista 32bit a 64bit, Windows XP, Windows 2003, Windows 2008 a Windows 7.

Instalace Avastu probíhá velmi rychle a bez problémů. Uživatelské rozhraní programu je jednoduché a přehledné, graficky dobře zpracované. Celý program je plně lokalizován do češtiny a s jeho ovládáním by neměl mít problém žádný uživatel.

Po spuštění Avastu si uživatel může prohlédnout informace o stavu ochrany systému, o počtu dní zbývajících do registrace, případně spustit tichý režim. V záložce *Testovat počítač* si lze vybrat z několika variant kontroly a v záložce *Rezidentní štíty* se zobrazují informace o jednotlivých částech rezidentního štítu. Ručně aktualizovat program lze v záložce *Údržba*.

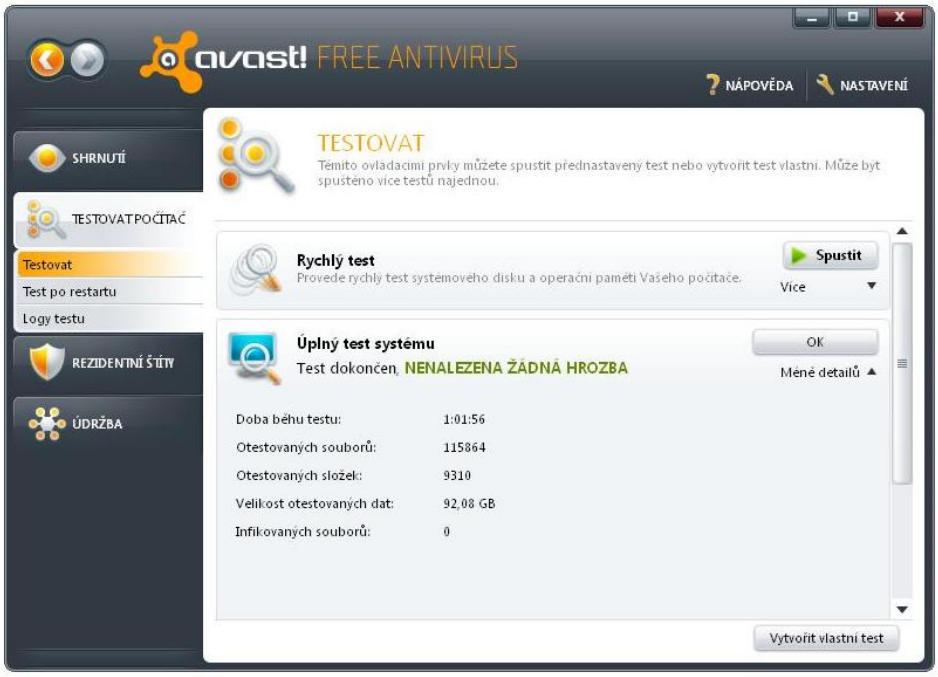


obrázek č. 11 - Úvodní okno Avast! Free Antivirus

Záložka *Testovat počítač* nabízí na výběr z několika možných typů kontroly:

- Rychlý test - provede rychlý test operační paměti a systémového disku (obvykle disku C:\, testovány jsou pouze začátky a konce spustitelných souborů, tedy části, kde se většinou nachází infekce
- Úplný test systému – provede podrobný test všech pevných disků, kontrolovány jsou všechny soubory v závislosti na jejich obsahu
- Test výměnných médií - otestuje všechna přenosná média aktuálně připojená k počítači, např. USB paměti, externí pevné disky apod. Kontroluje se přítomnost autorun programů, které by se mohly při připojení média spustit.
- Test vybraných souborů či složek – kontroluje infikovatelné soubory a archivy na vybraných discích, případně složkách na přítomnost virů, spywaru, červů apod.
- Zvolit složku k testování – provede úplný test určené složky

Doba trvání kontroly samozřejmě závisí na jejím typu a na množství dat uložených v počítači. U testovaného počítače trval Rychlý test 18min 14s při průměrném vytížení CPU na 30%, Úplný test systému trval 61min 56s při průměrném vytížení CPU na 25%.



obrázek č. 12 - Výsledek úplného testu systému

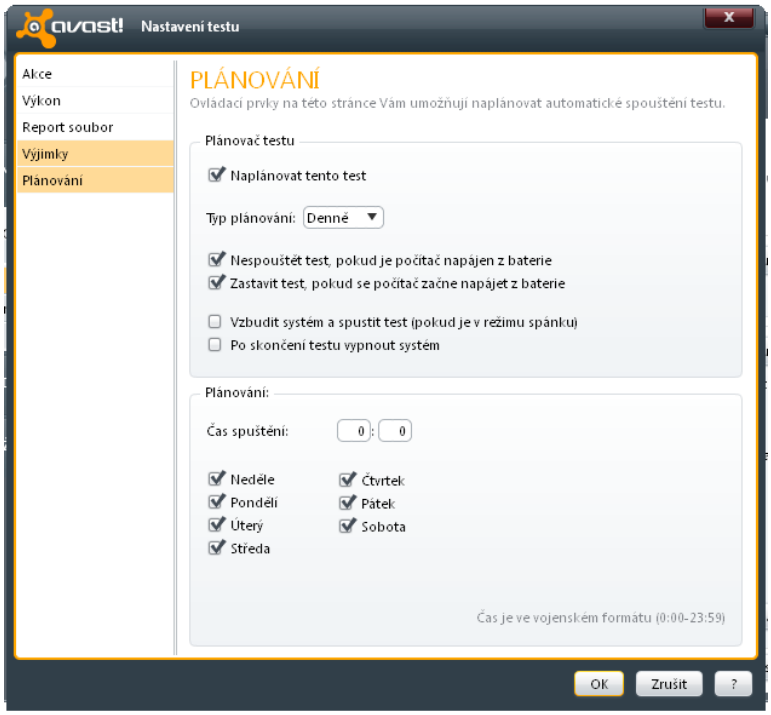
Na konci kontroly se zobrazí informace o provedeném testu – doba trvání, počet otestovaných souborů a složek, velikost otestovaných dat a případně počet infikovaných objektů. Pokud je nalezen virus nebo jiný malware, zobrazí se ve spodní části okna zpráva "Nalezen virus". Pro zobrazení informace o detekovaném viru je třeba klepnout na tlačítko *Zobrazit výsledky*. Na stránce *Výsledky testu* lze také stanovit, jaké další akce má Avast s napadeným souborem provést, jestliže se mu nepovedlo provést přednastavenou akci.

Důležitou součástí programu je i rezidentní štít, chránící nepřetržitě počítač proti infekci. Rezidentní štít Avastu se skládá z několika částí:

- Štít souborového systému - kontroluje programy při spouštění a ostatní soubory při otevírání a zavírání. Pokud jsou zjištěny infikované soubory, štít souborového systému je zablokuje a zabrání jejich otevření nebo spuštění.
- Mailový štít - kontroluje příchozí a odchozí emailové zprávy a zastaví všechny, které by mohly obsahovat virovou infekci.
- Webový štít - chrání počítač před viry šířícími se po Internetu, detekuje a blokuje známé nebo potencionální hrozby z webových stránek. Pokud je detekován virus při stahování souboru z Internetu, stahování je přerušeno.

- P2P štít - kontroluje soubory stahované pomocí běžných programů na sdílení souborů
- IM štít - kontroluje soubory stahované chatovacími nebo IM programy.
- Síťový štít - kontroluje veškerou síťovou aktivitu a blokuje hrozby detekované v síti, blokuje přístup ke známým škodlivým webovým stránkám.
- Behaviorální štít - hlídá všechnu aktivitu v počítači a detekuje a blokuje jakoukoliv neobvyklou aktivitu, která by mohla naznačovat přítomnost malware.

Avast rovněž umožňuje provést přizpůsobení programu podle požadavků uživatele, např. naplánování budoucích kontrol, nebo nastavení aktualizací. Tyto možnosti lze však u dnešních programů považovat za standardní.



obrázek č. 13 - Nastavení plánu kontrol v Avastu

5.1.4. Vyhodnocení antivirových programů

Pro vyhodnocení testovaných antivirových programů a výběr nejvhodnějšího byla použita následující hodnotící kritéria:

- doba trvání kontroly
- zatížení procesoru v průběhu kontroly

- kvalita uživatelského rozhraní
- kvalita programu podle testu AV Comparatives

Pro srovnání programů podle prvního zmíněného kritéria byla u programu AVG použita doba trvání *Testu celého počítače*, u programu NOD32 doba trvání *Chytré kontroly* a u Avastu doba trvání *Úplného testu systému*.

U každého ze sledovaných kritérií byly testované programy ohodnoceny, rozsah hodnocení je 1 – 5. Význam hodnocení je stejný jako ve škole, 1- výborně, 5 – nedostatečně. Každé z hodnotících kritérií také má svou váhu v rámci celkového hodnocení. Hodnocení testovaných programů a váha jednotlivých kritérií na celkové hodnocení jsou uvedeny v tabulce.

	Váha hodnocení (%)	AVG	AVAST	NOD32
Doba trvání kontroly	30	1	3	2
Zatížení CPU	20	3	2	1
Kvalita uživatelského rozhraní	30	1	2	2
Bezpečnost dle AVC	20	1	1	2
	Celkové hodnocení	0,35	0,525	0,45

obrázek č. 14 - Tabulka vyhodnocení antivirů

Výsledek je tvořen váženým průměrem všech hodnocení daného programu. Za nejlepší je považován program s nejnižším ohodnocením. Z testovaných antivirových programů tak lze za nejlepší považovat program AVG Free Edition s hodnocením 0,35.

5.2. Antispyware

Z antispywarových programů byly testovány:

- Spyware Terminator
- Spybot Search&Destroy
- Ad-Aware 2009 Free Edition

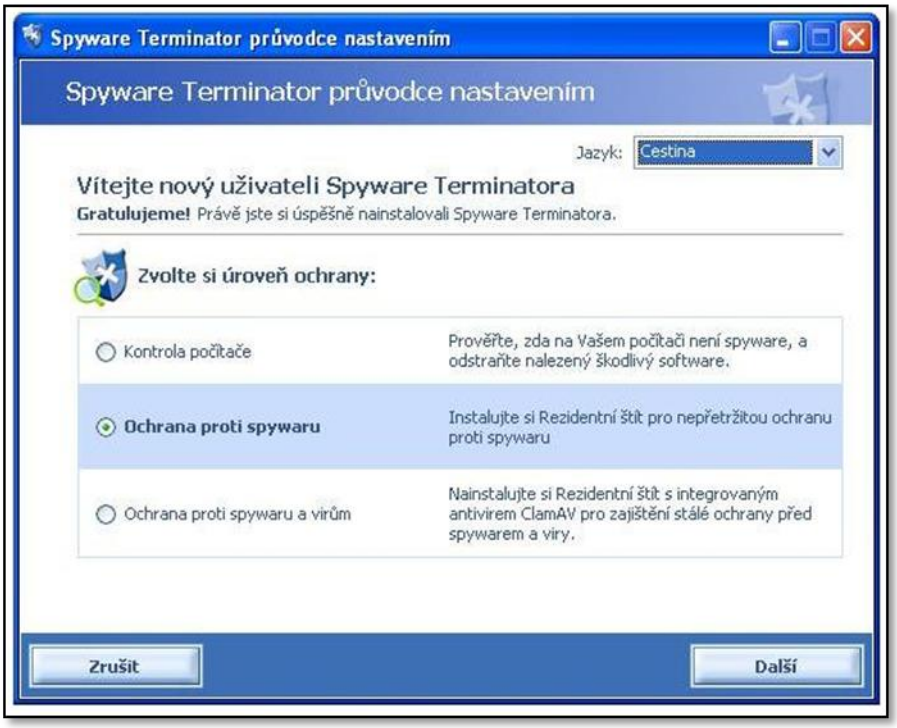
5.2.1. Spyware terminator

Spyware Terminator je softwarový nástroj na vyhledávání a odstraňování spywaru z počítače. Kromě spywaru si však dokáže poradit i s adwarem, trojskými koni a některými dalšími formami malwaru.

Tvůrcem programu je společnost Crawler LLC. Program je freeware a uživatel ho tedy může využívat zdarma. Velikost stahovaného souboru je cca 640kB. Spyware Terminator je možno stáhnout buď přímo na stránkách www.spywareterminator.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 2.6.6.196.

Spyware Terminator lze využívat pod operačními systémy Windows Vista 32bit, Windows XP, Windows 2000 a 2003 a Windows 7.

Instalace programu trvá asi 5min a neměl by se při ní vyskytnout žádný problém. Při prvním spuštění programu uživatele uvítá jednoduchý průvodce, ve kterém si může nastavit jazyk včetně češtiny a jak hodlá program používat.



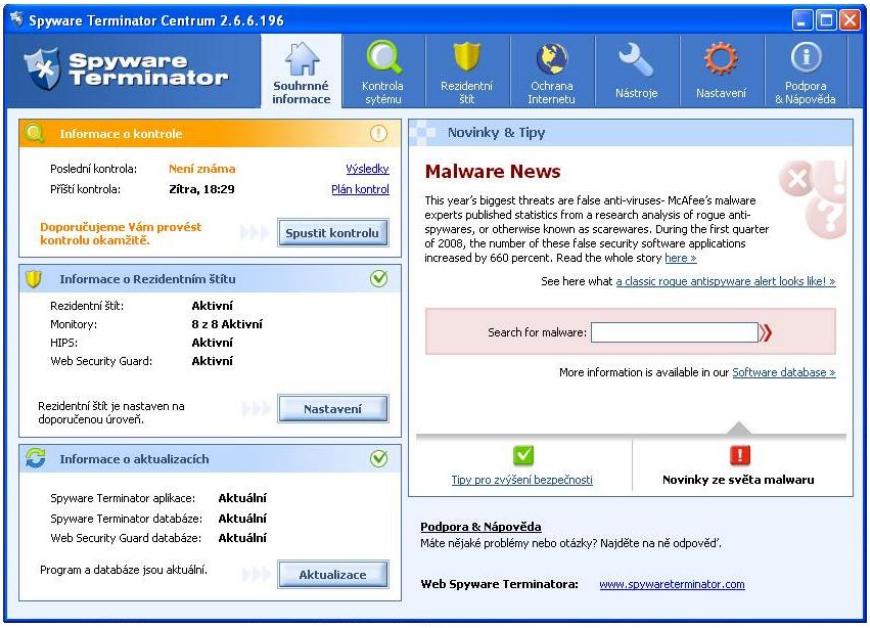
obrázek č. 15 - Možnosti instalace Spyware Terminatora

K dispozici jsou možnosti:

- Spyware skener – pokud chce uživatel program používat pouze na kontrolu a odstranění havěti z počítače
- Ochrana před spyware – Spyware Terminator spustí rezidentní štít běžící na pozadí a bude tak chránit počítač pře spywarem v reálném čase.

- Ochrana před spyware a viry – do rezidentního štítu se navíc stáhne štít antiviru Clam, který bude počítač chránit také před viry. K využití zejména pokud uživatel nemá nainstalovaný antivirový program.

Uživatelské rozhraní programu je jednoduché, přehledné, v češtině a s ovládáním by neměli mít potíže ani uživatelé-začátečníci. Hlavní okno programu obsahuje informace o kontrole počítače, včetně možnosti jejího okamžitého spuštění, informace o rezidentním štítu a informace o aktualizacích.



obrázek č. 16 - Hlavní okno Spyware Terminatora

Nejčastěji je zřejmě využívána záložka *Kontrola Systému*, kde si uživatel může zvolit úroveň kontroly. K dispozici jsou možnosti:

- Rychlá kontrola - prohlíží důležité části systému (běžící procesy, knihovny, služby, NHO, start sekci registru, cookies apod.)

- Kompletní kontrola - hloubková kompletní analýza počítače na přítomnost spywaru
- Virová a spywarová - kompletní analýza včetně vyhledávání virů pomocí ClamAV antiviru
- Volitelná kontrola - uživatel si volí sám, co se má kontrolovat

Vlastní kontrola počítače může trvat i několik desítek minut, v závislosti na typu zvolené kontroly a množství dat na pevných discích počítače.

Rychlá kontrola bez zapnutého antivirového štítu trvala na testovaném počítači 1min 33s. Procesor byl v jejím průběhu využíván průměrně na 35%.

Kompletní kontrola bez zapnutého antivirového štítu trvala na testovaném počítači 10min 16s. Procesor byl v jejím průběhu využíván průměrně na 30%.

Rychlá kontrola se zapnutým antivirovým štítem trvala na testovaném počítači 1min 50s. Procesor byl v jejím průběhu využíván průměrně na 35%.

kompletní kontrola se zapnutým antivirovým štítem trvala na testovaném počítači 10min 26s. Procesor byl v jejím průběhu využíván průměrně na 38%.

Výsledky kontrol jsou shrnuty v následující tabulce:

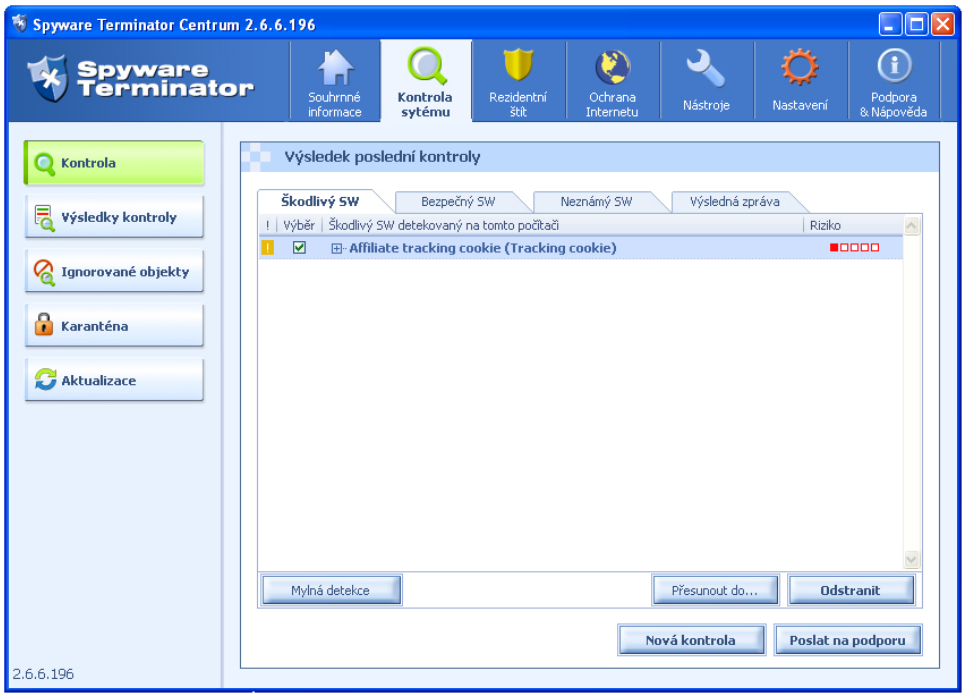
Typ Kontroly	**štít ClamAV**	**Doba trvání**	**průměr. využití CPU**
Rychlá	NE	**1min 33s**	30%
Kompletní	NE	**10min 16s**	33%
Rychlá	ANO	**1min 50s**	35%
Kompletní	ANO	**10min 26s**	38%

obrázek č. 17 - Výsledky provedených kontrol

Po ukončení kontroly se objeví okno se zobrazenými výsledky. Záložka *Škodlivý SW* obsahuje objekty, které Spyware Terminator vyhodnotil jako škodlivé a které mohou být odstraněny tlačítkem *Odstranit* nebo mohou být přesunuty do karantény.

Tlačítkem *Výsledky kontroly* je možné zobrazit detaily a souhrn všech informací o všech dosud proběhnutých kontrolách.

Tlačítkem *Karanténa* je možné zobrazit Objekty, jež jsou pravděpodobně infikované, ale lze je později smazat nebo obnovit.



obrázek č. 18 - Výsledek kontroly na přítomnost spyware

Součástí programu je i rezidentní štít, který dokáže blokovat podezřelé operace jako je pokus o změnu domovské stránky, instalaci nových toolbarů do webového prohlížeče atd. Systém HIPS (Host Intrusion Prevention System) dále počítač chrání před spuštěním nebezpečných aplikací. Program si po první kontrole vytvoří seznam spustitelných souborů v počítači a pokud je spuštěn .exe soubor mimo seznam, uživatel musí soubor manuálně povolit.

Spyware Terminator také disponuje širokými možnostmi nastavení. Mimo jiné si uživatel může nastavit automatické provedení kontroly ve zvolenou dobu, je možné upravit nastavení aktualizace, rezidentního štítu, průběhu kontroly, plánovače apod.

5.2.2. Ad-Aware 2009

Ad-Aware 2009 je specializovaný program na vyhledávání a odstraňování spywaru z počítače.

Tvůrcem Ad-Awaru je společnost Lavasoft. Také tento program je freeware, uživatel ho tedy může využívat zdarma.

Velikost stahovaného souboru je cca 63MB v případě verze Game Edition, nebo 93MB v případě Free. Program je možno stáhnout buď na www.stahuj.cz, případně na jiných odkazech. K 29. Březnu 2010 je v případě Ad-Aware 2009 Game Edition aktuální verze 8.1.1.0. a u Ad-Aware 2009 Free to je verze 8.2.0.0.

Obě verze programu Ad-Aware lze provozovat pod operačními systémy Windows Vista, Windows XP, Windows 2000 a Windows 7.

Instalace probíhá standardně a trvá asi 5min. Uživatel si může vybrat z několika jazykových lokalizací, bohužel ale chybí čeština. Uživatelské rozhraní programu je jednoduché a přehledné, graficky dobře zpracované. Grafické zpracování verze Game Edition je poněkud horší. Uživatel by s ovládáním neměl mít problémy. Hlavní okno programu obsahuje informace o stavu aktualizací, rezidentního štítu, příští naplánované kontrole, apod.

obrázek č. 19 - Hlavní okno programu Ad-Aware Free

Verze Ad-Aware 2009 Game Edition obsahuje i rezidentní štít Ad-Watch chránící počítač v reálném čase. Brání spuštění známých škodlivých procesů, hlídá změny v registrech a brání připojení ke známým IP adresám z černé listiny databáze Lavasoftu. Ve Free verzi bohužel funguje pouze dohlížení nad procesy. Pokud je zaznamenán pokus o spuštění známého nebezpečného procesu, program ho zablokuje a uživateli dá možnost výběru, co se má s procesem vykonat.

obrázek č. 20 - Stav rezidentního štítu Ad-Aware Game Edition

Při spouštění kontroly počítače na přítomnost spywaru si uživatel může vybrat z několika možností:

- Smart kontrola – kontrolovány jsou kritické oblasti systému, běžící aplikace, registry, spustitelné soubory apod.
- Úplná kontrola – kromě výše zmíněného jsou kontrolovány host files, archivy, poslední dokumenty apod.
- Volitelná kontrola – uživatel si sám určí, co se má kontrolovat

Doba trvání vlastní kontroly je různá, závisí na typu zvolené kontroly, množství dat a objektu v počítači.

Rychlá kontrola v případě Game Edition verze trvala 4min 51s, procesor byl při ní vytížen v průměru na 55%.

Úplná kontrola v případě Game Edition verze trvala 41min 4s, procesor byl při ní vytížen v průměru na 60%.

Rychlá kontrola v případě Free verze trvala 2min 57s, procesor byl při ní vytížen v průměru na 35%.

Úplná kontrola v případě Free verze trvala 24min 37s, procesor byl při ní vytížen v průměru na 40%.

Výsledky kontrol jsou shrnuty v následující tabulce:

Typ Kontroly	verze	Doba trvání	průměr. využití CPU
Rychlá	Game Edition	**4min 51s**	55%
Kompletní	Game Edition	**41min 4s**	60%
Rychlá	Free	**2min 57s**	35%
Kompletní	Free	**24min 37s**	40%

obrázek č. 21 - Výsledky kontrol

Po skončení kontroly se objeví okno s výsledky. Zobrazené objekty Ad-Aware vyhodnotil jako nebezpečné. Uživatel si může prostřednictvím menu *Recommended* vybrat co s danými objekty udělá. Tlačítko *Perform Actions Now* potom provede zvolenou akci.

obrázek č. 22 - Výsledek kontroly na přítomnost spywaru

Program umožňuje i několik možnosti nastavení. U verze Game Edition si uživatel může nastavit, kdy budou automaticky prováděny další kontroly, u Free verze to bohužel není možné. Kromě toho si lze nastavit automatické zasílání aktualizací programu, což je však u tohoto typu programů standartem.

5.2.3. Spybot Search& Destroy

Spybot Search& Destroy je softwarový nástroj na vyhledávání a odstraňování spywaru z počítače. Kromě spywaru a adwaru však dokáže odstranit i trojské koně, dialery, keyloggery a jiné formy malwaru.

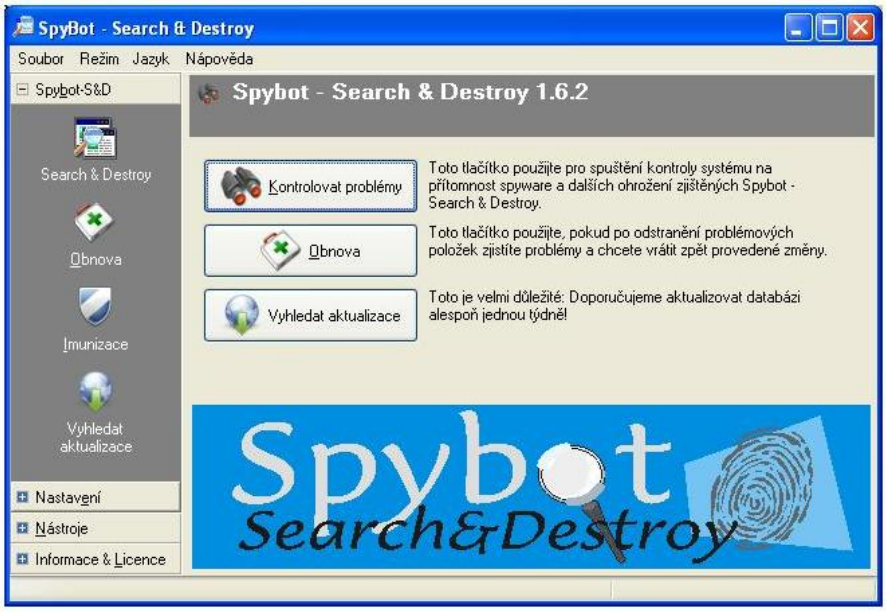
Autorem programu je společnost Patrick M. Kolla. Program je freeware a uživatel ho tedy může využívat zdarma. Velikost stahovaného souboru je cca 15,6MB. Spybot Search& Destroy je možno stáhnout z domovských stránek programu - www.safer-networking.org, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 1.6.2.46.

Spybot Search& Destroy lze využívat pod operačními systémy Windows Vista 32bit, Windows XP, Windows 2000 a 2003 a Windows 7.

Instalace programu je bezproblémová a trvá velmi krátce. Spybot zahrnuje i českou lokalizaci, avšak pouze základního menu a ovládání.

Uživatelské rozhraní programu je velmi jednoduché, až strohé, ale někdy poněkud nepřehledné. Poprvé se program spustí v režimu pro začátečníky. Ten neobsahuje všechny možnosti a nastavení programu, uživatel může provést test na přítomnost spyware, obnovit předchozí stav systému v případě problémů vyvolaných odstraněním nalezených položek, další možností je provedení imunizace a vyhledání aktualizací.

Režim pro pokročilé nabízí možnost upravit ochranu počítače přesněji podle požadavků uživatele. Umožňuje například určit složku, do které se stahují soubory z internetu a kterou bude Spybot prohledávat na přítomnost nebezpečných souborů. Dále je možné změnit skin, nastavit plánovač, nastavit ignorované položky, přípony atd. V pokročilém režimu Spybot nabízí dokonce bezpečné odstranění souborů z disku, nebo správu aplikací spouštěných při startu systému.



obrázek č. 23 - Úvodní okno Spybot S&D

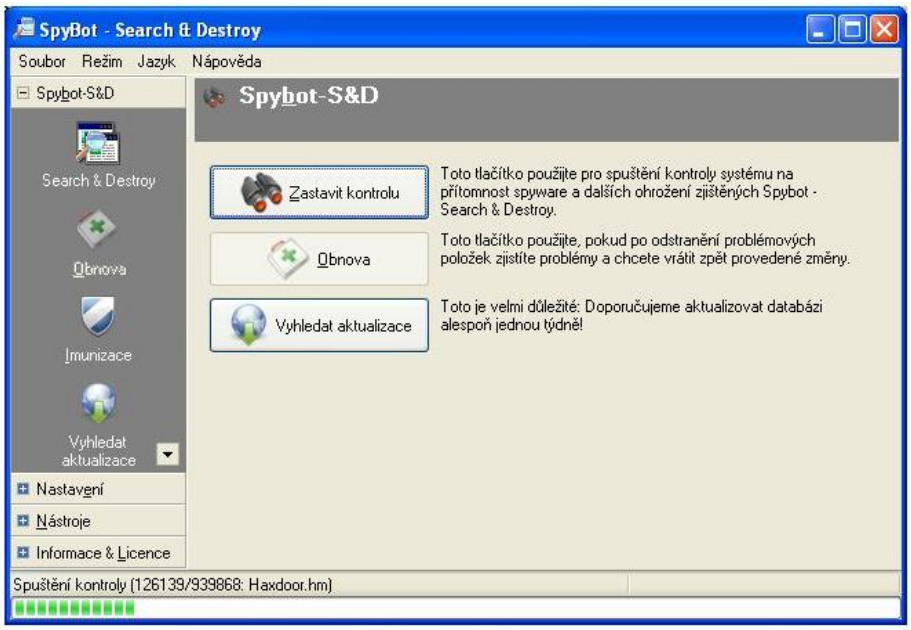
Spybot také obsahuje rezidentní štít, který počítač chrání před možnými hrozbami v reálném čase. Rezidentní štít Spybotu se skládá ze tří částí:

- Imunizace - zajišťuje preventivní ochranu počítače před stahováním a instalací nebezpečného obsahu stránek. Spybot udržuje databázi nebezpečných kódů a při

přístupu na stránku ověřuje, zda nejsou přítomny. Imunizaci by měl uživatel provádět po každé aktualizaci.

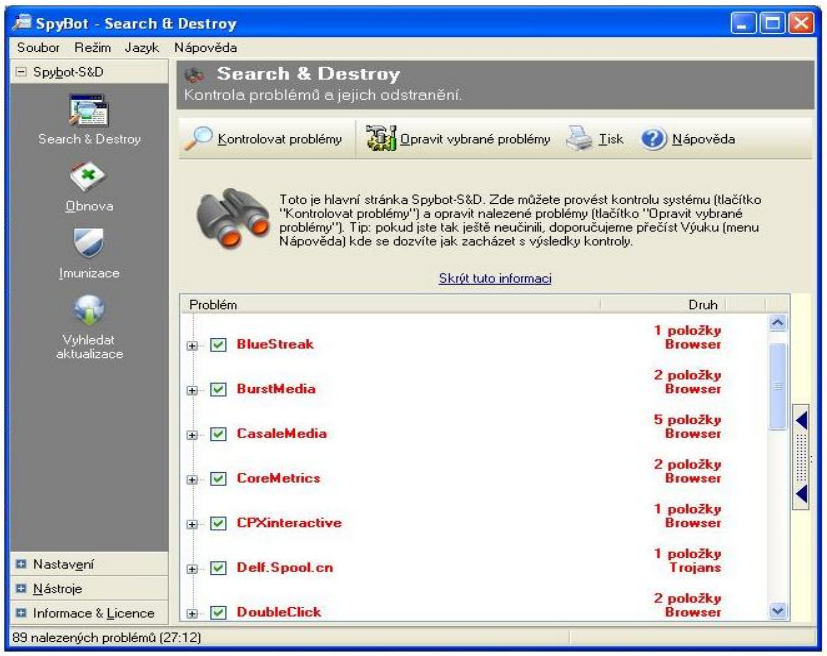
- SDS Helper – doplňuje možnosti imunizace, také zabraňuje stažení škodlivého softwaru využívajícího jiné metody stahování a instalace.
- TeaTimer – brání spuštění nebezpečných aplikací. Pokud se známá škodlivá pokouší spustit, program ji automaticky ukončí a uživateli dá na výběr, jak se s ní má příště vypořádat.

Vlastní kontrola počítače trvá poměrně dlouho, u testovaného počítače trvala kontrola 29min 11s. Procesor byl při ní využíván v průměru na 60%, což je téměř dvakrát více než u Spyware Terminatora. Informace o průběhu kontroly se zobrazují v dolní části okna.



obrázek č. 24 - Průběh kontroly v Spybot SD

Po skončení kontroly program zobrazí zjištěné výsledky. Všechny komponenty v počítači, které jsou dle aktuálních definic nežádoucí, jsou označeny červeně a připraveny k odstranění. Uživatel si také může prohlédnout bližší informace o zjištěných hrozbách, stačí jen na příslušnou hrozbu klepnout. Klepnutí na tlačítko *Opravit vybrané problémy* odstraní veškeré hrozby.



obrázek č. 25 - Nalezené infikované soubory

5.2.4. Vyhodnocení antispyware programů

Pro vyhodnocení testovaných antispywarových programů a výběr nejvhodnějšího byla použita následující hodnotící kritéria:

- doba trvání kontroly
- zatížení procesoru v průběhu kontroly
- kvalita uživatelského rozhraní

Pro srovnání programů podle prvního zmíněného kritéria byla u programu Spyware Terminator použita doba trvání *Kompletní kontroly*, u programu Spybot Search& Destroy doba trvání *Kontroly* a u Ad-Aware 2009 Free Edition doba trvání *Úplné kontroly*.

U každého ze sledovaných kritérií byly testované programy ohodnoceny, rozsah hodnocení je 1 – 5. Význam hodnocení je stejný jako ve škole, 1- výborně, 5 – nedostatečně. Každé z hodnotících kritérií také má svou váhu v rámci celkového hodnocení. Hodnocení testovaných programů a váha jednotlivých kritérií na celkové hodnocení jsou uvedeny v tabulce.

	Váha hodnocení (%)	Spyware Terminator	Spybot SD	Ad-Aware Free
Doba trvání kontroly	40	1	3	3
Zatížení CPU	20	1	3	2
Kvalita uživatelského rozhraní	40	1	4	3
	Celkové hodnocení	0,33	1,13	0,93

obrázek č. 26 - Vyhodnocení antispywarových programů

Výsledek je tvořen váženým průměrem všech hodnocení daného programu. Za nejlepší je považován program s nejnižším ohodnocením. Z testovaných antispywarových programů tak lze za nejlepší považovat program Spyware terminator s hodnocením 0,33.

5.3. Firewally

Z firewallů byly testovány programy:

- Sunbelt Personal Firewall 4
- ZoneAlarm 9 Free
- Comodo Internet Security Free

5.3.1. Sunbelt personal Firewall 4

Sunbelt Personal Firewall 4 je softwarový nástroj sloužící k důkladné kontrole dat a informací přenášených při komunikaci mezi počítači v Internetu nebo v lokální síti. Počítač je tak chráněn proti útokům hackerů, trojských koní, spyware a dalších hrozeb. Kromě této ochrany program zvládá i blokování pop-up oken, filtraci reklamních bannerů nebo úplný zákaz ukládání cookies souborů.

Autorem programu je společnost Sunbelt. Program není distribuován jako freeware, ale je možné ho po dobu 30 ti dnů bezplatně vyzkoušet. Pokud chce uživatel používat plnou verzi programu i po uplynutí této doby, je nutné si jej koupit a zaregistrovat se,

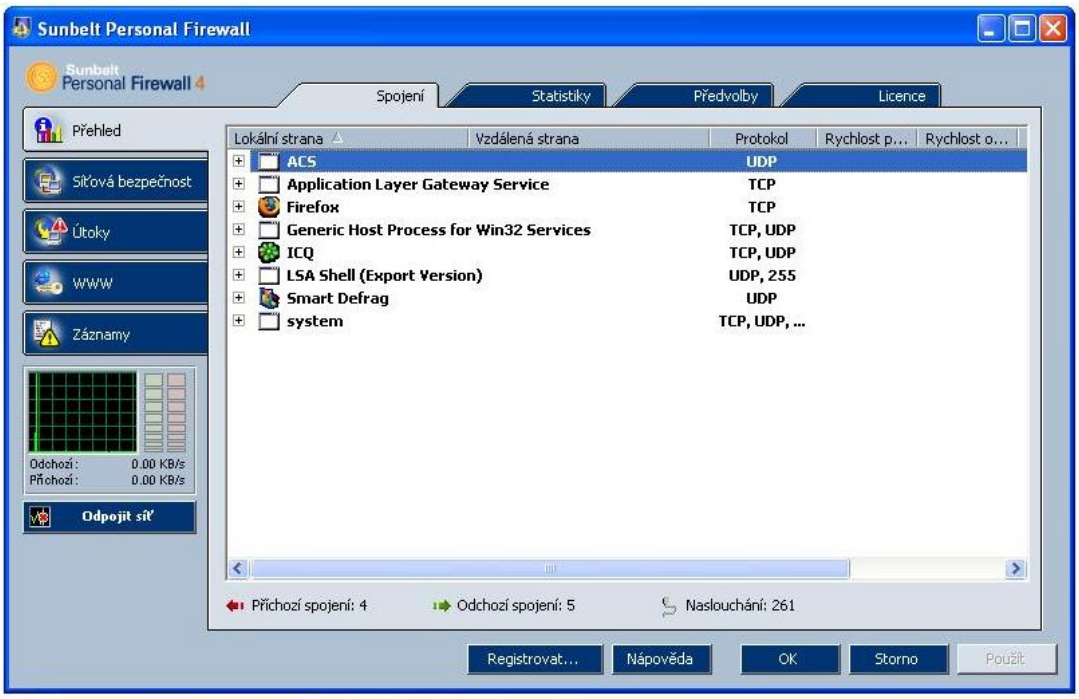
v opačném případě sice bude fungovat dále, ale v omezené míře. Velikost stahovaného souboru je cca 6 MB. Zkušební verzi Sunbelt Personal Firewall 4 je možno stáhnout buď přímo na stránkách http://www.sunbeltsoftware.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 4.6.1861.

Sunbelt Personal Firewall 4 lze využívat pod operačními systémy Windows 2000, Windows XP a Windows Vista 32bit.

Instalace probíhá velmi rychle, neměl by se vyskytnout žádný problém a program dá uživateli na výběr ze dvou možností instalace:

- Jednoduchý mód – program povolí veškerou odchozí a zablokuje veškerou příchozí komunikaci, nebude se uživatele nikdy ptát
- Pokročilý mód – poskytuje pokročilým uživatelům více bezpečnosti a přizpůsobivosti, firewall se uživatele zeptá při zjištění neznámé komunikace nebo spouštění neznámé aplikace

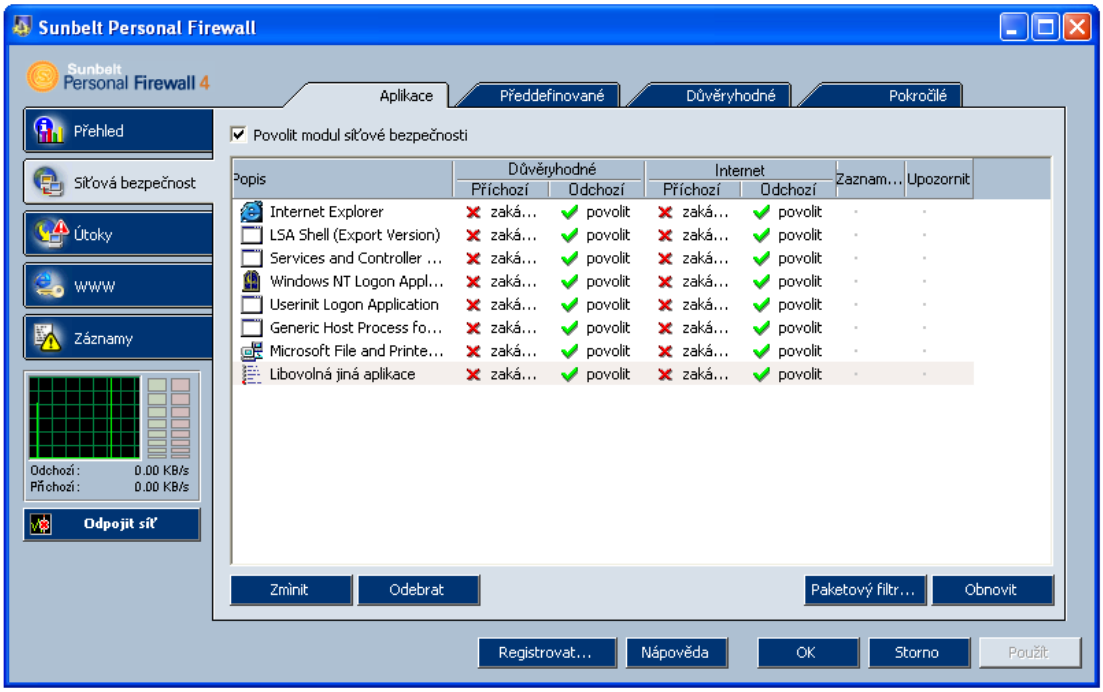
Uživatelské rozhraní programu je jednoduché, přehledné a dobře zpracované. K dispozici je i česká lokalizace, česká nápověda však bohužel chybí.



obrázek č. 27 - Hlavní okno programu Sunbelt Personal Firewall

Uživatelské rozhraní je rozděleno do 5 ti částí, každá je zastoupena tlačítkem v levé části okna programu:

- Tlačítko *Přehled* - zobrazuje seznam procesů se síťovou aktivitou, případně naslouchajících na některém z portů, informace o použitém přenosovém protokolu a příchozí i odchozí rychlosti spojení. Bližší pohled na tyto procesy pak poskytne záložka *Statistiky*.
- Tlačítko *Síťová bezpečnost* - zobrazuje tabulku se základním nastavením firewallu, uživatel ho však může změnit a určit tak, jakým procesům bude firewall povolovat připojení. Lze také nastavit volbu *Ptát se*, se kterou bude uživatel mít možnost rozhodnout se podle svého uvážení.



obrázek č. 28 - Základní nastavení firewallu Sunbelt

- Tlačítko *Útoky* – umožňuje zapnutí/vypnutí a úpravu nastavení pravidel systémů NIPS a HIPS, které vyhledávají a blokují stahování a instalaci nežádoucích procesů.
    - NIPS (Network Intrusion detection and Prevention System) - rozpoznává, blokuje a označuje známé typy proniknutí, ke své činnosti program používá databázi známých forem narušení.

  - HIPS (Host Intrusion and Prevention Systém) počítač chrání před nežádoucími změnami běžících aplikací a spuštěním škodlivého kódu.
- Tlačítko *www* - umožňuje změnit nastavení blokování reklam, pop-up oken a různých skriptů.
- Tlačítko *Záznamy* - zobrazuje zaznamenané případy pokusů o útok, průnik na počítač

Sunbelt Personal Firewall 4 je nenáročný na systémové prostředky, při běžné činnosti u testovaného počítače zatěžoval procesor na méně než 5% a využíval cca 11 800kB operační paměti.

5.3.2. ZoneAlarm 9 Free

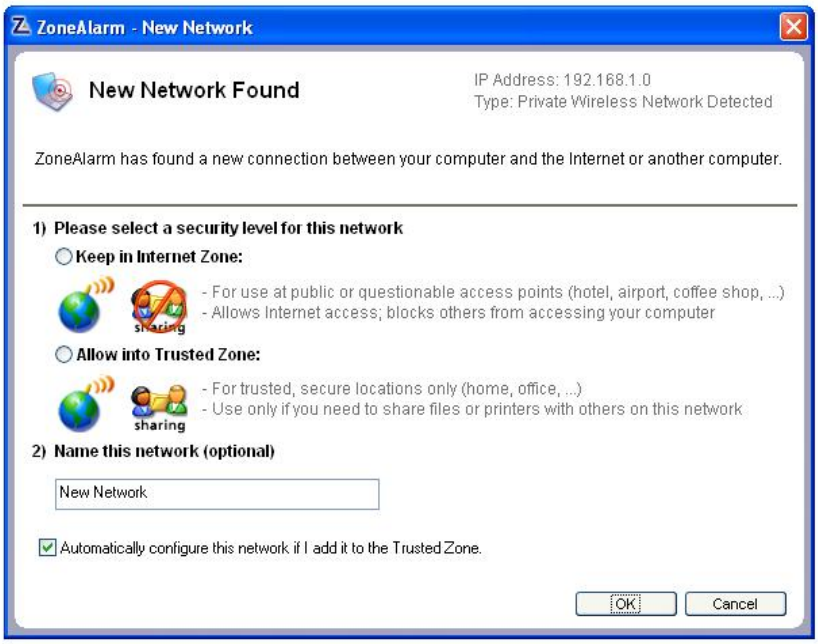
ZoneAlarm 9 Free představuje další z programů chránících počítač proti útokům z internetu, hlavně hackerům.

Autorem programu je společnost Check Point Software Technologies Ltd. Free verze tohoto firewallu je pro domácí uživatele a neziskové organizace k dispozici zdarma. Velikost stahovaného souboru je cca 38 MB. ZoneAlarm 9 Free firewall je možné stáhnout buď přímo na stránkách http://www.zonealarm.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 29. Březnu 2010 je aktuální verze 9.1.007.000.

ZoneAlarm 9 Free lze využívat pouze pod operačními systémy Windows XP a Windows Vista 32bit.

Instalace programu trvá poněkud déle a uživatel by ji měl věnovat určitou pozornost.

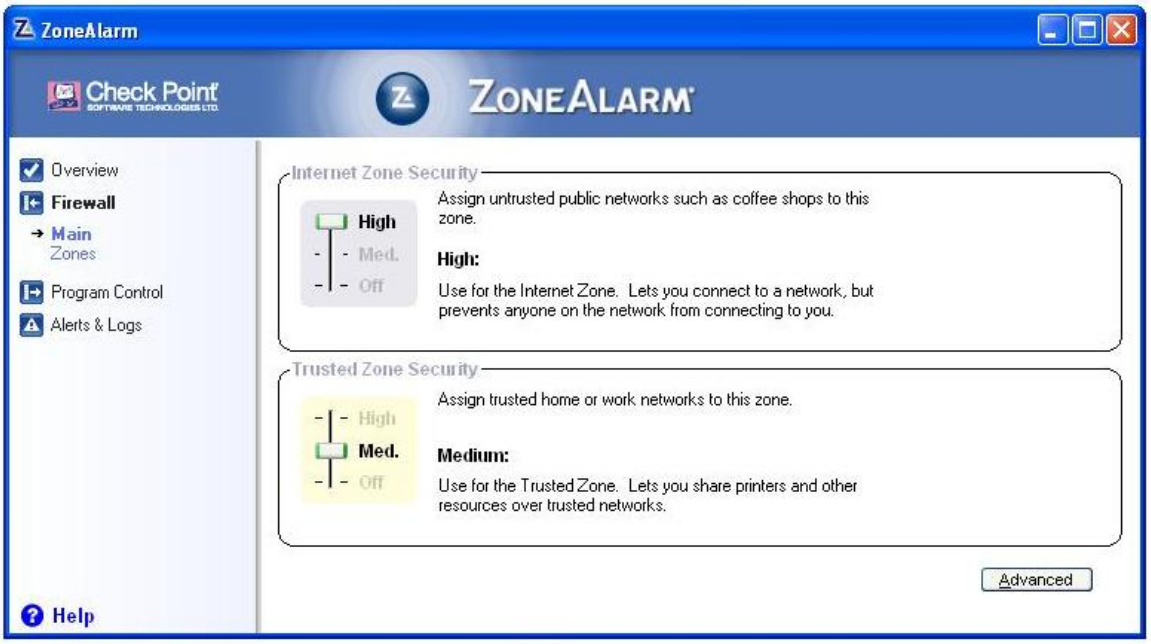
Jakmile je instalace dokončena, program při prvním spuštění detekuje síť, ke které je počítač připojen a vyzve uživatele k nastavení její důvěryhodnosti a jejího jména. Poté se již objeví hlavní okno programu. K dispozici je pouze anglická lokalizace a celkově působí program poněkud nepřehledně.



obrázek č. 29 - Nastavení důvěryhodnosti sítě

Uživatelské rozhraní je velmi jednoduché, a je rozděleno do několika částí, každá je zastoupena tlačítkem v levé části okna:

- Tlačítko *Overwiev* – zobrazuje funkční možnosti ochrany. V části *Product Info* obsahuje informace o verzi programu, registraci a licenční informace. Část *Preferences* pak umožňuje obecné nastavení programu, nastavení aktualizací a dalších možností.
- Tlačítko *Firewall* – umožňuje nastavení úrovně bezpečnosti pro komunikaci s Internetem a s důvěryhodnou sítí.
- Tlačítko *Program Control* – umožňuje nastavení úrovně potvrzování oprávněnosti akcí prováděných programy, které se pokoušejí o přístup na Internet.
- Tlačítko *Alert&Logs* – zobrazuje informace o zjištěných pokusech o napadení počítače.



obrázek č. 30 - Nastavení úrovně bezpečnosti firewallu

Činnost programu je ze začátku poněkud obtěžující, neboť se ptá pokaždé, když se některý program pokusí o přístup na Internet.

Free verze poskytuje pouze základní ochranu firewallovou ochranu počítače, placená verze Pro navíc zajišťuje ochranu proti virům, spyware, stažení a instalací nežádoucích aplikací apod.

ZoneAlarm 9 Free firewall je poměrně nenáročný na systémové prostředky, při běžné činnosti u testovaného počítače dosáhla hodnota zatížení procesoru 10% a program využíval cca 3200kB operační paměti.

5.3.3. Comodo Internet Security Free

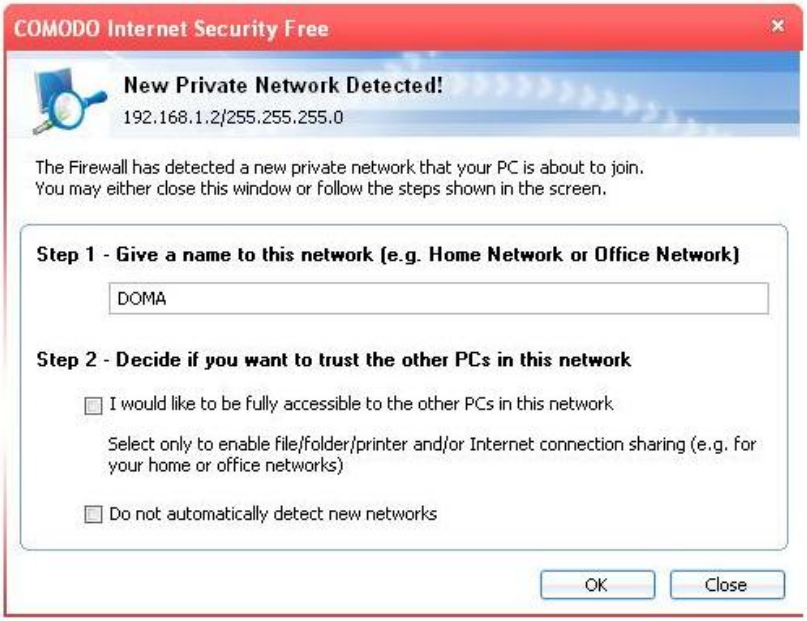
Comodo Internet Security Free představuje komplexní nástroj pro ochranu počítače a operačního systému nejen proti útokům z Internetu, ale díky integrovanému antiviru i proti všem druhům virů. Součástí programu je i funkce Sandbox, která umožňuje spustit neznámé a nedůvěryhodné aplikace ve zkušebním prostředí. Funkce Defense+ potom sleduje nežádoucí změny v důležitých systémových souborech a registrech a varuje před nimi uživatele.

Autorem programu je společnost Comodo Group, Inc. Program je distribuován jako freewarea uživatel ho tedy může používat zcela zdarma. Velikost stahovaného souboru je cca 41 MB. Program je ke stažení buď přímo na stránkách společnosti Comodo - www.comodo.com, nebo na některých jiných odkazech (Stahuj.cz, Sluněčnice.cz apod.). K 4. Dubnu 2010 je aktuální verze 4.0.138377.799.

Comodo Internet Security Free lze využívat pod operačními systémy, Windows XP, Windows Vista 32bit a Windows 7.

Instalace programu probíhá rychle, neměl by se vyskytnout žádný problém, takže by s ní neměli mít problémy ani uživatelé-začátečníci.

Po dokončení instalace program při prvním spuštění detekuje síť, ke které je počítač připojen a vyzve uživatele k nastavení její důvěryhodnosti a jejího jména. Poté se již objeví hlavní okno programu. To se sice poprvé zobrazí v angličtině, uživatel si však může přepnout program do češtiny.

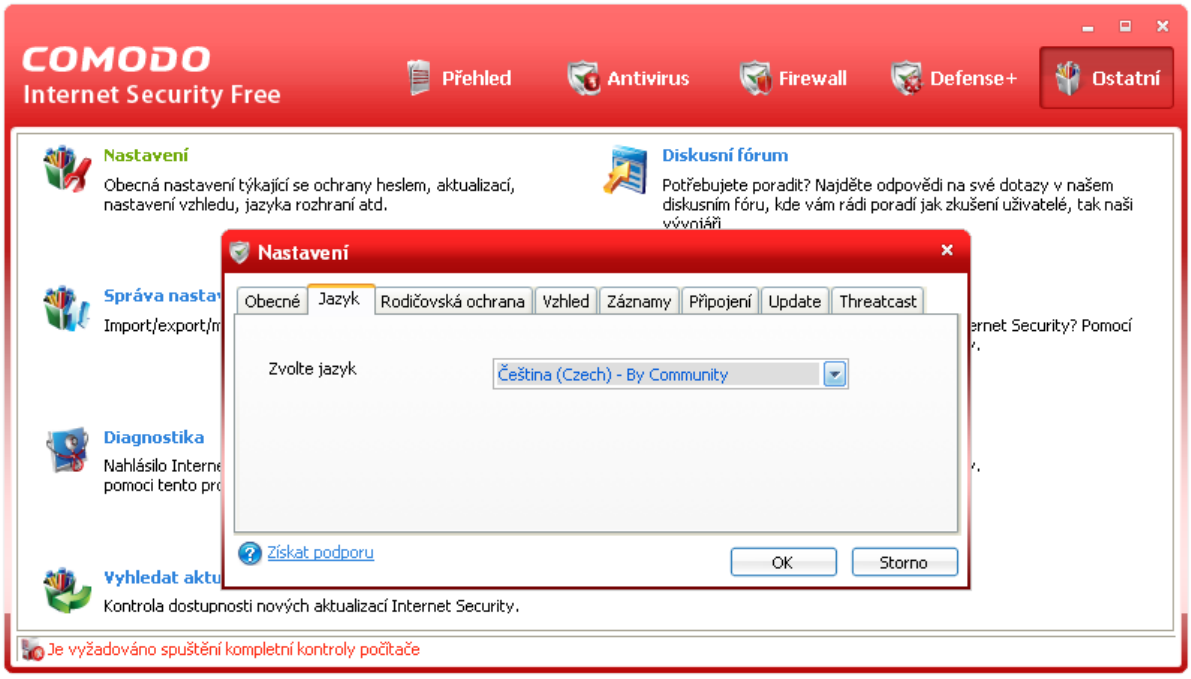


obrázek č. 31 - Pojmenování a nastavení důvěryhodnosti sítě

Uživatelské rozhraní je jednoduše a přehledně zpracované. Rozděleno je do několika částí, které zobrazují důležité informace o programu a stavu systému a umožňují též přehledně upravit vlastnosti nastavení.

Jednotlivé části programu jsou zastupovány tlačítky v horní části okna:

- Tlačítko *Přehled* – zobrazuje informace o akcích, které by měl program provést, informace o stavu rezidentní antivirové ochrany a aktualizaci virové databáze, informace o ochraně sítě, stavu komunikace a další informace a možnosti nastavení.
- Tlačítko *Antivirus* – umožňuje provádět akce a upravovat možnosti nastavení antivirové části programu, např. spustit antivirovou kontrolu, aktualizovat databázi, prohlédnout obsah karantény, upřesnit nastavení parametrů kontroly, vytvořit plán dalších kontrol apod.
- Tlačítko *Firewall* – umožňuje nastavení všech vlastností firewallu. *Základní funkce* firewallu umožňují prohlédnout si události a upozornění vyvolané případnými útoky, definovat důvěryhodné a nedůvěryhodné aplikace, prohlédnout si informace o aktuálních spojeních a další informace. *Pokročilé funkce* umožňují zkušenějším uživatelům upravit nastavení pravidel síťové komunikace, prohlédnout si a upravit předdefinovaná pravidla a upravit chování firewallu.
- Tlačítko *Defense+* - v základní části zobrazuje informace o souborech sledovaných funkcí Defense+. Část *Sandbox* umožňuje upravit nastavení Sandboxu, umístit do něj vybraný soubor a spustit ho v něm. Část *Pokročilé* umožňuje zkušenějším uživatelům upravit nastavení pravidel této funkce, prohlédnout si a upravit předdefinovaná pravidla a upravit její nastavení.
- Tlačítko *Ostatní* – umožňuje upravit obecná nastavení, zejména změnit jazyk, dále vyhledat aktualizaci programu, zobrazit nápovědu nebo informace o licenci a verzi Comodo Internet Security.



obrázek č. 32 - Změna nastavení jazyka

Program tedy disponuje širokými a přehledně uspořádanými možnostmi přizpůsobení podle požadavků uživatele.

Comodo Internet Security je nenáročný na systémové zdroje. U testovaného počítače při běžné činnosti dosáhla hodnota zatížení procesoru méně než 5% a program využíval cca 8000kB operační paměti.

5.3.4. Vyhodnocení firewallů

Pro vyhodnocení testovaných firewallů a výběr nejvhodnějšího byla použita následující hodnotící kritéria:

- zatížení procesoru
- kvalita uživatelského rozhraní
- kvalita programu podle testu matousec.com

U každého ze sledovaných kritérií byly testované programy ohodnoceny, rozsah hodnocení je 1 – 5. Význam hodnocení je stejný jako ve škole, 1- výborně, 5 – nedostatečně. Každé z hodnotících kritérií také má svou váhu v rámci celkového

hodnocení. Hodnocení testovaných programů a váha jednotlivých kritérií na celkové hodnocení jsou uvedeny v tabulce.

	Váha hodnocení (%)	Sunbelt Personal Firewall	ZoneAlarm Free	Comodo Internet Security
Zatížení CPU	20	1	1	1
Kvalita uživatelského rozhraní	40	2	3	1
Kvalita podle Matousec.com	40	4	4	1
	Celkové hodnocení	0,87	1	0,33

obrázek č. 33 - Vyhodnocení firewallů

Výsledek je tvořen váženým průměrem všech hodnocení daného programu. Za nejlepší je považován program s nejnižším ohodnocením. Z testovaných firewallů tak lze za nejlepší zcela oprávněně považovat program Comodo Internet Security Free s hodnocením 0,33.

6. Závěr

Diplomová práce rozebrala problematiku škodlivého softwaru ohrožujícím počítač a jeho ochrany před ním. Popsány byly jednotlivé formy ohrožení, škody, které mohou způsobit a způsoby jak se uživatelé mohou před tímto ohrožením chránit, včetně specializovaného ochranného softwaru.

Počítače byly a jsou ohrožovány velkým množstvím různých forem škodlivého softwaru. Jmenovat lze počítačové viry, červy, trojské koně, hoaxy nebo spyware a adware. Tyto hrozby využívají různé způsoby svého dalšího šíření mezi počítači a mohou způsobit rozsáhlé škody, např. ztrátu důležitých a osobních dat, omezení výkonu počítače, nestandardní chování programů a další škody.

Zajištění ochrany počítače před jeho napadením škodlivými programy představuje souhrn několika možností a použití specializovaných ochranných programů je jednou z nich. Ochranný software byl rozdělen do několika typů, a to podle hrozeb, proti kterým působí. Jednotlivé typy programů byly popsány a vysvětlena byla i jejich funkce a způsob činnosti.

Součástí práce bylo i testování a hodnocení vybraných zástupců volně dostupných antivirových programů, firewallů a programů proti spywaru. Tyto programy tvoří základ při ochraně počítače před škodlivým software. Z antivirů byly testovány programy AVG 9 Free Edition, AVAST! Free antivirus a ESET NOD32. Z firewallů byly testovány programy Sunbelt Personal Firewall 4, ZoneAlarm 9 Free a Comodo Internet Security Free. Programy na ochranu proti spywaru zastupoval Spyware Terminator, Spybot Search&Destroy a Ad-Aware 2009.

Vybrané programy byly vyzkoušeny a podrobněji popsány. Pozornost byla věnována jejich funkcím, možnostem a způsobům činnosti. Po ukončení testů byly programy ohodnoceny podle stanovených kritérií, představovaných např. dobou trvání kontroly testovaného počítače, kvalitou uživatelského rozhraní, zatížením systémových prostředků apod. Srovnání výsledků vytvořilo základ pro výsledné hodnocení, které umožnilo výběr nejvhodnějších programů v příslušných kategoriích.
V kategorii antivirových programů tak byl jako nejvhodnější vybrán program AVG 9 Free

Edition, z antispywaru potom program Spyware Terminator. V kategorii firewallů byl jako nejvhodnější z testovaných produktů vybrán program Comodo Internet Security Free. Vybrané programy lze uživatelům doporučit jako vhodnou volbu k zajištění bezpečnosti jejich počítače.

7. Použitá Literatura

1) HÁK, Igor – ZELENKA, Josef. *Ochrana dat: škodlivý software*. 1. vyd. Hradec Králové: Gaudeamus, 2005. 211 s. ISBN 80-7041-594-0.

2) SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. 1. vyd. Brno: Zoner Press, 2006. 608s. ISBN 80-86815-04-8.

3) KOCMAN, Rostislav – LOHNICKÝ, Jakub. *Jak se bránit virům, spamu, dialerům a spyware*. 1. vyd. Brno: CP Books, 2005. 148 s. ISBN 80-251-0793-0.

4) HEINIGE, Karel. *Viry a počítače*. 1. vyd. Praha: Mobil Media, 2001. 80 s. ISBN 80-86593-02-9.

5) SZOR, Peter. *The art of computer virus research and defense*. 1. vyd. Upper Saddle River: Addison-Wesley, 2005. 713 s. ISBN 0-321-30454-3.

6) BAUDIŠ, Pavel – ZELENKA, Josef. *Antivirová ochrana*. 1. vyd. Praha: Plus, 1996. 183 s. ISBN 80-85297-74-4.

7) JALŮVKA, Josef. *Moderní počítačové viry: Podstata, prevence, ochrana*. 2. aktualiz. vyd. Praha: Computer Press, 2000. 224 s. ISBN 80-85896-64-8.

8) KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně*. 1. vyd. Praha: Grada, 2006. 334 s. ISBN 80-247-1408-6.

9) KALUŽA, Radovan. *SPAM - pěkně hnusná konzerva*. [online]. 2010, http://radovan.bloger.cz/IT-internet/SPAM-pekne-hnusna-konzerva

10) OHNESORG, Dan. *Bezpečnost Linuxu proti virům*. [online]. 2010, http://www.linux.cz/viry.html

11) Denial of Service Attacks. [online] 2006, http://www.bluetack.co.uk/forums/lofiversion/index.php/microsoft.com/t8462.html

12) VAŠEK, Jiří. *Zabezpečení počítače - firewall a jeho nastavení.* [online]. 2007, http://pctuning.tyden.cz/software/ochrana-pocitace/8590-zabezpeceni_pocitace-firewall_a_jeho_nastaveni

13) KUCHAŘ, Martin. *Firewall – obrňte své počítače.* [online]. 2005, http://pctuning.tyden.cz/index.php?option=com_content&view=article&id=4296&catid=52&Itemid=78

14) SLUNEČNICE.CZ. *AVG 9 Free Edition.* [online]. 2010, http://www.slunecnice.cz/sw/avg-anti-virus-free/

15) SLUNEČNICE.CZ. *ESET NOD32 Antivirus.* [online]. 2010, http://www.slunecnice.cz/sw/nod/

16) STAHUJ.CZ. *Avast! Free antivirus.* [online]. 2010, http://www.stahuj.centrum.cz/utility_a_ostatni/antiviry/kompletni/avast/

8. Seznam obrázků