Západočeská univerzita v Plzni

Fakulta pedagogická

Bakalářská práce

SOFTWAROVÉ ZABEZPEČENÍ OSOBNÍHO POČÍTAČE V SYSTÉMECH WINDOWS

Veronika Staňková

Plzeň 2012

Prohlašuji, že jsem práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, dne

Veronika Staňková

……....

Poděkování

Děkuji vedoucímu svojí bakalářské práce Mgr. Tomáši Jakešovi

za poskytnuté rady a podnětné konzultace.

Obsah

Seznam použitých odborných výrazů[1]

Active X – ovládací prvky (nejčastěji u internetových aplikací)
Cloud-computing – technologie poskytování služeb a aplikací uložených na Internetu
Cookies – speciální data, která webové servery ukládají na disku návštěvníka stránky
EXE soubor – nejběžněji používaný spustitelný soubor
Firewall – program, který monitoruje internetovou komunikaci
Flash – grafický vektorový program, používá se pro tvorbu internetových aplikací
Freeware – počítačový program, který je distribuován bezplatně
IBM PC – označení pro počítač kompatibilní se standardem IBM
IP adresa – adresa, která identifikuje počítač v síti
Makro – posloupnost akcí, které následují vyvoláním určitého povelu
Malware – program určení k průniku do počítače či jeho poškození
Open-source – počítačový software s otevřeným zdrojovým kódem
Paket – blok dat přenášených v počítačové síti
Port (síťový port) – speciální číslo, které slouží k detailnější komunikaci v poč. síti
Registr – prostor pro ukládání systémových klíčů a hesel v OS Windows
Rootkit – program, který maskuje přítomnost jiných škodlivých programů
Spam – nevyžádaná e-mailová pošta
Spyware – program, který odesílá data z PC uživatele bez jeho vědomí
VBScript – skriptovací programovací jazyk

Seznam použitých zkratek[1]

API – Application Programming Interface – rozhraní pro programování aplikací
AVS – Antivirový systém
CPU – Central Processing Unit - procesor
DLL – Dynamic Link Library – dynamicky linkovaná knihovna v OS Windows
DNS – Domain Name System – hierarchický systém doménových jmen (servery+protokol)
EULA – End-User-License-Agreement - licence pro koncového uživatele softwaru
HTML – HyperText Markup Language – značkovací jazyk pro hypertext
IMAP – Internet Message Access Protocol – internetový protokol pro přístup k e-mailu
IP – Internet Protocol – internetový protokol
IS – Internet Security
MB – Megabajt – jednotka informace v číslicové a výpočetní technice
MHz – MegaHertz – jednotka frekvence (základní jednotkou je Hz – Hertz)
MS – Microsoft
NAT – Network Address Translation – překlad síťových adres
OS – Operační systém
OSI – Open Systems Interconnection – standard komunikace v počítačových sítích
PC – Personal Computer – osobní počítač
PDF – Portable Document Format – přenosný formát souboru pro dokumenty
POP3 – Post Office Protocol 3 – internetový protokol pro stahování e-mailových zpráv
RAM – Random-access memory – druh počítačové paměti

[1] Wikipedia. Wikipedie - Otevřená encyklopedie [online]. 2011 [cit. 2011-12-10]. Dostupné z WWW: <http://cs.wikipedia.org/>.

Úvod

Dnes si lze jen stěží představit, že na úplném počátku rozvoje počítačů a osobních počítačů téměř neexistovaly počítačové viry ani jiné dnes zcela běžné bezpečnostní hrozby. Tehdejší uživatele výpočetní techniky vůbec nenapadlo, že by jejich počítač mohl být nějakým způsobem napaden a jejich data poškozena či zneužita. Naproti tomu většina dnešních uživatelů ví, že existují počítačové viry a jiné škodlivé programy, přesto je to mnohdy bohužel nedonutí zabývat se ochranou svého počítače. Zabezpečením počítače se tak mnohdy začnou zabývat až příliš pozdě, většinou poté, co byla například jejich data vymazána, operační systém jejich počítače nenabíhá či byla zneužita jejich platební karta. Tato práce je ale určena nejen těmto uživatelům, ale všem, kteří se chtějí seznámit s dnešními běžnými bezpečnostními riziky a zejména počítačovými programy, pomocí kterých se jim lze bránit.

První kapitola práce stručně představuje historii nejznámějších softwarových bezpečnostních rizik od jejich počátku v 60. letech 20. století na tehdejších sálových počítačích až po rok 2000 a moderní osobní počítače. Dále obsahuje současné základní druhy bezpečnostních hrozeb (jako např. makroviry, spyware atd.).

Následující kapitola se zabývá obecnými možnosti ochrany proti počítačové infiltraci v operačním systému Windows. Kapitola obecně představuje základní počítačové programy, pomocí kterých lze osobní počítač s Windows zabezpečit, zabývá se rovněž standardní ochranou, kterou má tento operační systém v sobě integrovanou a v neposlední řadě problematikou nepoučeného uživatele, který mnohdy představuje největší riziko možné infiltraci do svého vlastního počítače.

Třetí kapitola samotné práce představuje formou porovnávacích tabulek jednotlivé bezpečnostní balíky, antiviry a firewally. Zároveň jsou v ní popsány konkrétní testy, které se zabývají porovnáváním a sledováním kvality těchto produktů, včetně konkrétních výsledků z jednotlivých testů, je zde rovněž dopočten celkový výsledek vždy za daný produkt po přepočtení výsledků všech testů.

Závěrná kapitola vlastní práce blíže popisuje konkrétní produkty, které se nejlépe umístily v testech, kromě členění na antiviry a firewally se ještě rozděluje na popis bezplatných (nekomerčních) a komerčních aplikací.

1 Členění a historie softwarových bezpečnostních rizik

Počítačovou infiltraci lze charakterizovat jako neautorizovaný (neoprávněný) vstup do systému počítače. Počítačovou infiltraci způsobuje škodlivý software, nejběžněji „malware“ (MALicious softWARE).

Nejznámějším příkladem malwaru je počítačový virus. Samotné označení „vir“ je odvozeno od klasického biologického viru. Počítačový virus se tedy obdobně jako viry různých nemocí dokáže samostatně rozšiřovat na úkor svého hostitele (napadaného EXE souboru, systémové části pevného disku, makro souboru, ...).

Níže v mé práci konkrétněji představuji jednotlivé typy malwaru.

1.1 Historie nejznámějších softwarových rizik[2]

Historie počítačových virů začíná v 60. letech, kdy se na tehdejších sálových počítačích objevuje program „Králík“, který byl schopný klonovat sám sebe a obsazovat systémové prostředky počítače. Nešlo však o klasický virus, jak je známe dnes, ale pouze o chybu programátora. V 70. letech se objevuje vir „The Creeper“ (OS Tenex), který se šířil tehdejší globální počítačovou sítí a na jehož odstranění byl vytvořen první „antivir“ pod názvem „Reeper“.

Prvním virem pro IBM PC byl „Brain“ z roku 1986, který napadal tehdejší běžné diskety (kapacita 360 kB). Autoři viru, bratři Basit a Amjad Farooq Alvi z Pakistánu, byli prodejci softwaru, kteří chtěli zjistit rozsah počítačového pirátství, a tak v těle viru zanechali zprávu se svými jmény, adresou a telefonem. Už tehdy se tedy jasně ukázalo, jak úzká hranice je mezi počítačovými ochránci a útočníky. Vir jako první dokonce využíval stealth techniku (vir se aktivně kryje, aby nebyl detekován) - pokud se OS pokoušel číst z infikovaného sektoru, vir ho nahradil čistým původním sektorem.

Ve stejném roce Ralf Burger zjišťuje, že program může svůj „škodlivý“ kód přidat do kódu ostatních spustitelných programů v OS DOS – vzniká první takový typ viru pod názvem „VirDem“.

V roce 1992 se objevuje první panická historie vyvolaná počítačovým virem, způsobil ji vir „Michelangelo“ – jedna americká antivirová společnost oznámila, že 6. března 1992

[2] MICHAL, Jindřich. *Historie a vývojové trendy ve výpočetní technice* [online]. 2001 [cit. 2011-07-31]. Historie počítačových virů. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2001/xmichal1.html>.

budou zničena data v 500 000 000 počítačů. Důsledkem tohoto sdělení byl rekordní zisk antivirových společností, ve skutečnosti tento vir napadl necelých 10 000 počítačů.

Ve stejném roce se objevuje i první Windows vir, který nikdy nebyl oficiálně pojmenován a který napadal spustitelné soubory pro OS Windows. Reakcí na první viry pro relativně nový operační systém Microsoftu byl první antivirový systém vytvořený přímo Microsoftem – MSAV (vycházel z antiviru CPAV od společnosti CentralPoint).

V roce 1994 se začínají používat CD disky pro přenos počítačových dat a s nimi i přenos počítačových virů. Stávalo se, že oficiální distribuce aplikace na CD nosiči byla napadena virem a všechny CD musely být následně staženy a zničeny.

Tentýž rok je ve Velké Británii na stránky zpravodajské stanice BBS umístěn soubor infikovaný viry „SMEG.Pathogen“ a „SMEG.Queen“.

Počátek roku 1995 znamenal pěknou ostudu pro společnost Microsoft – disky s demonstrační verzí systému Windows 95 byly infikovány virem „Form“, napadený systém se dostal i k beta testerům. V závěru roku se objevuje, pod označením „Concept“, první vir pro kancelářský editor Microsoft Word – během měsíce se stal statisticky nejrozšířenějším virem.

Rok 1996 znamenal první vir pro produktivní verzi Windows 95 – „Win95.Boza“. Objevuje se první vir pro tabulkový procesor MS Excel, který je stejně jako zmíněný „Concept“ založen na zneužití maker, vir nesl označení „Laroux“. Na závěr roku vzniká první rezidentní vir pro Windows 95 – „Win95.Punch“ (rezidentní vir zůstává v operační paměti Windows, hlídá přístup k souborům a napadá otevřené EXE soubory).

V srpnu 1998 se objevuje první vir založený na zneužití technologie Java – „Java.StrangeBrew“, následují viry založené na VBScriptu a HTML.

Posledním známým virovým hitem se stal v roce 2000 „ILOVEYOU“, který se šířil v e-mailu se stejnojmenným předmětem. V těle zprávy se nachází text „kindly check the attached LOVELETTER coming from me“. V příloze je soubor „LOVE-LETTER-FOR-YOU.TXT.vbs“. Spuštění tohoto souboru aktivuje vir, který při každém startu PC přepíše všechny soubory s příponami JPG, JPEG, MP3, MP2, VBS, VBE, JS, JSE, CSS, WSH, SCT a HTA přepíše svou kopií. Rovněž se zašle na všechny e-maily uvedené v adresáři aplikace Outlook.

Obrázek 1-E-mail šířící vir ILOVEYOU

(Převzato z http://disinfo.s3.amazonaws.com/wp-content/uploads/2010/05/virus_iloveyou.gif)

1.2 Základní druhy softwarových bezpečnostních rizik[3]

1.2.1 Virus

Základní vlastností standardního počítačového viru je možnost vlastního rozmnožování na základě využití zdrojů hostitele, jak ostatně uvádím výše. Označení virus rovněž souhrnně označuje další níže uvedené typy, mnohdy však nesprávně označuje za vir např. spyware. Viry jsou ovšem stejně jako právě například spyware podkategorií škodlivých infekcí – tedy malware.

1.2.1.1 Rezidentní a nerezidentní viry

Viry dělíme do několika kategorií, např. podle způsobu činnosti na „rezidentní“ (nacházejí se v operační paměti počítače, kde jsou sice snáze odhalitelné, ale zároveň snáze a rychleji napáchají škodu hostitelskému počítači) a „nerezidentní“, které se nacházejí ve spustitelných souborech, do kterých se infiltrují (hůře odhalitelný, ale statisticky a teoreticky spáchají menší škodu).

1.2.1.2 Klasifikace hostitele viru

Virus se šíří prostřednictvím prostředků svého hostitele, hostitelů může být několik druhů, např.:

spustitelný soubor (u Windows soubory s příponou EXE a COM)

[3] HÁK, Igor. Moderní počítačové viry. Hradec Králové, 2005. 110 s. Bakalářská práce. Univerzita Hradec Králové.

boot (zaváděcí) sektory diskových oddílů

Master Boot Record (MBR, hlavní spouštěcí záznam umístěný v prvním sektoru disku)

dávkový soubor či skript (např. BAT soubory)

soubory obsahují makra (nejčastěji soubory aplikací Microsoft Office – Word, Excel či Access) – tzv. makroviry

1.2.1.3 Stealth viry

Stealth viry nebo-li tajné (maskované) viry se obdobně jako známá letadla americké armády snaží před nepřítelem (tzn. antivirem) skrýt svojí přítomnost a to sice pomocí kontroly požadavků přerušení – monitorují veškeré požadavky na čtení ze souboru – takové požadavky dává i antivirus při kontrole obsahu souboru. Pokud se požadavek na čtení týká infikovaného souboru, tak do něj vrátí původní (neinfikovaný) obsah a antivirus nic nepozná. Naštěstí výrobci antivirových systémů mají účinné protiopatření – antivirus soubor čte přímo prostřednictvím řadiče disku, případně kontroluje adresu přerušení, zda nebyla upravena. Na stealth viry navazují tzv. rootkity, o kterých se zmiňuji níže.

1.2.1.4 Bootviry

Bootvir je dnes spíše historický a raritní druh, zmiňuji jej však pro úplnost. Bootvir je vir, který se nachází v MBR nebo boot sektoru pevného disku (viz Klasifikace hostitele viru). Vir přepíše boot sektor vlastním záznamem a původní archivuje na jiné části disku. Tyto viry se šířily zejména pomocí disket a to především v operačním systému DOS a společně se slávou disket a DOSu skončila i jejich slavná éra.

1.2.2 Trojské koně

Trojský kůň není narozdíl od klasických virů schopen vlastního množení a neinfikuje ani samotné soubory. Typický trojský kůň je prezentován jako spustitelný soubor, který se mnohdy vydává za užitečný program, ale ve skutečnosti vykonává škodlivou činnost (dříve nejčastěji odstraňoval data na pevném disku počítače).

Kromě klasického „trojana“ odstraňujícího data na disku se můžeme setkat ještě s „Password-stealing trojan“, jak již vyplývá ze samotného názvu, tak tato verze „koně“ se zabývá monitorováním a ukládáním všech stisknutých kláves („keyloggers“) a jejich následným odesláním na přednastavené e-mailové adresy. Příjemce e-mailu tak kromě nepodstatných informací získá např. i Vaše hesla vč. hesel např. do internetového

bankovnictví. Vzhledem k tomu, že odesílání se děje bez vědomí uživatele, tak lze tento druh koně chápat i jako spyware.

„Downloader“ je typ koně, který se snaží po své infiltraci škodlivé programy stahovat z internetových adres uložených v jeho kódu. Stažené programy mohou stahovat další a další škodlivé kódy. Po několika takových vlnách je počítač již znatelně zpomalen, což může být signálem pro uživatele, na druhou stranu v tomto případě již je většinou pozdě a je třeba celý systém kompletně přeinstalovat.

Oblíbený je rovněž „Proxy Trojan“, který zneužívá napadaný počítač pro neautorizovanou činnost, jako je třeba odesílání nevyžádané pošty (spamu). Díky využití proxy je pravý původce e-mailu takřka nevypátratelný.

1.2.3 Backdoors aneb zadní vrátka

Nejznámější skupina trojských koní je nazývána Backdoors (nebo-li v překladu zadní vrátka), věnují se jí proto samostatně, a to i z toho důvodu, že často bývá v odborných publikacích samostatně prezentována.

Backdoors představuje neautorizovanou obdobu aplikací na vzdálenou správu počítače (např. Remote Administrator, DameWare, VNC atp.), tyto aplikace většinou pracují viditelně a uživatel o jejich činnosti ví. „Zadní vrátka“ narozdíl od nich pracují skrytě, útočník tedy vidí vaši činnost na počítači a může s ním na dálku (skrytě) pracovat, aniž to tušíte. Backdoors často využijí chyby a slabá místa OS Windows, ty jsou následně opravovány pomocí bezpečnostních aktualizací, opět se tedy ukazuje, že je skutečně důležité tyto aktualizace přijímat.

1.2.4 Rootkit

Označení rootkit je ve světě počítačové „havěti“ poměrně nové, jak již uvádím výše, tak rootkity navazují na stealth viry. Rootkit slouží k tomu, aby zakrýval neautorizovanou činnost útočníka či jiného malwaru. Rootkit ke skrývání používá dvě varianty - modifikaci cest a modifikaci systémových struktur.

Modifikaci cest představuje často přesměrování API funkcí OS – rootkit je umístěn mezi uživatelskou aplikací a DLL knihovnou (ta obsahuje danou API funkci).

Druhá metoda (modifikace systémových struktur) představuje především maskování změn v registrech či systémových procesech OS.

1.2.5 Worms (červi)

Pokud jsem uváděla, že kvůli „backdoors“ je třeba stahovat aktualizace OS, tak kvůli červům je to naprosto nutné. Červi totiž využívají právě chyby a díry v zabezpečení, které se týkají přístupu k síti. Nejde o klasické viry ve formě souborů, červ je obsažen v infikovaných paketech. Ty se z napadeného systému šíří dále a dále (buď organizovaně nebo náhodně), teoreticky tak mohou ohrozit celou síť, tj. celý internet. Naštěstí však dnes výrobci softwaru reagují poměrně rychle, a tak je tato situace prakticky vyloučena. Jelikož červi pracují na úrovni paketů, tak pro jejich detekci nelze využít klasický antivirový program – je třeba spoléhat zejména na firewall a aktualizovaný OS i ostatní aplikace.

Prvním červem byl tzv. Morrisův červ, který v roce 1989 zahltil většinu tehdejší globální počítačové sítě (předchůdce dnešního internetu). Jedním z doposud nejznámějších červů je „SQLSlammer“, který zneužil bezpečnostní díry v aplikaci MS SQL Server. Přesto, že Microsoft vydal již několik měsíců před vypuštěním červa záplatu, která tuto bezpečnostní díru spolehlivě zacelila, tak byl útok „SQLSlammeru“ velice úspěšný.

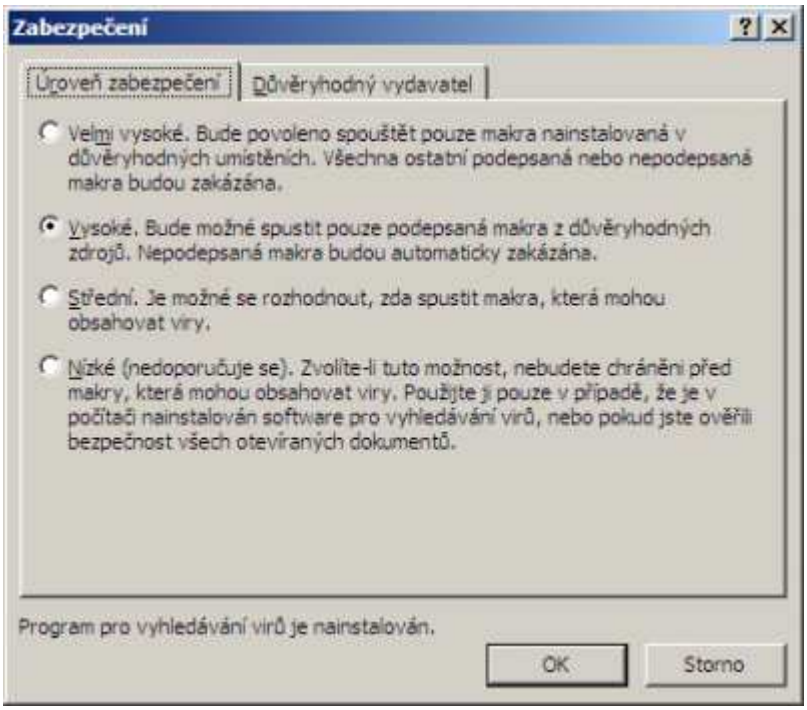
1.2.6 Makroviry

Tyto viry zneužívají automatizovanou posloupnost akcí (kláves) ve formě makra, to využívá většina softwarových kancelářských balíků – odtud také název „makroviry“. Makroviry mají tu vlastnost, že jsou schopni se kopírovat mezi jednotlivými dokumenty. Dnešní makra jsou vytvářena i za pomoci vyšších programovacích jazyků, mohou manipulovat s daty aplikace a ovlivňovat další spojená makra, stejně jako data v počítači.

Makroviry se orientují zejména na dnes nejrozšířenější kancelářské aplikace MS Word a MS Excel.

Princip činnosti makra u aplikace Word popisuje ve své práci Igor Hák (2005): *„Pro Word funguje většina makrovirů následujícím způsobem: makrovirus je uložen v napadeném dokumentu. Pokud je takový dokument otevřen a načten danou aplikací, může být za určitých podmínek virus spuštěn (např. pomocí automaker, ale i jinými způsoby, o nichž se zmíníme za chvíli). Virus pak může zkopírovat sebe sama do nějakého globálního dokumentu, který mu zajistí aktivaci při každém následujícím spuštění aplikačního programu (u Word je to soubor NORMAL.DOT). Při dalších spuštěních aplikace tak zůstává aktivní a může napadat všechny vytvářené, modifikované či jen čtené*

dokumenty. Toto samozřejmě není jediná cesta, jak se mohou makroviry šířit, je však rozhodně nejpoužívanější.“[4]



Obrázek 2-Nastavení zabezpečení maker v MS Office 2003

1.2.7 Spyware

Spyware bývá mnohdy uživateli nejrůznějších prapodivných „bezplatných“ aplikací podceňován, stejně jako ochrana před ním. Lze jej definovat jako program, který odesílá data z počítače bez vědomí uživatele. Jedná se zejména o statistická data – přehled navštívených stránek, soupis nainstalovaných programů či dokumentů. Tato statistická data jsou pak mnohdy využita pro cílenou reklamu. Spyware si mnohdy (vědomě) instalujeme s některými běžnými aplikacemi (např. některé verze multimediálního přehrávače BSPlayer), ale nikdy se přesně nedozvíme, jaká data odesílá, a zda nedochází k jejich zneužití. Kromě využívání antispywaru je tedy důležité věnovat pozornost instalaci programů a zejména popisu jejich licence – pokud jste při instalaci programu na spyware upozorněni, tak jde vlastně o legální (autorizovanou) činnost.

1.2.8 Adware

Adware je v některých důležitých ohledech podobný spywaru, resp. z něj vychází. Jde vlastně o propojení vašeho počítače a světa reklamy. Adware může představovat druh

[4] HÁK, Igor. Moderní počítačové viry. Hradec Králové, 2005. 110 s. Bakalářská práce. Univerzita Hradec Králové.

licence počítačových programů, mezi nejznámější programy s takovou licencí patří komunikační program ICQ. Adware (ať už označen i licencí a v licenčních podmínkách či nikoliv) zobrazuje uživateli reklamu, kterou přijímá z internetu (obsah této reklamy je mnohdy určen statickými daty, která byla získána právě pomocí spyware). Mnohdy si lze vybrat mezi verzí programu s reklamou či bez, samozřejmě ta s reklamou není nijak funkčně omezena a má většinou více funkcionalit. Kromě výše uvedeného jsou termínem adware označována i vyskakovací okna v internetovém prohlížeči (tzv. pop-up okna).

1.2.9 Hoax

Hoax je založen na lidské důvěřivosti, mnohdy až hlouposti. Jedná se o nejrůznější poplašné zprávy, které nejtypičtěji varují před nebezpečným virem. Šíří se buď e-mailem nebo v poslední době i pomocí sociálních sítí (Facebook, Twitter). Většina uživatelů zprávu zašle ostatním známým, a tak se zpráva šíří dál.

Databázi hoaxů spolu se souvisejícími informacemi lze najít na webové stránce http://www.hoax.cz.

Předmět:Fw: WAP Ericsson

Mili pratele,

Nas hlavni konkurent Nokia zacal prostrednictvim Internetu
rozdavat sve mobilni telefony. My u Ericssonu jsme presli
do protiutoku a zacali jsme rozdavat nejnovejsi WAP pristroje.
Tento mobil byl vyvinut pro zakazniky, kteri jsou fanousky
Internetu, tedy pro ty, co dovedou ocenit spickovou
technologii. Rozdavanim WAP telefonu ziskame odezvu od uzivatelu
a vybornou reklamu. Tvoji ulohou je poslat tuto zpravu osmi
pratelum a v prubehu dvou tydnu se dopracujes k telefonu
Ericsson T18. Kdyz posles tuto zpravu 20 pratelum,
dostanes nejnovejsi model WAP telefonu Ericsson R320.
Nezapomen tuto zpravu poslat i mne:
Anna.Svedlund@ericsson.com

Je to jediny zpusob, jak zjistit, kolika pratelum jsi poslal tuto zpravu.

Hodně zdaru preje Anna Svedlund - Executive Promotion Manager
for Ericsson Marketing.

Obrázek 3-Ukázka hoaxu - Mobilní telefon zdarma

(upraveno z http://hoax.cz/hoax/mobil-zdarma/)

1.2.10 Spam

Spam je označení pro nevyžádané sdělení (zprávu), která má většinou reklamní charakter a je hromadně šířena prostřednictvím internetu. Spam býval kdysi pouze součástí elektronických poštovních zpráv (e-mailů), postupem doby se rozšiřoval společně

s rozšiřováním internetových služeb, a tak jej dnes můžeme najít např. ještě v diskuzních fórech, ve službách umožňujících komunikaci v reálném čase (tzv. IM – Instang Messaging služby) a u dalších služeb.

1.2.11 Exploit

Exploit je speciální program s příkazy, které využívají nedostatků v zabezpečení aplikace, a díky tomu tak může útočník počítač na dálku ovládat a např. využívat jeho prostředků či instalovat svůj škodlivý software bez vědomí uživatele.

Chyba v aplikaci může být např. nedostatečně chráněný určitý port síťové komunikace v konkrétním firewallu, třeba Windows Firewall. Po odhalení takové chyby, ke kterému dojde většinou až díky útokům, které zmíněný nedostatek využijí, následuje vydání aktualizací, které chybu opraví (v našem případě aktualizace WindowsUpdate, resp. MicrosoftUpdate).

1.2.12 Phishing

Phishing označuje podvodné e-maily, které si kladou za cíl obohatit svého skutečného odesílatele na úkor příjemce. Phishing se zaměřuje zejména na falšování e-mailů z bank, což je v době internetového bankovnictví logické. Příjemce v e-mailu obdrží prosbu o vyplnění formuláře (např. z důvodu aktualizace údajů či přijetí nestandardní platby na jeho účet) a samozřejmě i související fingovaný odkaz, který pochopitelně nesměřuje na stránky banky, ale k podvodníkovi. Příjemce na něm poctivě vyplní svoje přihlašovací údaje do bankovnictví a ty odešle útočníkovi. Ten se pak díky nim přihlásí do skutečného internetového bankovnictví postiženého. Toto zpětné využití informací využívá principů tzv. sociálního inženýrství (to je jinak známo zejména v průmyslu – výrobce nejčastěji v Číně rozebere a prozkoumá originální výrobek, zpětně podle něj vytvoří dokumentaci a začne vyrábět jeho kopie).

Naštěstí většinu bankovních transakcí pomocí internetového bankovnictví je dnes třeba potvrdit pomocí SMS kódu zaslaného na mobilní telefon klienta, banky se rovněž snaží pomocí informačních kampaní své klienty varovat.

Obrázek 4-První phishingová bankovní zpráva v České republice (rok 2006)

(Převzato z http://www.viry.cz/viry.cz/novinky/060303a.gif)

1.2.13 Skriptové viry

Mezi nejčastější technologie na kterých jsou založeny skriptové viry, patří VBS (VisualBasic Script) a Java Script (Java). Z historického pohledu patřily mezi skriptové viry i dávkové BAT soubory, ale to je dnes opravdu výjimečná rarita.

Jednoduché, ale i přesto škodlivé skripty umí ve výše uvedených skriptovacích jazycích vytvořit každý pokročilejší tvůrce webových stránek. Skript s virem je pak nejběžněji umístěn do kódu HTML stránky a v případě nedostatečně zabezpečeného či benevolentně nastaveného internetového prohlížeče se může při prohlížení takové stránky aktivovat.

Další rozšířenou skupinou skriptových virů jsou ovládací prvky Active X, které využívá internetový prohlížeč Internet Explorer od Microsoftu. Implicitní nastavení, především starších verzí, tohoto prohlížeče způsobovalo, že viry obsažené ve skriptech Active X se spouštěly automaticky a měly dostatek prostoru pro svoje útoky. Naštěstí v novějších verzích Explorer je již tento problém s větší části potlačen, navíc jej řeší i rezidentní štíty a doplňky antivirových systémů.

1.2.14 Síťové viry

Mezi nejznámější síťové viry patří dva hlavní typy síťových útoků, tzv. DoS a DDoS.

DoS (Denial of Service, v překladu nedostupnost služby) je typ útoků, při kterém je napadaná služba (systém, server) přetížena požadavky, tím pádem je nedostupná a nemůže své služby poskytnout běžným uživatelům. K zahlcení služby dochází nejčastěji zaplavením jejího přístupu náhodnými daty, narušením nastavení, bráněním přístupu konkrétním uživatelům a podobně. Obranu představuje zejména logika ve formě preventivního systému na straně služby, která dokáže včas odlišit útok od běžného požadavku.

DDoS (Distributed DoS, distribuovaný DoS útok) je podobný standardnímu DoS útoku, ale k útoku jsou v tomto případě využity většinou tisíce napadených a zneužitých počítačů, které se najednou snaží ke službě připojit a tím způsobí její pád. Obrana proti takovému útoku je poměrně obtížná, nejčastěji spočívá v omezení přístupu jen pro určité rozsahy IP adres, velká část systémů souboj vzdá a službu dočasně odpojí.

1.2.15 Ostatní

1.2.15.1 Pharming

Pharming („farmaření“) je pokročilá verze phishingu, stejně jako phishing je zaměřena na získání citlivých údajů (nejčastěji přístupových dat k internetovému bankovnictví). Phishingovým útokům může zkušenější uživatel snadno předejít svojí zralou úvahou. Naproti tomu pharming využívá útok na DNS, kde nahradí překlad vybraných IP adres na falešné stránky. Adrese stránek banky tak nebude odpovídat správná IP adresa, ale falešná. Uživatel se po zadání adresy internetového bankovnictví (např. www.servis24.cz) nedostane na stránky banky, ale na falešné stránky, které vypadají obdobně jako stránky banky. Na stránkách vyplní své přihlašovací údaje k bankovnictví, následně se mu obvykle objeví chybová hláška o nedostupnosti služby a aniž by cokoliv tušil, tak své přihlašovací údaje právě sdělil podvodníkům. Pharming je tedy evidentně daleko více nebezpečnější než phishing, ale zároveň daleko náročnější na úroveň a přípravu útočníků.

1.2.15.2 Dialer

Dialer ohrožuje pouze uživatele, kteří se připojují k internetu pomocí vytáčeného spojení přes telefonní linku (tzv. dial-up připojení), tedy pomocí klasického analogového modemu.

Princip dialeru je jednoduchý – změní se tel. číslo vytáčené pro připojení k internetu a namísto klasického tarifu je zákazníkovi účtována zvláštní tarifikace (desítky Kč/min), zisk telefonní operátor vyplatí provozovateli linky se zvláštní tarifikací.

V České republice již dnes tento druh infiltrace ohrožuje zanedbatelné množství uživatelů, navíc moderní operační systémy, spolu se specializovaným softwarem, jej dovedou spolehlivě a bleskově odhalit. Dialer tak může představovat riziko hlavně v rozvojových zemích, kde se dial-up stále ještě hojně využívá. Na druhou stranu internetoví piráti se již věnují modernějším způsobům internetové kriminality (viz výše), a tak dial-up pro ně již nepředstavuje příliš lákavý nástroj výdělku.

2 Obecné možnosti ochrany proti počítačové infiltraci v OS Windows

V níže uvedené kapitole popisuji základní možnosti ochrany proti počítačové infiltraci pro počítače vybavené operačním systémem Microsoft Windows. Mezi tyto prvky ochrany patří zejména antivirový systém, firewall, antispyware, aktualizovaný operační systém i samotné aplikace a v neposlední řadě poučený a zodpovědný uživatel.

2.1 Základní technické prostředky ochrany proti infiltraci v OS Windows

Standardní prvky ochrany proti počítačové infiltraci představují zejména:

- Antivirový systém
- Antimalware
- Antispam - Ochrana proti spamu
- Firewall
- Automatické aktualizace OS a aktualizace programů
- Aktualizovaný internetový prohlížeč
- Rootkit a jeho detekce

2.1.1 Antivirový systém

Antivirový systém je počítačový program, který detekuje, zabraňuje přístupu či odstraňuje počítačové viry a jiné škodlivé programy (obecně malware). Antivir prohledává soubory na disku počítače a detekuje podezřelé chování programů. Další nezbytnou součástí antivirového systému je rezidentní štít, který v reálném čase monitoruje právě probíhající činnosti na vašem počítači. Antivirový systém je třeba pravidelně aktualizovat, neaktualizovaný postrádá účinnost.

2.1.2 Antimalware

Antimalware (resp. antispyware) chrání váš počítač před malware (spyware). Spyware jsou programy, které se pokoušejí odesílat data z vašeho počítače bez vašeho vědomí. Řada antispywarů je naštěstí dostupná bezplatně, mnohdy jsou i součástí antivirového systému (např. u Kaspersky Anti-Virus).

2.1.3 Antispam - Ochrana proti spamu

Některé internetové statistiky uvádějí, že až 90%[5] e-mailové komunikace představuje spam. Bohužel stále se ještě najdou uživatelé, kteří na evidentní spam reagují, činnost spammerů (odesílatelů spamu) se tedy díky nim stále vyplácí. K odesílání spamu se nejčastěji používají napadané počítače, jejichž majitelé naprosto nic netuší. Základní ochranu proti spamu představuje spamový filtr. Ten je dnes nezbytnou součástí poštovního serveru a automaticky třídí vaši poštu, ta nevyhovují nejčastěji skončí v příznačné složce „Spam“. Velice podařený spamový filtr má v tomto ohledu zejména e-mailová služba Googlu, tzv. Gmail – dokáže odhalit většinu spamů a jen málokdy se stane, že ve složce „Spam“ skončí regulérní e-mail. Spamový filtr je rovněž součástí vyšších antivirových systémů a je samozřejmě propojen s poštovním klientem (např. MS Outlook, Mozilla Thunderbird, The Bat!,...) , můžete si jej ale do počítače nainstalovat i samostatně, tato možnost ovšem není nijak hojně využívána.

2.1.4 Firewall

Softwarový firewall v rámci své základní funkce kontroluje jednotlivé pakety internetové komunikace. Kontroluje se zdrojová IP adresa vč. portu a cílová (opět včetně portu). Standardní nastavení každého firewallu blokuje určité nestandardní komunikační porty, ovšem pokud si uživatel některé či dokonce všechny porty bez omezení povolí, pak je činnost firewallu takřka zbytečná. Implicitní nastavení u většiny dnešních firewallů představuje odpovídající zabezpečení bez ohrožení uživatelského komfortu. Další funkcionality dnešních firewallů jsou popsány u jednotlivých produktů níže v práci (např. blokuje podezřelé servery a IP adresy, monitoruje pokusy o změnu systémových souborů, sleduje vstupní údaje z klávesnice a zabraňuje pokusům o jejich odeslání atp.).

Při kontrolování paketů pracuje firewall na čtvrté vrstvě standardizovaného modelu síťové komunikace (tzv. ISO/OSI model) – jedná o se o tzv. paketový filtr. Naproti tomu vyšší a novější firewally provádějí vlastní kontrolu dat předaných aplikaci na nejvyšší vrstvě tohoto modelu, tzv. aplikační vrstvě.

[5] SPAM už dělá přes 90% emailů. *Zpovedka.cz* [online]. 2010 [cit. 2012-06-06]. Dostupné z: http://www.zpovedka.cz/000431.php

V rámci firewallů se v uživatelském prostředí nejčastěji setkáváme s pojmem „personální firewall“. Jedná se o firewall určený pro koncové stanice, který brání útokům z interní (LAN) sítě.

Obrázek 5-Nastavení vyjímek u brány firewallu systému Windows

2.1.5 Rootkit a jeho detekce

Mezi méně známá bezpečnostní rizika patří bezesporu „rootkity“. Rootkit maskuje škodlivou činnost prováděnou na napadeném počítači tak, aby nebyla bezpečnostním softwarem odhalena. Jde zejména o maskování změn v systémových registrech či procesech. Většina dnešních antivirových systému v sobě naštěstí zahrnuje i detekci na přítomnost rootkitu.

2.2 Aktualizovaný software

2.2.1 Automatické aktualizace OS a aktualizace programů

Aktualizace vycházejí nejčastěji v momentě, kdy se objeví slabina či bezpečností riziko v daném produktu a je tedy následně třeba pomocí nich co nejrychleji zabezpečit váš počítač. Automatické aktualizace operačního systému jsou naprostým základem (více o nich v části Centrum zabezpečení). Je třeba ovšem aktualizovat i ostatní programy – např. Adobe Flash Player, který slouží k přehrávání animací a videí na internetu; aplikaci Java; Adobe Acrobat Reader, kancelářský balík (nejčastěji Microsoft Office) a další.

2.2.2 Aktualizovaný internetový prohlížeč

Internetový prohlížeč je třeba udržovat v dobré kondici tak, aby stíhal držet krok s novými bezpečnostními riziky. Kromě toho, že je třeba mít nastaven prohlížeč s nějakou rozumnou mírou zabezpečení (není možné internetovým stránkám povolit vše), tak je třeba jej pravidelně aktualizovat. Stará verze prohlížeče představuje obrovské bezpečností riziko. Sám Microsoft nedávno v rámci své osvětové a reklamní kampaně varoval své uživatele před používám internetového prohlížeče Internet Explorer 6 a doporučil jim přechod na novější verze.

2.3 Chování uživatele – největší riziko infiltrace

Počítačoví odborníci na celém světě se shodují, že největší riziko počítačové infiltrace představuje sám uživatel svými neuváženými zásahy a svým stylem práce s počítačem. Bohužel osvěta chybí a poučených a uvědomělých uživatelů je minimum. Této problematice se kvůli její důležitosti detailněji věnuji v samostatné části níže.

Systém Windows, ač se nám to mnohdy nezdá, patří mezi uživatelsky nejpřívětivější operační systémy a pracuje s ním tedy největší část počítačových uživatelů. Většina těchto uživatelů má pouze (základní) uživatelské znalosti práce s PC, a tak velice často představuje sama pro sebe obrovské bezpečnostní riziko. Pro lepší představivost se pokusím uvést konkrétní příklad:

Zvědavý teenager má nelegálně pořízené Windows od kamaráda, bezpečnostní aktualizace má vypnuté, přítomnost či aktuálnost antivirového systému neřeší, zuřivě instaluje všechny aplikace, které na internetu nalezne a které vypadají alespoň trochu lákavě. Dále má vypnutý firewall, aby mu neblokoval online hraní po internetu, ze zvědavosti kliká na odkazy, které mu chodí od neznámých zahraničních uživatelů (spam), stahuje software z pirátských internetových fór atd. Sám pro sebe tedy představuje obrovské riziko a je jen otázkou času, kdy jeho počítač začnou využívat počítačoví piráti např. k rozesílání spamu, odcizí jeho osobní data či dokonce finanční prostředky z bankovních účtů jeho rodičů, kteří využívají stejný počítač k přístupu na internetové bankovnictví.

Bohužel vyučující na školách či pořadatelé různých počítačových kurzů mnohdy podceňují bezpečnostní osvětu, a tak se ani nemůžeme divit, že jejich svěřenci se chovají tak, jak uvádím výše.

Sebelepší antivirový systém či jiný bezpečnostní prvek nedokáže ohlídat nezodpovědného či neznalého uživatele a to myslím bude platit ještě dlouhou dobu.

2.4 Centrum zabezpečení

Obecné, resp. spíše základní, možnosti zabezpečení počítače s operačním systémem Windows představuje tzv. „Centrum zabezpečení“. Tuto součást obsahují všechny systémy Windows od verze XP Service Pack 2 výše, tedy aktuálně navíc Vista a Windows 7.

Centrum kontroluje tři základní aspekty ochrany počítače. Nejprve přítomnost brány firewall, pokud systém neobsahuje alternativní bránu, tak lze použít tu, která je bezplatnou a standardní součástí samotného systému – Windows Firewall. Funkce paketový filtr ve firewallu kontroluje síťový provoz, tedy jednotlivé pakety a jejich adresování včetně zdrojového a cílového portu. Pro úplnost doplňuji, že klasický firewall naopak není program, ale síťové zařízení, které rovněž kontroluje síťovou komunikaci, ovšem na nižší vrstvě síťové komunikace. Integrovaný firewall samozřejmě poskytuje pouze základní možnosti kontroly a nastavení, většina uživatelů jej dokonce používá se základním automatickým nastavením, avšak pro koncové uživatelské počítače bez vlastní veřejné IP adresy, tj. počítače, které jsou součástí NAT, je myslím dostačujícím řešením.

Další nezbytnou součást Centra zabezpečení představují automatické aktualizace. Bohužel jejich důležitost a vliv na zabezpečení počítače mnohdy podceňují především domácí uživatelé, kteří vlastní nelegální licenci systému Windows, a tak mají příjem automatických instalací vypnutý, jelikož při stahování aktualizací systém kontroluje produktové číslo licence a pokud to je na seznamu čísel, které se vyskytují ve více instalacích, než je povoleno, tak může po nějaké době zobrazování varování na nelegálnost systému či znepříjemnění práce dojít až k jeho zablokování. Právě chyby v systémech, které „záplatují“ zmíněné aktualizace, však nejčastěji využívají útočníci k získání přístupu do vašeho počítače či vašich dat. Neaktualizovaný počítač připojený do sítě internet je tak logicky daleko více ohrožen. Bohužel tento jednoduchý fakt si většina uživatelů neuvědomuje a to i přesto, že z takto ohroženého počítače přistupuje např. do internetového bankovnictví. Přitom díky rozmachu open-source a bezplatných aplikací v posledních letech může být investice do nákupu licence operačního systému jediným výdajem uživatele za software, zde se opravdu nevyplatí šetřit každou korunu. Automatické aktualizace lze stahovat, ale i instalovat zcela automaticky, což je zároveň i výchozí možnost. Standardně lze přijímat aktualizace Windows Update, tzn. aktualizace

pouze pro Windows a základní aplikace (např. Internet Explorer), druhou vyšší možností je Microsoft Update – přijímáte aktualizace pro všechny produkty Microsoft (např. i pro kancelářský balík Microsoft Office). Kromě standardních aktualizací vycházejí vždy po nějaké době servisní balíčky (Service Pack), které sdružují všechny předchozí vydané aktualizace a mnohdy přinášejí do systému nějaké další možnosti či rozšíření.

Třetí základní součást představuje kontrola přítomnosti Ochrany proti malwaru (u Windows XP Ochrana proti virům). U Windows XP je tedy standardně kontrolována přítomnost antivirového systému, u Windows Vista a 7 navíc přítomnost škodlivého a nežádoucího softwaru (zejména spyware). Windows Vista a 7 totiž obsahují integrovanou základní ochranu proti spywaru, tzv. Windows Defender. Pro Windows XP je ovšem Defender taky určen, ale nenaleznete jej v základní nabídce Centra zabezpečení. Pokud používáte alternativní ochranu, lze jej částečně vypnout obdobně jako u firewallu. Navíc nejméně každý měsíc spolu s automatickými aktualizacemi přijímá systém i aktualizaci na kontrolu škodlivého softwaru za uplynulý měsíc. Centrum zabezpečení vás, co se týká antiviru, upozorňuje buď na jeho nepřítomnost nebo neaktuálnost. Důvodem neaktuálnosti antiviru může být nejčastěji chybějící funkční připojení k internetu či vypršená licence daného antivirového programu. Pro domácnost dostačují bezplatné antivirové systémy, takový dnes nabízí i samotný Microsoft, a to sice Microsoft Security Essentials. Ten je po kontrole legálnosti vaší instalace Windows na základě licence EULA dostupný pro nekomerční použití či „malý domácí obchod“.

U Windows Vista a 7 nalezneme kromě výše uvedených i „Další nastavení zabezpečení“, konkrétně jde o kontrolu nastavení zabezpečení internetu. Tato funkce hlídá nastavení internetového prohlížeče (při výchozích nastaveních je úroveň „OK“, ale pokud např. povolíte automatické spouštění Active X prvků pro všechny stránky bez ověření, tak vás centrum zabezpečení upozorní, že takové nastavení snižuje zabezpečení vašeho počítače).

Poslední součástí u Windows Vista a 7 je kontrola spuštění „Řízení uživatelských účtů“, tento doplněk pomáhá předcházet nežádoucím změnám ve vašem počítači. Řízení uživatelských účtů vás požádá o akceptaci či heslo správce, než se provedou požádané akce, které by mohly nepříznivě ovlivnit chod počítače nebo změnit nastavení pro ostatní uživatele. Nástroj rozlišuje čtyři druhy zobrazovaných zpráv[6]:

[6] Windows [online]. 2011 [cit. 2011-07-31]. Microsoft.com. Dostupné z WWW: <http://windows.microsoft.com/cs-CZ/windows-vista/What-is-User-Account-Control>.

 Funkce operačního systému Windows nebo program, který může ovlivnit i ostatní uživatele, potřebuje ke spuštění vaše povolení.

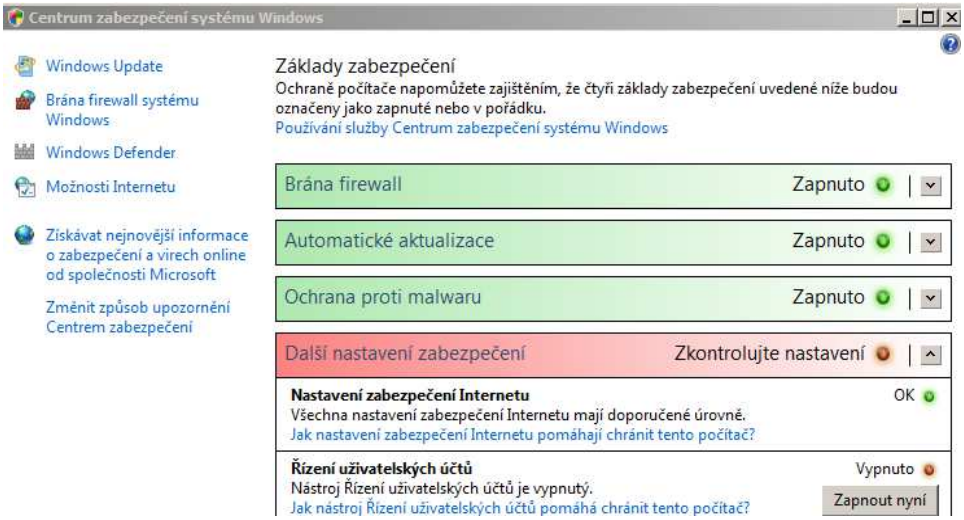
 Aplikace, která není součástí OS Windows, potřebuje ke spuštění vaši akceptaci. Aplikace má platný digitální podpis označující název programu a vydavatele.

 Neznámý program (program bez platného digitální podpisu) požaduje akceptaci ke spuštění.

 Tento program byl zablokován správcem, aby nemohl být v počítači spuštěn. Pro činnost tohoto programu je třeba, aby jej správce odblokoval.

Zejména u posledních dvou zpráv by měl být uživatel v pozoru, ovšem neznámý či blokovaný program vždy nutně neznamená riziko ohrožení vašeho počítače. V případě nejistoty doporučuji obracet se na speciální a především ověřená internetová fóra či stránky, kde lze k dané aplikaci dohledat relevantní informace.

Obrázek 6-Centrum zabezpečení (Windows XP)



Obrázek 7-Centrum zabezpečení (Windows Vista)

3 Porovnání kvality bezpečnostních produktů pro OS Windows

V dnešní době je k dispozici nepřeberné množství antivirových řešení. Pro běžného uživatele je tak velice obtížně se na trhu zorientovat a vybrat si pro sebe vhodný produkt. Stejně jako trh počítačů a informačních technologií se rozvijí i „trh“ se zneužíváním dat a počítačů, před těmito riziky je třeba se chránit. To si uvědomuje mnohem více softwarových společností a ty tak nabízejí stále větší počet bezpečnostních produktů, které mají chránit naše počítače. Následující dvě tabulky poskytují základní přehled většiny na trhu dostupných antivirových systémů, které mohou v prvotní fázi usnadnit výběr uživatelům.

Většina bezpečnostních řešení se v dnešní době prodává formou uceleného balíku, který obsahuje několik součástí (antimalware, antispyware, antispam, firewall). Bezplatná řešení obsahují zpravidla pouze antimalware, pokud uživatel chce více nástrojů, musí většinou zaplatit.

První tabulka níže uvedená zobrazuje v češtině dostupné, pro nekomerční použití bezplatně použitelné antiviry, včetně zobrazení dostupných nástrojů, informace o tom, zda je k dispozici i plnohodnotná 64 bitová verze.

Druhá tabulka představuje komerční AVS, kde kromě antimalwaru je většinou k dispozici minimálně firewall, případně antispyware nebo antispam. Součástí tabulky je i aktuální cena daného produktu za roční licenci pro jeden počítač (zdroj cen: Sw.cz - http://www.sw.cz, Zbozi.cz - http://www.zbozi.cz).

V obou tabulkách antivirových systémů jsou zobrazeny AVS, které se pravidelně účástní některého ze specializovaných testů antivirů (AV-comparatives, AV-test či VB). AVS, který se těchto testů neúčastní, ale zúčastňují se například pouze testů firewallů (test Matousek), nejsou v přehledových tabulkách obsaženy z důvodu, že nešlo nijak objektivně ohodnotit skutečnou kvalitu jejich vlastního antiviru (v jejich hodnocení musela být u všech antivirových testů použita hodnota median, nikde reálný výsledek), proto jsem logicky vlastní přehled zúžila pouze na antiviry, které se účastní testů určených pro antiviry.

3.1 Přehledové tabulky nekomerčních a komerčních AVS

Bezplatné AVS	Plná 64 bit verze*	Antimalware	Antispyware	Antispam	Firewall	Lokalizace	Cena vč. DPH 1 licence/rok
Avast Free	✖	✓	✖	✖	✖	✓	zdarma pro nekomerční použití
AVG Free	✓	✓	✓	✖	✖	✓	zdarma pro nekomerční použití
Avira Free	✓	✓	✖	✖	✖	✖	zdarma pro nekomerční použití
Clam-won	✖	✓	✖	✖	✖	✖	zdarma pro nekomerční použití
Comodo IS	✖	✓	✓	✖	✓	✖	zdarma pro nekomerční použití
Microsoft SE	✓	✓	✖	✖	✖	✓	zdarma do 10 PC i pro komerční použití (dle EULA podmínek)

*** Všechny aktuální verze AVS podporují 32/64 bit OS Windows (pod 64bit OS běží kompatibilní 32bit verze, tzn. emulovaná podpora), označeny jsou plnohodnotné 64bit verze (nativní podpora)**

Tabulka 1-Přehled nekomerčních AVS

Placené AVS	Plná 64 bit verze*	Antimalware	Antispyware	Antispam	Firewall	Lokalizace	Cena vč. DPH 1 licence/rok
Avast IS	✖	✓	✓	✓	✓	✓	899,00 Kč
AVG IS	✓	✓	✓	✓	✓	✓	899,00 Kč
Avira Premium IS	✓	✓	✓	✓	✓	✖	1 212,00 Kč
BitDefender IS	✓	✓	✓	✓	✓	✖	1 234,00 Kč
BullGuard IS	✖	✓	✖	✓	✓	✖	2 568,00 Kč
Comodo IS	✓	✓	✓	✓	✓	✓	1 250,00 Kč
Emsisoft	✓	✓	✓	✖	✖	✖	937,00 Kč
eScan	✖	✓	✓	✓	✓	✖	315 Kč***
Eset Smart Security	✓	✓	✓	✓	✓	✓	1 499,00 Kč
F-Secure IS	✖	✓	✓	✖	✓	✖	770,00 Kč
G Data IS	✖	✓	✓	✖	✓	✖	882 Kč***
GFI	✖	✓	✖	✖	✖	✖	1 259,00 Kč
K7	✓	✓	✓	✓	✓	✖	630 Kč***
Kaspersky IS	✖	✓	✓	✓	✓	✓	1 129,00 Kč
McAfee	✖	✓	✓	✓	✓	✓	960,00 Kč
Norman	✓	✓	✖	✓	✓	✖	1 295,00 Kč
Panda IS	✖	✓	✓	✓	✓	✖	1 572,00 Kč
PC Tools IS	✖	✓	✓	✓	✓	✖	740,00 Kč
Qihoo Antivirus	✖	✓	✖	✖	✖	✖	315 Kč***
SecurityCoverage	✓	✓	✖	✖	✖	✖	882 Kč***
Sophos	✖	✓	✓	✓	✓	✖	756 Kč***
Symantec Norton IS	✓	✓	✓	✓	✓	✓	1 028,00 Kč
TotalDefense IS	✖	✓	✓	✓	✓	✖	1 009,00 Kč
TrendMicro IS	✖	✓	✓	✓	✓	✖	1 440,00 Kč
TrustPort IS	✖	✓	✓	✓	✓	✓	786,00 Kč
Webroot IS	✖	✓	✖	✖	✓	✖	1 547,00 Kč

*** Všechny aktuální verze AVS podporují 32/64 bit OS Windows (pod 64bit OS běží kompatibilní 32bit verze, tzn. emulovaná podpora), označeny jsou plnohodnotné 64bit verze (nativní podpora)**
**** IS = Internet Security**
***** Není dostupný na českém trhu, přepočet cen z GBP dle kurzu ČNB ze dne 15.6.2012 (31,523 Kč/1 GBP), zdroj cen: amazon.co.uk**

Tabulka 2-Přehled komerčních AVS

3.2 Kritéria hodnocení AVS

Základní metoda testování antivirových systémů spočívá v tom, že se použije databáze škodlivých kódů, které testovací organizace průběžně aktualizují. Jednotlivé antiviry testují datové médium, kde se tyto kódy nacházejí, tím se zjistí, kolik škodlivých kódů odhalí (např. v databázi jich je 20 000, antivir odhalí 19 565, tím je dána i základní úspěšnost, v našem fiktivním případě 97,825 %). Součástí databáze jsou pochopitelně i neškodlivé kódy, pokud je antivir vyhodnotí jako škodlivé, tak se snižuje jeho spolehlivost detekce (jedná se o tzv. planý poplach). Při testech se rovněž zkouší odstranění viru ze zavirovaného počítače, testuje se, zda se vir podařilo z počítače odstranit úplně a již nepředstavuje žádnou hrozbu.

Dále se např. testují rezidentní štíty antivirů, prohlíží se nebezpečné webové stránky, které rovněž obsahují škodlivé kódy a antivir musí reagovat na jejich přítomnost, pokud nereaguje či naopak zareaguje i na neškodnou stránku, tak se opět snižuje jeho spolehlivost.

Rovněž se při podrobnějších testech či recenzích antivirů hodnotí náročnost programu na hardwarové vybavení počítače, vytížení počítače během testování, délka testování (některý program může teoreticky testovat shodné množství souborů pár minut a některý třeba i několik hodin), náročnost ovládání, velikost a perioda aktualizací, celkové vybavení antiviru (např. zda má i firewall), u placených produktů hraje svoji roli i cena.

Nejdůležitějším faktorem však bezpochyby zůstává vlastní spolehlivost detekce, které prověřují například souhrnné testy uvedené níže. Detailní skladba testů nebývá u profesionálních a ověřených společností k dispozici i proto, aby se na ni výrobci nemohli předem připravit.

3.3 Zvolené testy pro rozpoznávání kvality bezpečnostních řešení

Pro porovnání kvality jednotlivých bezpečnostních softwarových produktů jsem zvolila několik různorodých a mezi odborníky uznávaných testů. Konkrétně šlo u antivirů o testy VB100, AV-test.org, AV-comparatives.org a u firewallů o test Matousek.com. Skladba těchto testů je různorodá, stejně jako skladba testovaných produktů, nejznámější produkty jsou však zastoupeny u většiny z nich. Samozřejmě čím více testů se produkt zúčastnil, tím je jeho výsledek objektivnější.

V tabulce níže uvádím oblasti působnosti jednotlivých zvolených testů.

Zvolené testy	Detekce známých virů	Proaktivní ochrana	Detekce neznámých virů	Odstranění hrozeb	Dynamické testy	Firewall
VB100	✓	✗	✗	✗	✗	✗
AV-test.org	✓	✓	✓	✓	✗	✗
AV-comparatives.org	✓	✓	✓	✓	✓	✗
Matousek.com	✗	✗	✗	✗	✗	✓

Pozn.: **Detekce známých virů = Nalezení škodlivého kódu viru na testovaném datovém médiu.**
Proaktivní ochrana = Ochrana v reálném čase na základě monitorování činnosti jednotlivých aplikací (např. internetového prohlížeče) a uživatele.
Detekce neznámých virů = Detekce škodlivých kódů, které nejsou obsaženy přímo v databázi antivirového systému a je nutno ověřit podezřelý kód, např. heuristickou analýzou.
Odstranění hrozeb = Odstranění (vymazání) škodlivých či podezřelých kódů z počítače.
Dynamické testy = Testování na základě simulace běžné činnosti uživatele při práci s počítačem.

3.3.1 Virus Bulletin – VB100 Test 8/2011, 4/2012

Virus Bulletin je znám především díky svému ocenění VB100, které obdrží každý produkt, který úspěšně projde zkušební sadou testů. Základní kritéria pro obdržení tohoto ocenění jsou dvě – 100% detekce vzorků a žádný falešný poplach při skenování neinfikovaných souborů.

Detailní popisy jednotlivých testů nejsou k dispozici volně jako u předchozích dvou testů, ale je nutné si je zakoupit. Nicméně na stránkách VB100 lze dohledat stručné informace o použité metodě testování, tzv. RAP testování (proaktivní a reaktivní). Tento princip využívá nejčerstvější a doposud uschované vzorky v kombinaci s virovou databází

starší než vlastní vzorek, lze tak identifikovat, jak si produkty poradí s pro ně doposud neznámou nákazou.

VB100 přehledně archivuje veškeré výsledků testů a lze tak dohledat informace o úspěšnosti a odezvách výrobců jednotlivých bezpečnostních řešení v časové ose.

Vzhledem k tomu, že výsledkem tohoto testu je pouze obdržení certifikace „VB100“ při bezchybné a úplné detekci a nikoliv výsledné pořadí produktů, uvádím přehledovou tabulku z testu ze srpna 2011 a dubna 2012:

AVS	VB 8/2011	VB 4/2012	VB Celkem
Avast Free	100,00%	100,00%	Ano
Avast IS	100,00%	100,00%	Ano
AVG Free	Neprošel	100,00%	Ne
AVG IS	100,00%	100,00%	Ano
Avira Premium IS	100,00%	100,00%	Ano
BitDefender IS	100,00%	100,00%	Ano
BullGuard IS	100,00%	100,00%	Ano
eScan	100,00%	100,00%	Ano
Eset Smart Security	100,00%	100,00%	Ano
F-Secure IS	100,00%	Neprošel	Ne
G Data IS	100,00%	100,00%	Ano
GFI	100,00%	100,00%	Ano
Kaspersky IS	100,00%	100,00%	Ano
Microsoft SE	100,00%	100,00%	Ano
Sophos	100,00%	Neprošel	Ne
TotalDefense IS	100,00%	100,00%	Ano

Pozn. Bezplatné AVS vyznačeny modře

Tabulka 3-Srovnávací test VB100 8/2011, 4/2012

(Upraveno z http://www.virusbtn.com/vb100/archive/summary)

Ve výsledném porovnání jsem použila celkový výsledek, v případě splnění testu je hodnota 100 %, v případě nesplnění 0 %.

3.3.2 AV-test.org 8/2011[7]

Institut AV-test provádí každoročně více než 3000 srovnávacích a individuálních testů bezpečnostních produktů. Použité vzorky jednotlivých škodlivých kódů jsou z důvodu nezávislosti tvořeny a sestavovány pomocí vlastní analýzy. Detailní představu o hodnocení jednotlivých produktů pomocí AV-test.org lze získat z přílohy, kde je přeložen výstup z detailního testu bezplatné aplikace Avast! Free.

[7] AV-TEST - The Independent IT-Security Institute. AV-TEST [online]. 2011 [cit. 2011-10-14]. Test Reports > Quarter 2/2011. Dostupné z WWW: <http://www.av-test.org/en/tests/test-reports/quarter-22011/>.

Všechny produkty jsou testovány ve třech kategoriích se stejnou stupnicí (0 nejhorší-6 nejlepší) a to detekce, oprava a použitelnost.

Ve své práci jsem použila srovnávací test ze srpna 2011:

Produkt	Výsledek (0 nejhorší – 6 nejlepší)				
	Detekce	Oprava	Použití	CELKEM	%
BitDefender: Internet Security 2011 & 2012	6	5	5,5	**5,5**	**91,7**
Kaspersky: Internet Security 2012	6	4,5	5	**5,2**	**86,1**
F-Secure: Internet Security 2011	5,5	5	5	**5,2**	**86,1**
Panda: Internet Security 2012	5,5	5	5	**5,2**	**86,1**
AVG: Internet Security 10.0	5	4,5	5	**4,8**	**80,6**
G Data: Internet Security 2012	5,5	4,5	4	**4,7**	**77,8**
Panda: Cloud Antivirus Free 1.5.1	5	3,5	5,5	**4,7**	**77,8**
AVG: Anti-Virus Free Edition 10.0	5	3,5	5,5	**4,7**	**77,8**
SecurityCoverage: SecureIT Plus 2011	4,5	3	6	**4,5**	**75**
Symantec: Norton Internet Security 2011	5	3	5	**4,3**	**72,2**
Qihoo: 360 Antivirus 2.0	5	4,5	3	**4,2**	**69,4**
Avast: Free AntiVirus 6.0 (Int. Security)*	5	2,5	5	**4,2**	**69,4**
Avira: Premium Security Suite 10.2	4	4	4,5	**4,2**	**69,4**
BullGuard: Internet Security 10.0	4,5	3	4,5	**4**	**66,7**
Trend Micro: Titanium Internet Security 2011	4,5	2	5	**3,8**	**63,9**
GFI: Vipre Antivirus Premium 4.0	4,5	3,5	3,5	**3,8**	**63,9**
ESET: Smart Security 4.2	3,5	2,5	5	**3,7**	**61,1**
Microsoft: Security Essentials 2.0	2,5	3,5	5	**3,7**	**61,1**
PC Tools: Internet Security 2011	4	4	2,5	**3,5**	**58,3**
Emsisoft: Anti-Malware 5.1	5	2,5	2,5	**3,3**	**55,6**
McAfee: Total Protection 2012	4	2	4	**3,3**	**55,6**
Total Defense: Internet Security Suite 2011	2,5	3,5	3	**3**	**50**
Webroot: Internet Security Complete 7.0	2	3,5	3,5	**3**	**50**
K7 Computing: Total Security 11.1	2	3	2,5	**2,5**	**41,7**
Norman: Security Suite Pro 8.0	2	2	3	**2,3**	**38,9**

***Avast Internet Security netestuje Av-test.org samostatně ; ** Bezplatné AVS označeny modře**

Pozn.: Detekce = Nalezení škodlivého kódu viru na testovaném datovém médiu.
Oprava = Odstranění nebo zablokování nalezeného škodlivého kódu.
Použití = Uživatelská použitelnost aplikace (rychlost, úroveň nastavení atp.).

Tabulka 4-Srovnávací tabulka AV-test.org 8/2011

(upraveno z http://www.av-test.org/en/tests/test-reports/quarter-22011/)

3.3.3 AV-Comparatives.org – Testy AVS 2011[8]

AV-Comparatives.org provádí souhrnné testování bezpečnostních produktů zhruba jednou za tři měsíce.

Použité vzorky jednotlivých škodlivých kódů jsou podobně jako u AV-test z důvodu nezávislosti tvořeny a sestavovány pomocí vlastní analýzy. Všechny vzorky jsou

[8] AV-Comparatives.org. AV-Comparatives.org [online]. 2011 [cit. 2011-10-14]. Antivirus Comparatives 2011. Dostupné z WWW: <http://www.avcomparatives.org/images/stories/test/ondret/summary2011>.

zkopírovány na server, následně dojde k jejich případnému dešifrování a rozbalení z archivů, rovněž k odstranění duplicit. Názvy souborů jsou systematicky a jednoznačně pojmenovány. Automatický nástroj doplňuje správnou spustitelnou příponu všem souborům, nerozpoznané formáty dostávají příponu *.VIR a jsou odděleny do zvláštního prostoru. Vzorky jsou analyzovány specializovanými nástroji AV-Comparatives, ale i nástroji antivirové komunity, nefunkční vzorky jsou odstraněny, notoricky známé vzorky se nepoužívají v hlavním testu. Malware je analyzován v zabezpečeném prostředí AV-Comparatives. Viry jsou prověřeny replikací, při které se zároveň odhaluje, zda se soubor chová jako virus, pokud ne, tak může být vyřazen z hlavní databáze vzorků. Testovací sety AV-Comparatives neobsahují vzorky, které nejsou schopné provozu pod OS Windows NT/2000/2003/XP či Vista. Makra starší než z verze Office 97 jsou rovněž vyřazena, podobně jako notoricky známé HTML soubory. Ověřené a probrané vzorky jsou detailně tříděny dle kategorií (worms, backdoors,..), dojde k jejich opětovné validaci a následně k téměř finálnímu zařazení do vlastních testovacích setů. Před vlastním spuštěním testovacích setů ještě totiž dochází k opětovné kontrole a případné úpravě složení setů. Po otestování dochází k analýze zpracování jednotlivých vzorků a porovnání s výsledkem testovaných antivirů. Tato analýza má opět vliv na složení budoucích testovacích vzorků.

Ve své práci jsem použila dostupné testy antivirů z roku 2011, abych kromě více různých nezávislých testů zahrnula i více období – v každém období se liší skladba testů, a tím se může lišit i výsledek jednotlivých programů. Použití více období je tedy objektivnější.

AV-Comparatives se obecně zaměřuje na výkonnostní testy, testy celých produktů, testy odstranění a opravy infekce, testy potencionálně nežádoucích aplikací a další.

Přehled výsledků jednotlivých testů AV-Comparatives uveden níže:

AVS	Test detekce malware 02/2011	Heuristický test 02/2011	Výkonnostní test 07/2011	Komplexní dynamický test za 03-06/2011	Test detekce malware 8/2011	Heuristický test 08/2011	Výkonnostní test 08/2011	Test odstraňování malware 11/2011	Komplexní dynamický test za 08-01/2011	Celkový výsledek
Avast!	ADV	N/A	ADV+	ADV+	ADV+	ADV	ADV+	STD	STD	73,3%
AVG	STD	N/A	ADV+	STD	ADV	N/A	ADV+	STD	ADV	56,7%
Avira	ADV+	ADV+	ADV+	ADV	ADV+	ADV+	ADV+	ADV	ADV	93,3%
BitDefender	ADV+	ADV	ADV	ADV+	ADV+	ADV+	ADV	ADV+	ADV+	93,3%
eScan	ADV+	ADV	N/A	N/A	ADV	ADV	ADV	N/A	N/A	46,7%
ESET	ADV	ADV	ADV+	ADV+	ADV+	ADV+	ADV+	STD	ADV	87,8%
F-Secure	ADV+	ADV	ADV+	ADV+	ADV+	ADV+	ADV+	STD	ADV+	92,2%
GDATA	ADV	ADV	ADV	ADV+	ADV+	ADV+	ADV	STD	ADV+	85,6%
K7		N/A	ADV+			N/A	ADV+	STD	STD	33,3%
Kaspersky	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	100,0%
McAfee	ADV+	N/A	ADV		ADV	ADV	ADV+	ADV	N/A	54,4%
Microsoft	ADV	ADV	N/A	N/A	ADV	ADV	ADV+	ADV	N/A	55,6%
Panda	ADV	ADV	ADV+	ADV+	ADV+	ADV	ADV+	STD	ADV	85,6%
PC Tools	STD	N/A	STD			N/A	STD	ADV+		27,8%
Qihoo 360	STD	N/A	ADV	ADV	ADV	ADV	STD	STD	ADV+	63,3%
Sophos	ADV	STD	ADV+	STD	N/A	N/A	ADV+	STD	ADV+	53,3%
Symantec	ADV	N/A	ADV+	ADV	ADV	N/A	ADV+	ADV+	ADV+	71,1%
TrenMicro	STD	N/A	ADV	ADV+	ADV+	N/A	ADV	ADV	ADV	63,3%
TrustPort	ADV+	ADV	N/A	N/A	ADV	ADV	STD	N/A	N/A	43,3%
Webroot		N/A	STD		N/A	N/A	ADV+	ADV		25,6%

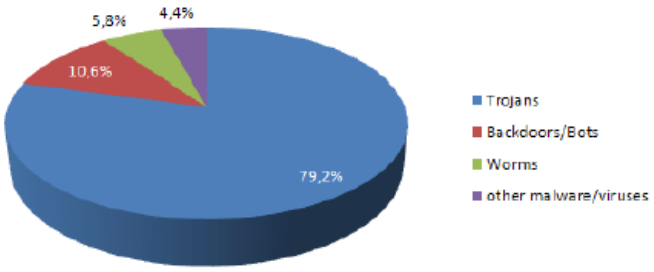
*ADV+=100 %, ADV=80 %, STD=50%, ostatní 0 %

Pozn. : Test detekce malware = Nalezení škodlivého kódu viru na testovaném datovém médiu.
Heuristický test = Detekce škodlivých kódů, které nejsou obsaženy přímo v databázi antivirového systému a je nutno ověřit podezřelý kód.
Výkonnostní test = Test rychlosti práce AVS, zejména rychlosti skenování dat.

Tabulka 5-Srovnávací tabulka AV-Comparatives.org 2011

(upraveno z http://www.av-comparatives.org/images/stories/test/ondret/summary2011)

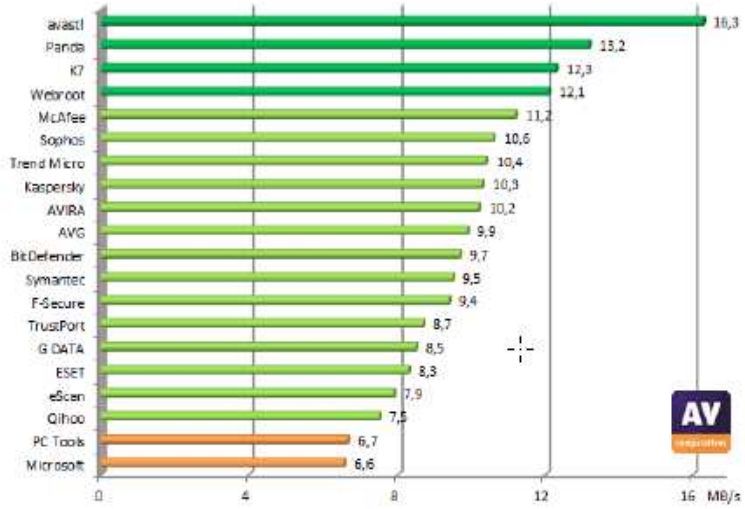
Graf níže zobrazuje skladbu použitých škodlivých kódů v testu malware za období 2/2011. Nejvíce (79,2 %) jsou zastoupeni trojské koně (v orig. Trojans), dále byly podílem 10,6 % zastoupeny boot viry a tzv. zadní vrátka (Bots, Backdoors), téměř polovičním podílem (5,8 %) jsou zastoupeni červi (worms), ostatní malware tvoří skladbu testů z 4,4 %.



Graf 1-Podíl použitých druhů nákaz (celkem 400 škodlivých kódů

(Zdroj: http://www.av-comparatives.org/images/stories/test/ondret/avc_od_feb2011.pdf)

V rámci prevence ochrany proti škodlivým kódům je nutné pravidelně testovat data ve vašem počítači na výskyt škodlivých kódů. V případě, že máte velký pevný disk nebo dokonce několik pevných disků s velkým množstvím dat, tak je pro vás zajímavá hodnota rychlosti skenování antiviru. V rámci testu 2/2011 AV-Comparatives.org byl nejrychlejší systém Avast!, který byl zhruba 2,5x rychlejší než nejpomalejší systém od Microsoftu, což znamená, že testování vašeho počítače by trvalo 2,5x menší dobu. Jedná se sice o důležitý parametr, ale kromě něj je třeba zohlednit kvalitu a výsledek skenování, nejrychlejší totiž ne vždy znamená kvalitní v detekci.



Graf 2-Porovnání rychlosti skenování (MB/s)

(Zdroj: http://www.av-comparatives.org/images/stories/test/ondret/avc_od_feb2011.pdf)

3.3.4 Matousec.com Proactive Security Challenge[9]

V rámci testování firewallů jsem se rozhodla vycházet z nejdůležitějšího a nejuznávanějšího portálu – matousec.com. Tento server podrobuje firewally specializované sadě 148 testů. Testování probíhalo v deseti úrovních, ke každému produktu lze stáhnout podrobný popis testování v PDF souboru, na serveru lze rovněž nalézt oficiální reakce výrobců k výsledkům testů. V příloze je přeložen popis z testu vítězného produktu Comodo IS.

V testu bohužel chybí firewall integrovaný ve Windows, Windows Firewall, který odborná veřejnost do podobných testů záměrně nezařazuje, jelikož ho nepovažuje za plnohodnotný firewall se všemi možnostmi a funkcionalitami, nicméně jelikož jeho funkční výbava je skutečně pouze základní, tak by se jistě umístil spíše ve spodní části žebříčku.

Výsledky z posledního testu, který byl v říjnu 2011 k dispozici, uvádím zde:

Comodo Internet Security 5.3.176757.1236 FREE	100%	10+	Vynikající – 100 %
Online Solutions Security Suite 1.5.14905.0	99%	10+	Vynikající
Privatefirewall 7.0.25.4FREE	98%	10+	Vynikající
Outpost Security Suite Free 7.0.4.3418.520.1245.401FREE	97%	10+	Vynikající
Outpost Security Suite Pro 7.5.1.3791.596.1681	97%	10+	Vynikající
BitDefender Internet Security 2011 14.0.30.357	97%	10+	Vynikající
Kaspersky Internet Security 2012 12.0.0.374	93%	10+	Vynikající
Malware Defender 2.7.3.0002FREE	91%	10+	Vynikající
PC Tools Internet Security 2011 8.0.0.655	90%	10+	Velmi dobrý
Jetico Personal Firewall 2.1.0.10.2451	88%	10	Velmi dobrý
ZoneAlarm Extreme Security 2012 10.0.250.000	72%	9	Dobrý
Lavasoft Personal Firewall 3.0.2293.882**	67%	8	-
Rising Internet Security 2011 23.00.41.42	34%	5	Velmi špatný
CA Internet Security Suite Plus 2011 7.0.0.279	30%	5	Velmi špatný
Norton Internet Security 2012 19.1.1.3	20%	3	-
Avast! Internet Security 6.0.1000	15%	3	-
Dr.Web Security Space Pro 6.0.2.07290	14%	3	-
F-Secure Internet Security 2011 10.51.106	9%	2	-
Trend Micro Internet Security Pro 2010 17.50.1647.0000	9%	2	-
FortKnox Personal Firewall 6.0.205.0	7%	2	-
ZoneAlarm Free Firewall 9.2.076.000FREE	7%	2	-
ESET Smart Security 4.2.64.12	6%	2	-
AVG Internet Security 2011 10.0.1153	3%	1	-
Avira Premium Security Suite 10.0.0.608	3%	1	-
Look 'n' Stop 2.07	3%	1	-

[9] Difinex, Ltd. Proactive Security Challenge [online]. 2011 [cit. 2011-06-28]. Matousec.com. Dostupné z WWW:<http://www.matousec.com/projects/proactive-security-challenge/results.php>.

Sunbelt Personal Firewall 4.6.1861.0	3%	1	-
G Data InternetSecurity 2011 21.1.1.0	2%	1	-
McAfee Internet Security 2011 11.5.141	2%	1	-
Panda Internet Security 2011 16.00.00	2%	1	-
TrustPort Internet Security 2011 11.0.0.4584	2%	1	-

*** Bezplatné produkty vyznačeny modře**
**** Produkt byl testován pouze 84 testy, jedná se o starší verzi produktu**

Tabulka 6-Matousec.com - Hodnotící tabulka firewallů

(upraveno z http://www.matousec.com/projects/proactive-security-challenge/results.php)

3.4 Celkové porovnání a přepočet výsledků AVS a firewallů

Celkové srovnání výsledků jednotlivých bezpečnostních produktů je zobrazeno v tabulkách níže. Jednotlivé testy mají přiřazenou určitou váhu podle toho, jak komplexní test je, čím méně má druhů testů, tím menší je jeho váha.

U testu AV-Comparatives.org jsem písemným hodnotám přiřadila následující hodnoty: ADV+=100 %, ADV=80 %, STD=50%, ostatní 0 %. V tabulce je uveden průměr ze všech testů za rok 2011, pokud produkt nějaký test vynechal, tak nebyl započítán. Pokud se produkt testů AV-Comparatives.org vůbec nezúčastnil, ale má v sobě funkci AVS, tak je počítáno s celkovým medianem hodnot (bezplatné i placené produkty souhrnně), díky tomu může u tohoto i ostatních testů dojít ke zkreslení. V případě, že daný produkt vůbec nemá funkci AVS, je počítáno s hodnotou 0 %. Ve výsledném hodnocení (resumé) má tento test váhu 40 %.

VB test má dvě kritéria splnil/nesplnil (100 %/ 0 %), resp. celkově se počítá s hodnotou za oba dva uvedené testy, pokud splnil v obou uvedených testech, je výsledek 100 %, jestli nesplnil nejméně v jednom testu pak 0 %. V případě neúčasti antiviru je rovněž použit souhrnný median, pokud produkt nemá funkci AVS, je opět použita hodnota 0 %. Ve výsledném hodnocení má tento test váhu 10 %.

AV-test.org zobrazuje výsledky z testu detekce, v případě neúčasti AVS opět použiji hodnotu celkového medianu, pokud nemá funkci AVS 0 %. Ve výsledném hodnocení má tento test váhu 40 %.

Test Matousek je zaměřen na firewally, jsou v něm tedy převážně jiné produkty, které se ostatních testů neúčastnily, kromě bezpečnostních balíků, které mají rovněž firewall. U AVS bez firewallu je hodnota 0 %, v případě neúčasti, pokud systém obsahuje funkci firewallu, tak opět celkový median. Kvůli svému úzkému zaměření má váhu 10 %.

Bezplatné AVS (FW)	VB 8/2011, 4/2012	VB 8/2011, 4/2012 přepočet	AV-test 8/2011	AV-test 2011 přepočet	AV-comp. 2/2011	AV-comp 2/2011 přepočet	Matousek	Matousek - přepočet	Resumé přepočet
Comodo IS	N/A	10,00%	N/A	27,76%	N/A	24,00%	100,00%	10,00%	71,76%
MalwareDef	N/A	10,00%	N/A	27,76%	N/A	24,00%	91,00%	9,10%	70,86%
Panda Cloud Antivirus Free	N/A	10,00%	N/A	27,76%	N/A	24,00%	77,80%	7,78%	69,54%
Avast Free	100,00%	10,00%	69,40%	27,76%	73,30%	29,32%	-	0%	67,08%
Microsoft SE	100,00%	10,00%	61,10%	24,44%	55,60%	22,24%	-	0%	56,68%
AVG Free (u AV-comp komerční verze)	0%	0%	77,80%	31,12%	56,70%	22,68%	-	0%	53,80%
PrivateFirewall Free	-	0%	-	0%	-	0%	98,00%	9,80%	9,80%
OutPost Sec Free	-	0%	-	0%	-	0%	97,00%	9,70%	9,70%
ZoneAlarm Free	-	0%	-	0%	-	0%	7,00%	0,70%	0,70%

***AV-Comparatives.org: ADV+=100 %, ADV=80 %, STD=50%, v tabulce průměr ze všech testů za rok 2011**

**** Neúčast v testu = souhrnný median se zohledněním váhy testu (AV-test 27,76%, AV-comp. 24 %, VB 10 %, Matousek 1,5 %)**

*****Median nemůže reálně nahradit neúčast v testu = údaje jsou přibližné**

****** Absence antiviru (u testu firewallů) - 0 %, absence firewallu (u testu AVS) - 0%**

Tabulka 7-Celkové porovnání nekomerčních produktů

Placené AVS (FW)	VB 8/2011, 4/22012	VB 8/2011, 4/2012 přepočet	AV-test 8/2011	AV-test 2011 přepočet	AV-comp. 2011	AV-comp. 2011 přepočet	Matousek	Matousek - přepočet	Resumé přepočet
Kaspersky IS	100,00%	10,00%	86,10%	34,44%	100,00%	40,00%	93,00%	9,30%	93,74%
BitDefender IS	100,00%	10,00%	91,70%	36,68%	93,30%	37,32%	97,00%	9,70%	93,70%
Panda IS	N/A	10,00%	86,10%	34,44%	85,60%	34,24%	2,00%	0,20%	78,88%
G Data IS	100,00%	10,00%	77,80%	31,12%	85,60%	34,24%	2,00%	0,20%	75,56%
Avira Premium IS	100,00%	10,00%	69,40%	27,76%	93,30%	37,32%	3,00%	0,30%	75,38%
F-Secure IS	0,00%	0,00%	86,10%	34,44%	0,922	36,88%	9,00%	0,90%	72,22%
Online Solutions	N/A	10,00%	N/A	27,76%	N/A	24,00%	99,00%	9,90%	71,66%
OutPost Sec Pro	N/A	10,00%	N/A	27,76%	N/A	24,00%	97,00%	9,70%	71,46%
Eset Smart Security	100,00%	10,00%	61,10%	24,44%	0,878	35,12%	6,00%	0,60%	70,16%
ZoneAlarm Extreme Sec	N/A	10,00%	N/A	27,76%	N/A	24,00%	72,00%	7,20%	68,96%
Symantec Norton IS	N/A	10,00%	72,20%	28,88%	0,711	28,44%	N/A	1,50%	68,82%
Avast (u AV-test free verze)	100,00%	10,00%	69,40%	27,76%	73,30%	29,32%	15,00%	1,50%	68,58%
SecurityCoverage	N/A	10,00%	75,00%	30,00%	N/A	24,00%	N/A	1,50%	65,50%
AVG IS	N/A	10,00%	80,60%	32,24%	56,70%	22,68%	3,00%	0,30%	65,22%
Rising IS	N/A	10,00%	N/A	27,76%	N/A	24,00%	34,00%	3,40%	65,16%
Dr. Web	N/A	10,00%	N/A	27,76%	N/A	24,00%	14,00%	1,40%	63,16%
Qihoo Antivirus	N/A	10,00%	69,40%	27,76%	0,633	25,32%	-	0%	63,08%
FortKnox	N/A	10,00%	N/A	27,76%	N/A	24,00%	7,00%	0,70%	62,46%
BullGuard IS	100,00%	10,00%	66,70%	26,68%	N/A	24,00%	N/A	1,50%	62,18%
GFI	100,00%	10,00%	0,639	25,56%	N/A	24,00%	N/A	1,50%	61,06%
eScan	100,00%	10,00%	N/A	27,76%	46,70%	18,68%	N/A	1,50%	57,94%
Emsisoft	N/A	10,00%	55,60%	22,24%	N/A	24,00%	N/A	1,50%	57,74%
TotalDefense IS	100,00%	10,00%	50,00%	20,00%	N/A	24,00%	N/A	1,50%	55,50%
TrustPort IS	N/A	10,00%	N/A	27,76%	43,30%	17,32%	2,00%	0,20%	55,28%
McAfee	N/A	10,00%	55,60%	22,24%	54,40%	21,76%	2,00%	0,20%	54,20%
PC Tools IS	N/A	10,00%	58,30%	23,32%	27,80%	11,12%	90,00%	9,00%	53,44%
Norman	100,00%	10,00%	38,90%	15,56%	N/A	24,00%	N/A	1,50%	51,06%
Sophos	0,00%	0,00%	N/A	27,76%	0,533	21,32%	N/A	1,50%	50,58%
Webroot IS	N/A	10,00%	50,00%	20,00%	0,256	10,24%	N/A	1,50%	41,74%
K7	N/A	10,00%	41,70%	16,68%	0,333	13,32%	N/A	1,50%	41,50%
TrendMicro IS	N/A	10,00%	63,90%	25,56%	0,063	2,52%	9,00%	0,90%	38,98%

Jetico FW	-	0%	-	0%	-	0%	88,00%	8,80%	8,80%
Lavasoft FW	-	0%	-	0%	-	0%	67,00%	6,70%	6,70%
Look 'n' stop	-	0%	-	0%	-	0%	3,00%	0,30%	0,30%
Sunbelt Personal FW	-	0%	-	0%	-	0%	3,00%	0,30%	0,30%

***AV-Comparatives.org: ADV+=100 %, ADV=80 %, STD=50%, v tabulce průměr ze všech testů za rok 2011**
**** Neúčast v testu = souhrnný median se zohledněním váhy testu (AV-test 27,76%, AV-comp. 24 %, VB 10 %, Matousek 1,5 %)**
*****Median nemůže reálně nahradit neúčast v testu = údaje jsou přibližné**
****** Absence antiviru (u testu firewallů) - 0 %, absence firewallu (u testu AVS) - 0%**

Tabulka 8-Celkové porovnání komerčních produktů

3.5 Zhodnocení celkového výsledku testu

Jak vyplývá z tabulky, mezi nekomerčními antiviry dopadl v testech nejlépe Comodo Internet Security (resumé po přepočtu 71,76 %). Na druhé pozici skončil Malware Defender (70,86 %). Oba navíc kromě antiviru obsahují i firewall. Třetí v pořadí skončil produkt Panda Cloud Antivirus Free (69,54 %). Všechny tři první produkty se však neúčastnily ani jednoho testu zaměřeného na antiviry, byl u nich testován pouze firewall, svého výsledku tedy dosáhly díky použití hodnoty medianu. Navíc ani jeden z nich není dostupný v českém jazyce, což je u bezplatného antiviru zaměřeného na domácí uživatele, často bez bližších znalostí práce s počítačem a anglického jazyka, dle mého, zásadní problém.

V porovnání komerčních produktů zvítězil Kaspersky Internet Security (93,74 %), v těsném rozdílu za ním zůstal druhý produkt BitDefender Internet Security (93,70 %). Obě aplikace představují již ucelené a kompletní bezpečnostní balíky.

Při podrobnějším pohledu na výsledky jednotlivých produktů bych ráda zmínila Panda Internet Security, která má takřka vynikající výsledky v oblasti antimalware, ale slabý firewall, který celému balíčku výrazně sráží na hodnocení. Obdobný problém má i produkt G Data Internet Security.

Porovnání výsledků testů ukázalo, že pro důsledné zabezpečení počítače se vyplatí si připlatit za komerční produkt, který především díky širšímu spektru nástrojů a tím pádem i možností ochrany získává v testech vyšší hodnocení (celkový výsledek po přepočtu u nejlepšího komerčního produktu je 93,74% oproti 71,76 % u nekomerčního). Na druhou stranu i řada renovovaných placených produktů se umístila až za svojí neplacenou konkurencí, např. v České republice populární Eset Smart Security.

Z výše uvedeného vyplývá, že ne vždy je třeba kupovat placený produkt, ten se vyplatí zejména tehdy, pokud počítač skutečně aktivně a náročně využíváte, např. s internetovým bankovnictvím či v něm máte skutečně důležitá chráněná data, a potřebujete jistotu jeho zabezpečení. V takovém případě bych zvolila produkt Kaspersky Internet Security.

Pro zabezpečení běžného domácího počítače doporučuji pro znalce anglického jazyka pochopitelně vítězný produkt Comodo Internet Security. Pro ostatní podle mne postačuje i bezplatný antivir Avast! Free Antivirus v kombinaci s bezplatným firewallem OutPost Security Free, který skončil pouhé 1 % za dalším bezplatným firewallem Private Firewall Free, ale dlouhodobě je úspěšnější a domácí uživatel se v něm daleko snáze a rychleji zorientuje, navíc výrobce nabízí i jeho komerční alternativu. V testech bezplatný Avast! Free Antivirus dopadá nadprůměrně, za produkty Malware Defender a Panda Cloud Antivirus Free ve výsledku zaostal jen proto, že se ani jeden z nich neúčastnil antivirových testů a oba dva měly vysoké hodnocení z jediného testu, kterého se zúčastnily, tj. testu Matousek. Navíc Avast! Free Antivirus je dostupný v češtině a má poměrně přehledné ovládání, což může být pro řadu uživatelů rozhodující.

4 Představení vybraných produktů

4.1 Výsledek srovnání antivirů a bezpečnostních balíků

Velká část renomovaných testovacích serverů (viz předchozí kapitola) netestuje současně bezplatnou a placenou verzi produktů od jednoho výrobce, jelikož obě mají většinou shodné jádro programu, tento fakt jsem tedy musela začlenit i do mého srovnání. Například AV-test testoval z produktů společnosti Avast pouze bezplatnou verzi, její výsledky jsem tedy zařadila mezi výsledky ostatních testovacích serverů, které testovaly komerční verzi, použitá hodnota dle mého více odpovídá skutečnosti než median, který je použit v případě neúčasti v testu.

V rámci přepočtených hodnot se nejlépe umístily produkty BitDefender Internet Security a Kaspersky Internet Security a to zcela jednoznačně, jelikož oba produkty se zúčastnily všech testů. U bezplatných produktů, jak již uvádím v zhodnocení výše, je výsledek trochu problematický. Nejlépe dopadl produkt Comodo Internet Security, který se ale zúčastnil jen testu firewallů, stejně jako druhý v pořadí Malware Defender, třetí skončil Panda Cloud Antivirus Free. Z tohoto důvodu je hodnocení zjevně zkresleno, Comodo je poměrně známá bezpečnostní společnost, která má, jak lze odvodit z odborných diskusí na portálech Zive.cz (http://www.zive.cz) či Viry.cz (http://www.zive.cz), řadu uživatelů i v České republice, ale produkty Malware Defender a Panda zde nejsou příliš rozšířené, oba dva jsou navíc pouze v angličtině, jak již nastiňuji v předchozí kapitole. Jsem přesvědčena, že mezi běžnými domácími uživateli by se tak příliš neuplatnily, proto místo jejich popisu v práci popisuji a hodnotím bezplatné produkty společností AVG a Avast, které jsou lokalizované, zúčastnily se více testů a s ohledem na celkové výsledky skončily s nadprůměrným hodnocením.

Právě produkt Avast! Free Antivirus, který je z velké části vyvíjen v České republice, skončil sice zdánlivě čtvrtý mezi bezplatnými produkty, ale dá se říct, že i první v rámci těch produktů, které se zúčastnily i vlastních testů antivirů, ne pouze testu firewallů. V popisech níže uvádím stručně i druhého českého zástupce v pořadí – produkty AVG (Internet Security, Anti-Virus Free), které jsou v České republice známé a rozšířené, proto mi přišlo pro úplnost vhodné je do popisu zahrnout. U produktů AVG ovšem test VB100 odhaluje, že poměrně vysoká úspěšnost produktu je vykoupena vyšší mírou chybných detekcí, kdy neškodný program je detekován jako vir.

AVG Internet Security ztrácí na Avast! Internet Security pouze minimálně, na BitDefender a Kaspersky již o něco více. Větší rozdíl je mezi produkty AVG Anti-Virus Free a Avast! Free Antivirus, tam je znatelný rozdíl, proto z této dvojice jednoznačně doporučuji produkt Avastu.

Vzhledem k tomu, že každým dnem se na poli internetové bezpečnosti objevují nové a nové hrozby, s kterými se každý výrobce vypořádává pokaždé jinak, tak nelze jednoznačně určit, zda je lepší produkt BitDefender či Kaspersky, Kaspersky má ovšem výhodu v kompletní lokalizaci do českého jazyka.

Bezpochyby lze ale prohlásit, že rozdíl mezi placenými a neplacenými antiviry v rámci detekce není tak velký, jak bychom čekali. Testy rovněž ukazují, že bezplatný antivir od Avastu a AVG je v kombinaci s jinými bezplatnými produkty (např. OutPost Free) plně dostačují a vyrovná se velké části placených řešení.

Na základě porovnání výsledků testů, ale i na základě vlastní zkušenosti, doporučuji pro jednoduchou ochranu domácího počítače bezplatný český antivir od Avastu. Program je uživatelsky přívětivý, je v českém jazyce, v případě potřeby je k němu dostupná, nejen na internetu, řada informací, v neposlední řadě však celkově dosahuje nadprůměrných výsledků v uvedených testech.

Pro méně zkušené uživatele je však výhodnější placené komplexní řešení ve formě bezpečnostního balíčku, které obsahuje nejen antivir, ale i další části. Uživatel se nemusí o nic starat, většinou vše funguje automaticky v jednom produktu. Vlastní antivir je u placených či neplacených produktů obdobně kvalitní, ale chybí další funkcionality, jako například antispyware či antivir, v tom je hlavní výhoda placených balíčků. Z placených řešení doporučuji balíček od společnost Kaspersky, který má bohatou výbavu, a jedná se o plně lokalizovaný produkt. Pokud vám angličtina nedělá problém, tak lze doporučit i vítěze testů – BitDefender Internet Security.

4.2 Popis vybraných a otestovaných AVS

4.2.1 Bezplatné antivirové systémy

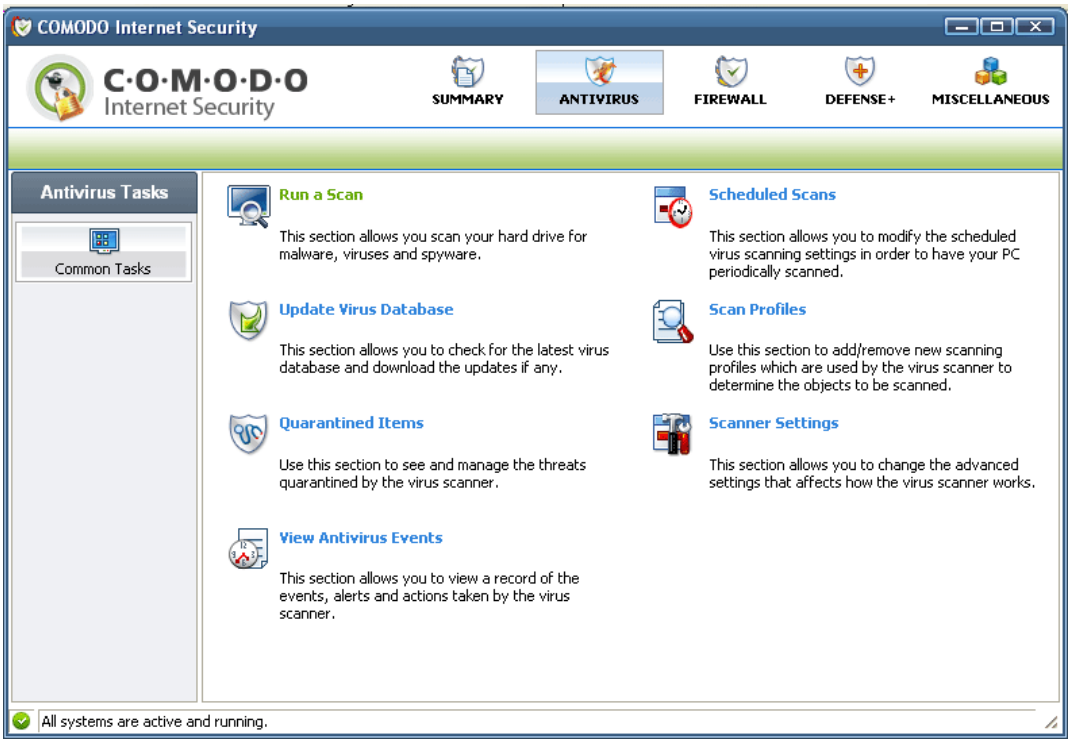
4.2.1.1 Comodo Internet Security - Comodo Antivirus

Comodo Antivirus je pro nekomerční účely k dispozici zdarma a to buď samostatně, nebo jako součást bezpečnostního balíčku Comodo Internet Security. Ačkoliv se balíček Comodo IS umístil v testu bezplatných produktů na první pozici, tak vlastní antivirus prakticky otestován nebyl, jelikož se neúčastnil ani jednoho z testů zaměřených na antiviry, jeho výsledky v těchto testech tedy představuje pouze median.

Kromě standardní ochrany proti malwaru obsahuje Comodo Antivirus, resp. Comodo IS, integrovaný i antispyware. Aktuální dění na počítači a činnost uživatele sleduje rezidentní štít označený “Defense+”, který díky integraci s technologií “Auto Sandbox” implicitně izoluje všechny podezřelé soubory, aby nemohly upravit ostatní data v počítači.

Při testování dat na přítomnost škodlivého kódu využívá Comodo databáze a výpočtu umístěných na vzdáleném serveru, který zpracovává a vyhodnocuje data zaslaná z testovaného počítače, jedná se o tzv. princip cloudu. V cloudu je umístěn i seznam důvěryhodných výrobců software (tzv. whitelisting), s kterým Comodo porovná instalované a provozované aplikace.

Celkově se jedná o povedený produkt s řadou pokročilých technologií, bohužel z důvodu chybějící lokalizace není pro domácí uživatele bez znalosti odborné počítačové angličtiny úplně vhodným řešením.



Obrázek 8-Comodo Internet Security – Antivirus

(Převzato z http://download.chip.eu/ii/4717163070_007558e8de.gif**)**

4.2.1.2 Avast! Free Antivirus

Avast! Free Antivirus je pro domácí (osobní) nekomerční použití dostupný zcela zdarma, nyní již ve verzi 6 a v českém jazyce. Autorem programu je původně ryze česká společnost Avast Software (dříve Alwil Software). Program je dostupný i v 64 bitové verzi. Součástí bezplatné verze tohoto programu je kvalitní antivirový a antispywarový systém, pochopitelně včetně rezidentního štítu, který monitoruje aktivity probíhající na počítači, pokud zaregistruje nějakou podezřelou, tak hned upozorní uživatele či provede předdefinované opatření. Stejně tak v sobě Avast obsahuje okamžitou detekci a blokaci rootkitů.

I bezplatná verze dále nabízí službu WebRep, která hodnotí spolehlivost a bezpečnost webových stránek, výsledky se pak zobrazují rovnou v prohlížeči při vyhledávání nebo přístupu na danou stránku. Oproti AVG Free však chybí anti-spyware.

Dobrovolně se lze účastnit Avast! CommunityIQ – Avast pak získává vaše data o surfování a ty zpracovává tak, aby na základě jejich analýzy podchytil všechny z nich získané bezpečnostní hrozby.

Avast bojuje proti konkurenci především rychlostí svojí práce, resp. rychlosti skenování, za kterou bývá pravidelně oceňován v odborných mediích (např. magazínu

AV-Comparatives.org). Avast skenuje rychlostí 16,3 MB/s, naproti tomu například níže uvedený antivir AVG rychlostí 9,9 MB/s.

Program je nutné jednoduše zaregistrovat (vyplněním jména, příjmení, e-mailu a informací, odkud jste se o produktu dozvěděli). Tuto jednoduchou registraci je pak nutné opakovat každý rok – program na to uživatele včas upozorní, avšak já v tom vidím drobnou nevýhodu. Nutnost každoročně obnovovat bezplatnou licenci může laickým uživatelům činit problém, prodloužení či registraci licence neprovedou včas a používají pak antivir se zastaralou databází, který sice zdánlivě funguje, ale ve skutečnosti před aktuálními hrozbami rozhodně nechrání.

V českých domácnostech se jedná o jeden z nejrozšířenějších a prověřených bezplatných antivirů a to zejména díky nenáročné obsluze a spolehlivému rezidentnímu štítu. Osobně tento program několik let používám na jednom ze svých počítačů a již několikrát mě svým rezidentním štítem zachránil od nákazy škodlivým kódem, proto jej i z vlastní zkušenosti mohu rozhodně doporučit.

Obrázek 9-Možnosti testování u aplikace Avast! Free Antivirus

(Převzato z http://avast.anti-virus.cz/design/images/avast-free-antivirus02.jpg)

4.2.1.3 AVG Anti-Virus Free Edition

Společnost AVG (dříve Grisoft), která má opět český původ, narozdíl od Avastu svůj bezplatný antivir tolik nepropaguje a dává spíše přednost svým komerčním řešením, což je pochopitelné. Na českých oficiálních stránkách programu tak lze získat pouze minimum informací, odborné servery se rovněž spíše věnují komerční verzi.

Tento produkt se v základu skládá z antiviru doplněného rezidentním štítem, ostatně rezidentní štít je dnes povinná výbava libovolného antiviru ať bezplatného či komerčního.

AVG v testech spolehlivosti detekce antivirů patří rovněž mezi ty spolehlivější produkty, které se pravidelně objevují na špici hodnocení. Bezplatná verze dokonce, a to považuji za velkou výhodu, nabízí anti-spyware, kontrolu odkazů v internetovém prohlížeči (Link Scanner) či automatickou kontrolu elektronické pošty v běžných poštovních klientech, resp. přenášenou běžnými poštovními protokoly. Pro další komponenty (např. firewall) již je zapotřebí zakoupit placený balík AVG IS.

Celý antivir a všechny jeho komponenty pracují po instalaci implicitně samostatně v plně automatizovaném režimu, což je výhoda pro méně zdatné uživatele, jelikož po nich není zbytečně vyžadována akce, u které by nevěděli, jak s ní naložit.

Kromě bezplatné verze pro desktopová zařízení nabízí společnost i ochranu chytrých telefonů a zařízeních s operačním systémem Android – AVG Mobilation, obdobných a přitom bezplatných produktů není zatím mnoho, z tohoto důvodu zde uvádím i tuto poznámku. Podle mne tak AVG chytře a nenápadně upozorňuje uživatele této mobilní platformy i na své ostatní produkty.

Jelikož se bezplatné AVG s produktem Avast! Free v testech antivirů pohybují na podobné úrovni a často si vzájemně mění pořadí (u AV-test první AVG, u AV-comparatives Avast), tak podle mne mohu pro ochranu běžného domácího počítače AVG i proto, že se jedná o produkt známé a velké bezpečnostní společnosti s velkým a dlouhodobým zázemím, doporučit.

Obrázek 10-AVG Anti-Virus Free - Výřez úvodní obrazovky

4.2.2 Komerční AVS

4.2.2.1 BitDefender Internet Security

BitDefender je komplexní bezpečnostní balík, který nabízí kvalitní a testy prověřenou ochranu. Největší nevýhodu především pro méně zkušené uživatele vidím v absenci české lokalizace, na druhou stranu je i v dnešní době stále dost kvalitních produktů, které jsou k dispozici nejčastěji pouze v angličtině, pro zkušenější uživatele by se tak nemělo jednat o nepřekonatelný problém. Méně zkušený uživatel si většinou bude pořizovat masivněji propagovaná řešení českých či u nás známějších společností (např. AVG, Avast, Eset).

Hlavní součástí balíčku je kvalitní antimalware Antivirus 2012, který lze poměrně detailně konfigurovat, kromě antispamu obsahuje řešení od BitDefender i antiphishing (upozorňování před možnými podvodnými e-maily). Počítač, tedy určité aplikace či zvolené webové stránky, resp. internet obecně, lze rovněž blokovat pomocí rodičovské ochrany. Přístup k internetu lze povolit/zakázat dokonce v konkrétně zvolený čas. Produkt rovněž dokáže monitorovat vaši domácí Wi-Fi síť a upozornit na každý nový počítač, který se do ní chce připojit. Mezi další nástroj patří možnosti ukládat vybrané soubory či složky v šifrované formě.

Hlavní negativum vidím pouze v již zmíněné absenci lokalizace a dále v prostoru, který produkt zabírá na disku počítače (až 2.8 GB, z toho 800 MB musí být na disku, kde

je systém), při dnešní velikosti a cenách pevných disků v tom však nevidím až tak velký problém.

Obrázek 11-BitDefender Internet Security 2012 - Úvodní obrazovka programu

(Převzato z http://download.bitdefender.com/resources/themes/awake2012/images/screenshots/en/is/MainView.png)

4.2.2.2 Kaspersky Internet Security

Produkt jedné z největších bezpečnostních společností nabízí opět několik ucelených součástí pro komplexní zabezpečení počítače a ochranu dat. Kromě antimalwaru, antispywaru, firewallu a antispamu obsahuje další níže popsané funkcionality.

Funkce SafeSurt kontroluje obsah prohlížených webových stránek a propojením na databázi Kaspersky zároveň varuje před vstupem na nebezpečné stránky.

Anti-phishingová ochrana společně s kontrolou proti zneužití zadaných vstupních uživatelských dat (zadávání hesel klávesnicí) zvyšuje bezpečnost při práci s internetovým bankovnictvím či e-shopem, jelikož varuje před podvodnými stránkami a blokuje podvodné odesílání dat zadaných klávesnici pro aplikace odlišné od té, která si vstup těchto informací vyžádala.

Rodičovská kontrola je ve stejném rozsahu jako u BitDefender (blokován může být internet, zvolené stránky či aplikace), vše lze opět doplnit blokací jen v určený čas.

Kaspersky zároveň kontroluje přístupy k systémových souborů u jednotlivých aplikací a pokud dojde u konkrétní aplikace k jejich změně, tak je uživatel upozorněn (např. při aktualizaci programu na novou verzi).

Program dále nabízí Safe Run – běh podezřelých stránek a aplikací v odděleném prostoru (tzv. sandbox), kde nemůže dojít jejich během k poškození počítače či ostatních aplikací.

Kaspersky rovněž nabízí po instalaci možnost vytvoření záchranného disku, který lze použít v případě obnovy systému. V nových verzích operačního systému Windows Vista a Windows 7 lze rovněž do miniaplikací přidat gadget Kaspersky, který zobrazuje aktuální informace o zabezpečení vašeho systému.

Celkově lze produkt Kaspersky IS určitě doporučit, jelikož nabízí všechny potřebné nástroje, je v testech dlouhodobě úspěšný, je plně v češtině, nabízí bohaté možnosti nastavení, ale na druhou stranu i automatický mód, při kterém chce po uživateli minimum akcí.

Obrázek 12-Kaspersky Internet Security 2012 - Úvodní obrazovka

(Převzato z http://www.swmag.cz/assets/clanky/2012-03/clanek00936/upload/photo/large_KIS_1.jpg)

4.2.2.3 AVG Internet Security

AVG Internet Security popisuji z toho důvodu, aby byl jednoznačně patrný rozdíl v množství komponent mezi bezplatným (AVG Free) a placeným produktem (IS). Právě balík AVG obsahuje velké množství přidaných nadstandardních modulů a komponent, a proto lze na něm přehledně deklarovat reálnou přidanou hodnotu placeného komerčního řešení.

Komplexní bezpečnostní balík od společnosti AVG se rovněž honosí označením Internet Security. AVG zatím nedisponuje oddělenou 64 bitovou verzí, nicméně 32 bitová verze je plně kompatibilní s 64 bitovými OS. Česká verze je ovšem samozřejmostí. AVG uvádím, ačkoliv v souhrnných testech skončil až jako pátý z důvodu toho, že většina jeho vývoje se odehrává v České republice a jednalo se o první komerčně celosvětově úspěšný AVS, jehož vývoj započal v České republice.

Oproti volně dostupné verzi obsahuje klasické doplňky, tj. firewall, anti-spyware a anti-spam. Dalšími doplňky jsou například: AVG Accelator (urychluje start systému a přehrávání internetových videí založených na technologii Adobe Flash), AVG System Tools (monitoruje počítač a umožňuje odhalit a vypnout aplikace, které automaticky startují po načtení Windows) či AVG Identity Protection (monitoruje aktivity na počítači, chrání zejména před odcizením identity a osobních údajů).

Aplikace AVG obsahuje narozdíl od konkurence několik opravdu specifických služeb, které výrazně přesahují typickou skladbu bezpečnostního balíku. Nicméně cílová orientace produktu AVG je jednoznačná - běžného a méně zdatného uživatele přítomnost takových služeb potěší a pomůže mu při jeho běžné práci nejen na internetu, ale i se samotným počítačem.

Obrázek 13-Porovnání možností AVG Anti-Virus a AVG Internet Security

(Převzato z: http://www.avg.com/cz-cs/internet-security)

4.3 Výsledek srovnání firewallů

V čele tabulky se umístil bezplatný bezpečnostní balík od společnosti Comodo, jehož samotný firewall je shodný s tím, který popisuji ve své práci. Vzhledem k tomu, že tento bezplatný produkt v rámci testů dlouhodobě předčívá své placené konkurenty, mohu jej jednoznačně doporučit, největším handicapem bude zřejmě pouze absence české lokalizace.

Placený produkt Outpost Security Suite Pro, jehož samotný firewall je opět shodný s tím, který v práci popisuji, se umístil rovněž na předních příčkách. Pokud tedy hledáte firewall pro komerční použití, jelikož z licenčních důvodů (jen nekomerční použití) nemůžete použít produkt Comodo a angličtina pro vás není překážkou, mohu Outpost rovněž doporučit. OutPost Security Suite získal sice o 2 % nižší hodnocení než konkurenční produkt Online Solutions, ale narozdíl od něj nabízí stejně kvalitní firewall i v nekomerční variantě a je více rozšířen v České republice, proto místo řešení Online Solutions níže popisuji právě jej.

Osobně bych ale možná přece jen dala přednost placenému produktu od Comodo Internet Security Pro nebo Internet Security Plus, za srovnatelnou cenu totiž nabízejí komplexní a o něco spolehlivější produkt. Firewall v placeném balíku Comodo je shodný, resp. stejně kvalitní, proto jej neuvádím zvlášť v komerčních produktech, ale pouze jednou v rámci neplacené varianty.

Pro úplnost uvádím i stručný popis firewallu integrovaného přímo v operačním systému Windows a to zejména proto, že je v poslední době velice rozšířen v domácnostech, kde často doplňuje bezplatný antivirus.

4.4 Popis vybraných a otestovaných firewallů

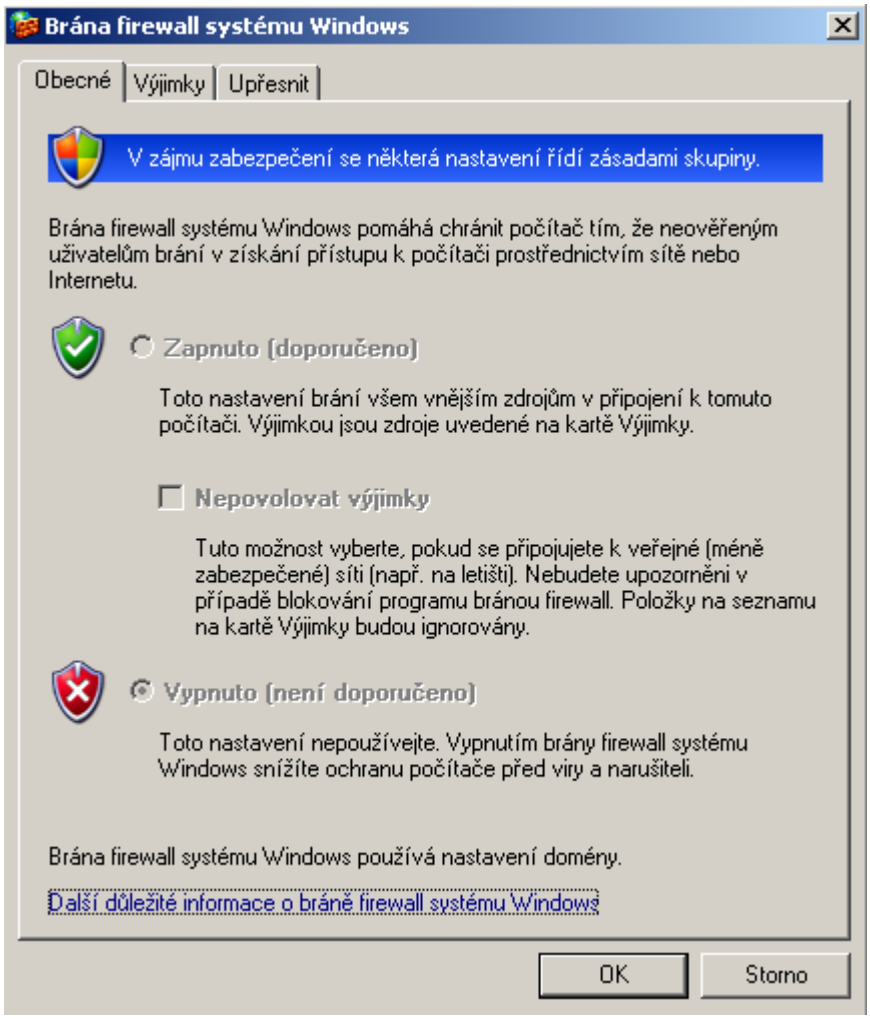
4.4.1 Bezplatné firewally

4.4.1.1 Windows Firewall

Standardní součástí operačního systému je již řadu let (od verze Windows XP SP2) brána „Windows firewall“. Nejedná se tedy úplně o bezplatný firewall, ale firewall je již v ceně operačního systému, záleží jen na vás, zda jej budete aktivně využívat či nikoliv, cena OS je stejná, tak jako tak, firewall je jen přidanou hodnotu. Vzhledem k tomu, že moje práce je zaměřena na počítače právě s OS Windows, tak jej v práci uvádím, ačkoliv se vlastních testů firewallů zpravidla nezúčastňuje z toho důvodu, že má jen základní funkce. Brána obsahuje základní možnosti monitoringu a tím i ostrahy síťového spojení.

Windows firewall splňuje základní funkcionalitu firewallu, která postačuje většině běžných uživatelů, kterým navíc vyhovuje, že vše funguje v implicitním režimu automaticky bez nutnosti konfigurace z jejich strany, což je hlavní výhoda oproti jiným nástrojům od specializovaných společností, které požadují po uživateli řadu akcí či úprav

nastavení. Na druhou stranu pak ale díky tomu přinášejí větší možnosti kontroly a monitoringu síťového provozu než Windows firewall.



Obrázek 14-Brána firewall systému Windows – Úvodní obrazovka

4.4.1.2 Comodo Internet Security – Comodo Firewall

Comodo Firewall 5.5 je distribuován samostatně nebo jako součást Comodo Internet Security, je známý pro domácí (nekomerční) použití bezplatný firewall, bohužel rovněž v anglickém jazyce. V testech matousec.com, cnet, ICSAlabs, Virus Bulletin se pravidelně umisťuje na předních příčkách a mnohdy dokonce před placenými konkurenty. Comodo Internet Security se účastnil pouze testu firewallů Matousek, kde se umístil na první pozici, jelikož se ale tento balík neúčastnil žádného jiného testu, kde by byla otestována i jeho druhá část, tzn. antivirus, tak zde popisuje pouze vlastní firewall.

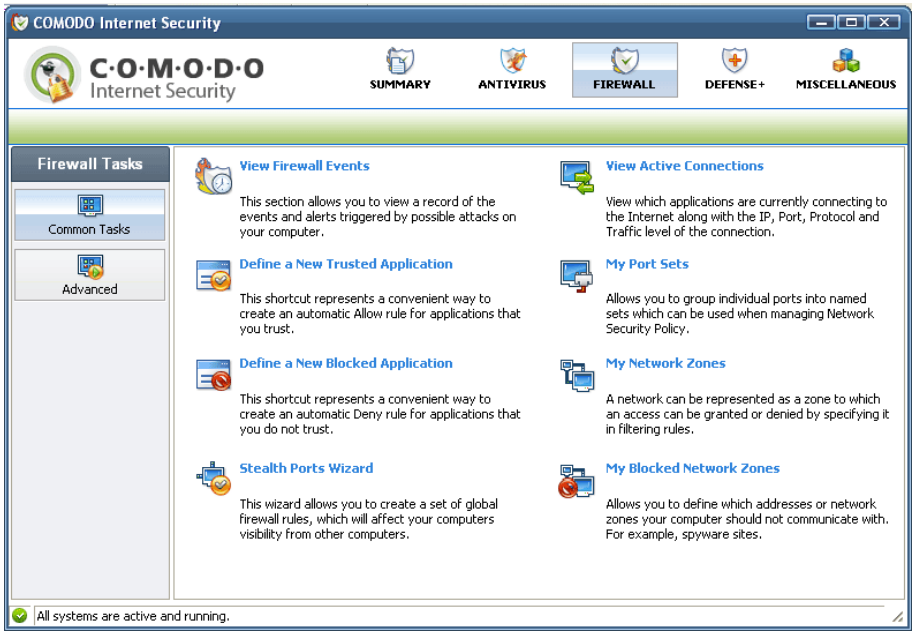
Kromě klasické detekce útoků na porty a kontroly souborů běžících na počítači obsahuje i základní monitoring malwaru díky DDP (Default Deny Protect) – seznamu potencionálně nebezpečných PC, které jsou automaticky blokovány. Dále technologii Auto

SandBox, která automaticky spouští potencionálně nebezpečné soubory v omezeném virtuálním prostředí.

Zkušenější uživatel může rovněž využít možnost analýzy chování podezřelých aplikací – firewall sleduje pokusy o změny DLL knihoven, změny operační paměti u jednotlivých procesů, DNS dotazy. Všechny tyto funkce jsou ve výchozím nastavení aktivní. Dále můžete omezit maximální počet paketů přenášených během jedné sekundy, při startu OS lze rovněž vypnout odchozí síťovou komunikaci. Comodo dále uchovává přehledné výpisy (odborně tzv. logy) síťové komunikace, které mohou pomoci při řešení vašich problémů (např. proč mně netiskne síťová tiskárna).

Společnost Comodo kromě firewallu nabízí rovněž řadu dalších bezplatných aplikací, kromě firewallu lze využít i bezplatný antivirus, který uvádím výše, k dispozici tak vlastně máte jednoduchý a bezplatný bezpečnostní balík od jediného výrobce. Balík však nemusíte ani skládat, jak již píši v úvodu, Comodo jej nabízí jako ucelený produkt, Comodo Internet Security, překvapivě rovněž zcela zdarma.

Dlouhodobé výsledky srovnávacích testů hovoří jasně, označují produkt Comodo za spolehlivý.



Obrázek 15-Comodo Internet Security - Firewall

(Převzato z http://download.chip.eu/ii/4717163070_007558e8de.gif)

Obrázek 16-Comodo Firewall - Nastavení zabezpečení

(Převzato z http://portforward.com/english/routers/firewalling/Comodo/ComodoFirewall/ComodoFirewall5.jpg)

4.4.2 Komerční firewally

4.4.2.1 Outpost Firewall Pro

Firewall „Outpost Firewall Pro“ od společnosti Agnitum je momentálně dostupný ve verzi 7 a to v anglickém jazyce. Tento firewall má dlouholetou tradici a patřil mezi první firewally určené pro operační systém Windows. V testu firewallů Matousek dosáhl vynikajícího ohodnocení (97 %) a nabízí i stejně kvalitní nekomerční bezplatnou alternativu, což je hlavní důvod, proč jej zde detailněji popisuji.

OutPost Firewall Pro je jako většina firewallů schopen provozu v plně automatickém režimu či pokročilém systému správy detailních síťových pravidel, což je ostatně jeden z důvodu, proč jej využívají i počítačoví profesionálové. Na firewall obsahuje trochu netradičně integrovaný modul antispyware, což je sice výhoda, ale na druhou stranu to může i vadit některému AVS, který má rovněž v sobě integrovaný antispyware, a může tak docházet ke kolizím mezi oběma aplikacemi.

Celkově se jedná o zajímavý produkt, pokud uživatel vysloveně hledá placená řešení, tak jde určitě o jednu z možných variant, nicméně osobně se přikláním ke konkurenčnímu produktu Comodo, který je lepší v testech a zároveň i ucelenější.

Obrázek 17-Outpost Firewall Pro - Úvodní obrazovka

(Převzato z http://www.fileflash.com/graphics/screens/Agnitum_Outpost_Firewall_Pro-191.gif)

Závěr

Při psaní této práce jsem zjistila, že bez ohledu na výrobce jsou si téměř všechny antivirové systémy či bezpečnostní balíky velice podobné, částečně to platí rovněž o firewallech, u bezpečnostních balíků řada výrobců dokonce užívá shodné a evidentně velice oblíbené marketingové označení „Internet Security“. Základní skladba produktů v takovém balíku je rovněž shodná, technologie k zabezpečení počítače a k detekci škodlivých kódů jsou si taktéž často podobné, ačkoliv každý výrobce se snaží právě tu svoji označovat jako unikátní a nejlepší na trhu. Jednotlivé produkty tak odlišují hlavně drobné, nicméně uživatelsky často velice zajímavé, doplňky.

Nákup antiviru či bezpečnostního balíku nelze rovněž uskutečnit na základě výsledků jednoho internetového testu, je třeba prostudovat více nezávislých testů za delší časový úsek – to, že některý výrobce včas či vhodně nezareagoval na určitý nový druh počítačové infekce, neznamená, že příště nepřijde s nejúčinnějším typem ochrany. Myslím, že v tomto ohledu se stačí spoléhat na produkty renomovaných značek s dlouholetou tradicí v oblasti počítačové bezpečnosti, což ostatně potvrzují např. výsledky společnosti Kaspersky ve výše uvedených testech.

Vzhledem k vzrůstající oblibě „cloud-computingu“ a s tím souvisejícím přesunem aplikací a dat z pevného disku osobního počítače na síťový disk serveru budou v následujících letech ještě více vzrůstat nároky zabezpečení zejména na poskytovatele webových aplikací, služeb a úložišť. Osobní počítač by měl být výhledově nahrazen obdobou terminálu, kde by se uživatel pouze přihlásil k webovému serveru a všechny potřebné aplikace a data by měl k dispozici online, uživatel se tak bude moci ke svým datům dostat z libovolného počítače s internetem. Ještě více tak vzroste datový provoz v rámci internetu, což s sebou bezpochyby přinese větší množství útoků a nové způsoby infiltrace, na které budou muset výrobci bezpečnostního softwaru promptně reagovat.

Organizované skupiny počítačových útočníků, pirátů či hackerů budou vždy o krok napřed oproti bezpečnostním aplikacím, kdyby tomu tak nebylo, tak by se již dávno počítačové kriminalitě nevěnovali. Nezbývá nám než doufat, že ten krok bude co nejmenší, a že nás tak alespoň zabezpečený a plně aktualizovaný počítač dokáže včas uchránit.

Seznam použitých zdrojů

Agnitum Ltd. . *The Essential Personal Firewall* [online]. 2011 [cit. 2011-11-07]. Outpost Firewall Pro. Dostupné z WWW: <http://www.agnitum.com/products/outpost/>.

AVAST Software a.s. *Antivirus a Anti-Spyware s firewallem* [online]. 2011 [cit. 2011-09-20]. Avast! Internet Security. Dostupné z WWW: <http://www.avast.com/cs-cz/internet-security>.

AVAST Software a.s. *Stáhněte si program pro ochranu před viry* [online]. 2011 [cit. 2011-09-13]. Avast! Free Antivirus. Dostupné z WWW: <http://www.avast.com/cs-cz/free-antivirus-download>.

AV-Comparatives e.V. Comparatives & Reviews [online]. 2008 [cit. 2011-06-28]. AV-Comparatives. Dostupné z WWW: <http://www.avcomparatives.org/en/comparativesreviews>.

AV-Comparatives.org. AV-Comparatives.org [online]. 2011 [cit. 2011-10-14]. Antivirus Comparatives 2011. Dostupné z WWW: <http://www.avcomparatives.org/images/stories/test/ondret/summary2011>.

AVG Technologies. *Antivir zdarma* [online]. 2011 [cit. 2011-09-13]. Antivir AVG. Dostupné z WWW: <http://www.avg.com/cz-cs/free-antivirus-download>.

AVG Technologies. *Internet Security 2012* [online]. 2011 [cit. 2011-10-11]. Antivir AVG. Dostupné z WWW: <http://www.avg.com/cz-cs/internet-security>.

AV-TEST - The Independent IT-Security Institute. AV-TEST [online]. 2011 [cit. 2011-10-14]. Test Reports > Quarter 2/2011. Dostupné z WWW: <http://www.av-test.org/en/tests/test-reports/quarter-22011/>.

Centrum holdings s.r.o. SW.cz [online]. 2011 [cit. 2011-10-14]. Outpost Firewall Pro 7 Single licence. Dostupné z WWW: <http://www.sw.centrum.cz/antiviry-bezpecnost/outpost-firewall-pro-7licence-na-rok/>.

Comodo Security Solutions, Inc. *Firewall Antivirus Software Free Download from Comodo* [online]. 2011 [cit. 2011-10-22]. Comodo Antivirus + Firewall. Dostupné z WWW: <http://personalfirewall.comodo.com/>.

Difinex, Ltd. Proactive Security Challenge [online]. 2011 [cit. 2011-10-28]. Matousec.com. Dostupné z WWW:<http://www.matousec.com/projects/proactive-security-challenge/results.php>.

HÁK, Igor. Moderní počítačové viry. Hradec Králové, 2005. 110 s. Bakalářská práce. Univerzita Hradec Králové.

Check Point Software Technologies Ltd. *Personal Firewall by ZoneAlarm* [online]. 2011 [cit. 2011-10-20]. Best Free Firewall Software for Download. Dostupné z WWW: <http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm>.

Check Point Software Technologies Ltd. *ZoneAlarm by Check Point* [online]. 2011 [cit. 2011-10-06]. Awards and Recognition – USA. Dostupné z WWW: <http://www.zonealarm.com/security/en-us/company/awards.htm>.

KOCMAN, Rostislav. Jak se bránit virům, spamu a spyware. Vyd. 1. Brno : CP Books, 2005. 148 s. ISBN 80-251-0793-0.

KRÄMER, Michel. Free Anti-Spam Filter [online]. 2011 [cit. 2011-12-01]. Spamihilator. Dostupné z WWW: <http://www.spamihilator.com/>.

Lavasoft. *Protect your Privacy with the World* [online]. 2011 [cit. 2011-09-13]. Ad-Aware. Dostupné z WWW: <http://www.lavasoft.com/products/ad_aware.php>.

Lavasoft. *Your ultimate Security Shield* [online]. 2011 [cit. 2011-11-01]. Lavasoft Personal Firewall . Dostupné z WWW: <http://www.lavasoft.com/products/lavasoft_personal_firewall.php>.

Microsoft Corp. *Microsoft Windows* [online]. 2011 [cit. 2011-11-06]. Principy nastavení brány Windows Firewall. Dostupné z WWW: <http://windows.microsoft.com/cs-CZ/windows-vista/Understanding-Windows-Firewall-settings>.

Microsoft. *Ochrana před viry, spywarem a škodlivým kódem* [online]. 2011 [cit. 2011-09-12]. Security Essentials . Dostupné z WWW: <http://www.microsoft.com/cs-cz/security_essentials/default.aspx>.

MICHAL, Jindřich. *Historie a vývojové trendy ve výpočetní technice* [online]. 2001 [cit. 2011-07-31]. Historie počítačových virů. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2001/xmichal1.html>.

POLESNÝ, David. *Živě.cz* [online]. 2011 [cit. 2011-10-04]. Test antivirů: Microsoft Security Essentials totálně propadl. Dostupné z WWW: <http://www.zive.cz/bleskovky/test-antiviru-microsoft-security-essentials-totalne-propadl/sc-4-a-156974/default.aspx>.

Safer Networking Ltd. *The home of Spybot-S&D* [online]. 2011 [cit. 2011-11-29]. Spybot - Search & Destroy. Dostupné z WWW: <http://www.safer-networking.org/cz/spybotsd/index.html>.

SZOR, Peter. Počítačové viry. Vyd. 1. Brno : Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.

Virus Bulletin Ltd. Virus Bulletin - Fighting malware and spam [online]. 2011 [cit. 2011-10-14]. VB100 Results Summary. Dostupné z WWW: <http://www.virusbtn.com/vb100/archive/summary>.

Wikipedia. Wikipedie - Otevřená encyklopedie [online]. 2011 [cit. 2011-12-10]. Dostupné z WWW: <http://cs.wikipedia.org/>.

Windows [online]. 2011 [cit. 2011-07-31]. Microsoft.com. Dostupné z WWW: <http://windows.microsoft.com/cs-CZ/windows-vista/Using-Windows-Security-Center>.

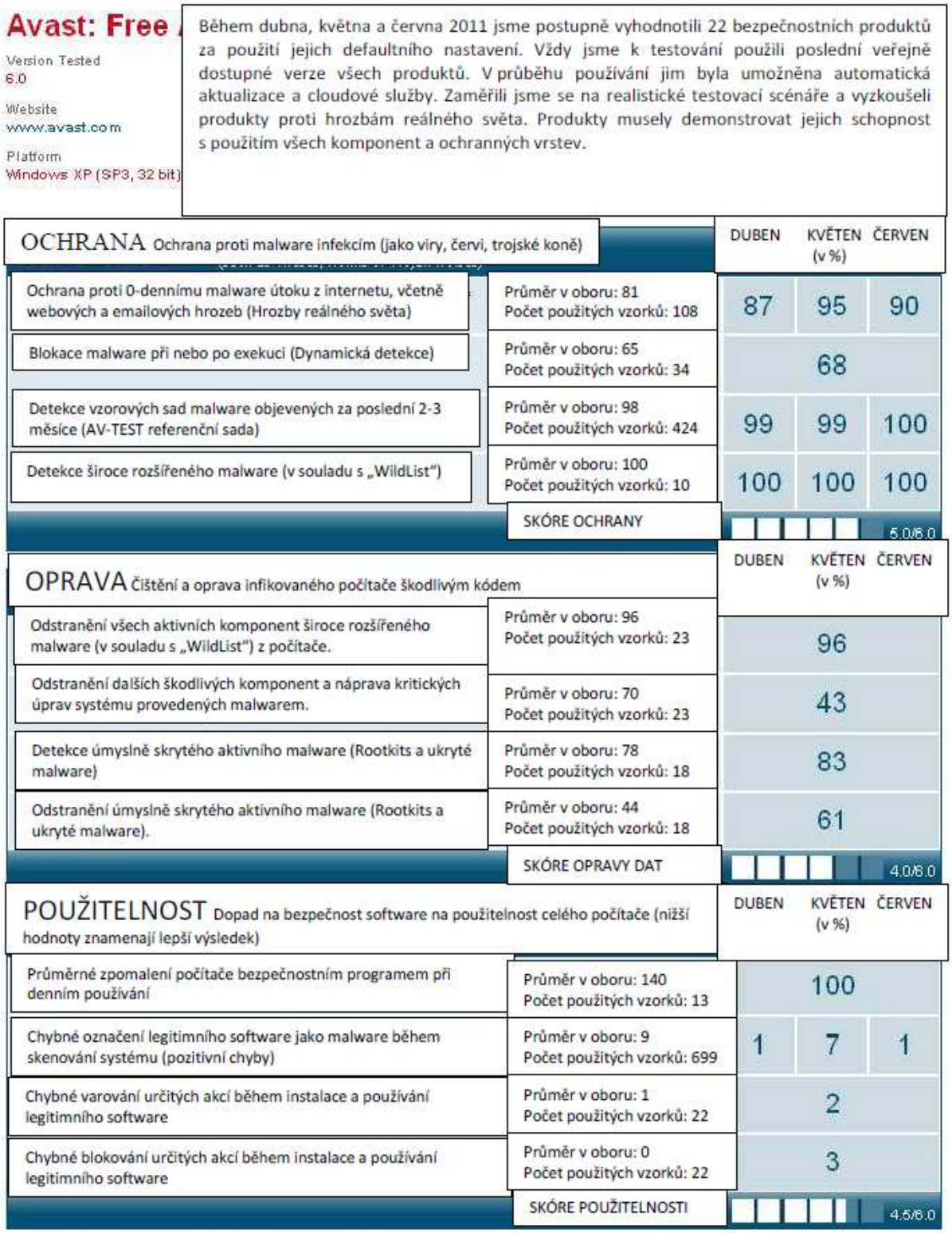
Windows [online]. 2011 [cit. 2011-07-31]. Microsoft.com. Dostupné z WWW: <http://windows.microsoft.com/cs-CZ/windows-vista/What-is-User-Account-Control>.

Seznam tabulek

Seznam obrázků

Seznam příloh

I. AV-test.org 8/2011: Detailní popis testu Avast! Free



Avast: Free

Version Tested
6.0

Website
www.avast.com

Platform
Windows XP (SP3, 32 bit)

Během dubna, května a června 2011 jsme postupně vyhodnotili 22 bezpečnostních produktů za použití jejich defaultního nastavení. Vždy jsme k testování použili poslední veřejně dostupné verze všech produktů. V průběhu používání jim byla umožněna automatická aktualizace a cloudové služby. Zaměřili jsme se na realistické testovací scénáře a vyzkoušeli produkty proti hrozbám reálného světa. Produkty musely demonstrovat jejich schopnost s použitím všech komponent a ochranných vrstev.

OCHRANA Ochrana proti malware infekcím (jako viry, červi, trojské koně)		DUBEN	KVĚTEN (v %)	ČERVEN
Ochrana proti 0-dennímu malware útoku z internetu, včetně webových a emailových hrozeb (Hrozby reálného světa)	Průměr v oboru: 81 Počet použitých vzorků: 108	87	95	90
Blokace malware při nebo po exekuci (Dynamická detekce)	Průměr v oboru: 65 Počet použitých vzorků: 34		68	
Detekce vzorových sad malware objevených za poslední 2-3 měsíce (AV-TEST referenční sada)	Průměr v oboru: 98 Počet použitých vzorků: 424	99	99	100
Detekce široce rozšířeného malware (v souladu s „WildList“)	Průměr v oboru: 100 Počet použitých vzorků: 10	100	100	100
	SKÓRE OCHRANY		5.0/6.0	

OPRAVA Čištění a oprava infikovaného počítače škodlivým kódem		DUBEN	KVĚTEN (v %)	ČERVEN
Odstranění všech aktivních komponent široce rozšířeného malware (v souladu s „WildList“) z počítače.	Průměr v oboru: 96 Počet použitých vzorků: 23		96	
Odstranění dalších škodlivých komponent a náprava kritických úprav systému provedených malwarem.	Průměr v oboru: 70 Počet použitých vzorků: 23		43	
Detekce úmyslně skrytého aktivního malware (Rootkits a ukryté malware)	Průměr v oboru: 78 Počet použitých vzorků: 18		83	
Odstranění úmyslně skrytého aktivního malware (Rootkits a ukryté malware).	Průměr v oboru: 44 Počet použitých vzorků: 18		61	
	SKÓRE OPRAVY DAT		4.0/6.0	

POUŽITELNOST Dopad na bezpečnost software na použitelnost celého počítače (nižší hodnoty znamenají lepší výsledek)		DUBEN	KVĚTEN (v %)	ČERVEN
Průměrné zpomalení počítače bezpečnostním programem při denním používání	Průměr v oboru: 140 Počet použitých vzorků: 13		100	
Chybné označení legitimního software jako malware během skenování systému (pozitivní chyby)	Průměr v oboru: 9 Počet použitých vzorků: 699	1	7	1
Chybné varování určitých akcí během instalace a používání legitimního software	Průměr v oboru: 1 Počet použitých vzorků: 22		2	
Chybné blokování určitých akcí během instalace a používání legitimního software	Průměr v oboru: 0 Počet použitých vzorků: 22		3	
	SKÓRE POUŽITELNOSTI		4.5/6.0	

Detailní popis testu AVS Avast Free

(Upraveno a přeloženo z: http://av-test.org/en/tests/test-reports/quarter-22011/)

II. Matousec.com Proactive Security Challenge: Detail testu

Proactive Security Challenge report

Testovaný produkt:	**Comodo Internet Security 5.3.176757.1236**
Výrobce:	**Comodo Security Solutions, Inc.**
Testovací platforma:	**Windows XP Service Pack 3, Internet Explorer 8**
Počet testů:	148

Dosažená úroveň:	10+
Celkové skóre:	**100 %**

Úvod

Tento report prezentuje výsledky testovaných produktů v seriálu známém jako „Proactive Security Challenge." Všechny informace vztahující se k testům, metodologii a hodnotícímu systému, jsou k dispozici na webových stránkách tohoto projektu. Reporty komerčního testování obyčejně obsahují výsledky všech možných úrovní, reporty veřejného testování obyčejně obsahují výsledky první úrovně a následujících úrovní až do nejvyšších úrovní dosažených testovaným produktem. Výsledky z veřejného testování jsou vždy k dispozici na stránkách projektu, zatímco výsledky komerčního testování jsou vždy publikovány až se souhlasem platícího zákazníka. Celkové skóre je vždy kalkulováno, jakoby byl report veřejný.

Pozn.: počet úrovní, testů nebo dokonce implementace testů se může změnit. Výsledky reportů jsou platné v době zveřejnění reportu a nejsou garantovány po dni zveřejnění.

Výsledky testů

Úroveň 1	
Počet testů:	**12**
O úroveň výš:	**50 %**
Skóre produktu:	**100 %**

Název testu	Výsledek	Komentář
Autorun1	100 %	PASSED
Autorun3	100 %	PASSED
Breakout2	100 %	PASSED
Coat	100 %	PASSED
ECHOtest	100 %	PASSED
FileDel2	100 %	PASSED
Kill1	100 %	PASSED
Kill2	100 %	PASSED

Ukázka z reportu testovaného produktu (Comodo IS)

(Upraveno a přeloženo z: http://www.matousec.com/projects/proactive-security-challenge/results.php)

Résumé

This work deals with the personal computer security software with Windows operating system. The paper briefly summarizes the history of the mostly known security risks for personal computer and there are also described the most serious security threats of today.

A separate chapter is devoted to general types of programs that allow these threats to prevent and detect them. The thesis also presents specifically selected safety programs and their comparison based on reputable independent tests.