Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Viry a Antiviry

Lukáš Bucvan

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Viry a antiviry" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2011 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Marku Píckovi za jeho pomoc a odborné rady při konzultacích při tvorbě této bakalářské práce.

Viry a antiviry

Viruses and antiviruses

Souhrn

Tato bakalářská práce se skládá ze dvou částí. První část je teoretická a obecně pojednává o počítačových virech a antivirech. U počítačových virů rozebírám jednotlivé druhy rozdělení a jejich charakteristiku. U antivirů poté charakterizuji jednotlivé detekce a odstranění viru. Kromě problematiky počítačových virů se v teoretické části věnuji i jinému škodlivému softwaru jako je například adware,spyware aj.

V praktické části se věnuji charakteristice čtyř druhů antivirů AVG, NOD 32, Asus a Kaspersky antivir. Poté jsem provedl jejich porovnání podle jednotlivých kritérií z hlediska domácího uživatele. V závěru bakalářské práce pro domácího uživatele doporučuji vítězný antivir, který v konečném hodnocení nasbíral nejvíce bodů.

Summary

This bachelor thesis consists of two parts. The first one is theoretical and deals with computer viruses and antiviruses in general. I analyze individual kinds of computer viruses and their definitions. For antiviruses, I then define individual detections of viruses and their resulting removal. Beside this, I also dissert on other harmful software, e. g. adware, spyware etc.

I've put thought into characteristic of four kinds of antivirus programs such as AVG, NOD 32, Asus and Kaspersky anitivir in the practical part. Than I made their comparison by individual criteria in terms of domestic user. At the end of bachelor thesis for domestic user I recommend winning antivirus, which in the final evaluation the most points scored.

Klíčová slova: viry, antiviry, červi, adware, spyware, NOD 32, AVG, Asus, Kaspersky antivir

Keywords: viruses, antiviruses, worms, adware, spyware, NOD 32, AVG, Asus, Kaspersky antivirus

Obsah :

Seznam tabulek

Seznam obrázků

1 Úvod

Po celém světě existuje celá řada různých bakterií a virů, které negativně ovlivňují život člověka. Může se jednat například o viry, způsobující více či méně závažná onemocnění, které napadají lidský organismus. V dnešním světě se může jednat například o velmi diskutabilní viry ptačí a prasečí chřipky, na které zemřelo po celém světě už desítky milionů obětí. Účinná léčba takových virů se provádí buď za pomocí vakcín, nebo za pomocí léků tzv.virostatik, které blokují daný virový enzym. Charakteristickou vlastností všech virů různého původu je existenci jejich hostitele. Bez hostitele by převážná většina virů zanikla, jelikož každý vir potřebuje pro svou existenci hostitelskou buňku, pomocí níž se bude v budoucnu dále reprodukovat.

Stejně jako v případě virů, které napadají lidský organismus, existuje celá řada tzv. počítačových virů, které útočí pomocí odvětví výpočetní techniky. Šíří se různými způsoby, ale mezi nejčastější způsoby se řadí šíření pomocí přílohy e-mailové pošty a pomocí stahování různých souborů z Internetu. Stejně jako se lidské tělo dokáže bránit pomocí již zmiňovaných léčebných praktik, tak i v odvětví výpočetní technologie jsou vytvořeny způsoby ochrany před napadením počítače virem.

Zatímco ve zdravotnictví se tyto způsoby ochrany nazývají vakcíny, v počítačové terminologii se mluví o tzv. antiviru neboli antivirovém programu. Mezi základní funkce těchto antivirů patří detekce daného viru a jeho následná eliminace.

2 Cíl práce a metodika

První teoretická část pojednává o obecné charakteristice virů a antivirů. V této části jsem se zaměřil na obecnou charakteristiku virů a antivirů. Rozebírám zde danou problematiku včetně historie a rozdělení jednotlivých typů škodlivého softwaru a antivirových metod, z které následně vycházím v praktické části.

Praktickou část jsem pojal z hlediska výběru antivirového programu pro konkrétní požadavky domácího uživatele. Na základě porovnání čtyř druhů antivirů, podle předem stanovených požadavků domácího uživatele, jsem pomocí vícekriteriální analýzy obodoval jednotlivá kritéria. V záverečné části bakalářské práce jsem domácímu uživateli doporučil antivir, který v mém systémů bodového hodnocení nejvíce vyhovoval zadaným požadavkům a získal nejvíce bodů.

3 Vývoj a historie počítačových virů

První program, který nesl prvky počítačového viru, se objevil v šedesátých letech. Jednalo se o počítačovou hru s názvem Core Wars, která při každém spuštění vytvořila svojí kopii a zabírala tak další paměťové místo. Autoři této hry se dají take považovat za jedny z prvních tvůrců antivirového programu, jelikož vytvořili současně program nazvaný Reeper, který měl za úkol vytvořené kopie hry Core Wars ničit. Obecně se o Core Wars nevědělo až do roku 1983, kdy byla tato hra popsána jedním programátorem ve vědeckém časopise. V roce 1975 se objevil počítačový virus Pervading animal, který se přidával na konec spustitelných souborů, aby následně poškozoval systémy Univac 1108. Další z významných škodlivých programů byl The Creeper, který se šířil pomocí modemu přes globální počítačovou síť. Jedinou obranou byl již zmiňovaný program Reeper.

První vir, který se šířil veřejně vznikl v roce 1981. Jednalo se o program pojmenovaný Elk Cloner, vyvinutý žákem deváté třídy Richem Skrentou v Pennsylvánii, který byl určen pro mikropočítače systému Apple-2. Program se distribuoval pomocí disket obsahujících samotný operační systém a zobrazoval žákovu báseň při každém padesátém zapnutí počítače. [2]

V roce 1983 byl pro účely semináře o bezpečnosti počítače vytvořen počítačový virus matematikem Dr. Fredem Cohenem, který byl testován třetinu dne počítačem VAX 11/750 na operačním systému Unix. Po tomto semináři byla představena práce s názvem Počítačové viry – teorie a experimenty, v které je tento virus popisován od jeho vývoje až po jeho působení na hostitele. Autorem této práce byl také Fred Cohen. Na semináři se také prvně oficiálně objevil pojem “počítačový vir”, který použil Fred Cohen na doporučení profesora Leonarda Adlemana, který je autorem tohoto pojmu. [1]

4 Dělení škodlivých programů

Malware[1] se rozděluje na několik jednotlivých typů. Mezi základní typy malware se řadí :

- počítačové viry
- trojské koně
- počítačoví červi
- adware
- spyware

Dále lze do této kategorie zařadit i phishing, hoax, dialer či rootkit, ale podrobně se budu v práci věnovat jen základním typům škodlivého programu.

4.1 Počítačové viry

Samostatný název pochází tedy od profesora Leonarda Adlemana. Co je to vlastně počítačový vir ? V dnešní době se bohužel chybně označuje jakákoliv škodlivá infiltrace[2] za počítačový vir. V postižených oblastech se ovšem nejčastěji škodlivý software prolíná a mnohdy nelze jednoznačně určit zda se jedná o trojského koně nebo například počítačového červa. První definice počítačového viru se vyskytla v práci Freda Cohena a měla tento tvar : " Virus je program, který je schopen infekce dalších programů a je schopen jejich modifikaci zajistit, aby obsahovaly potenciálně vyvíjející kopii jeho samotného."

4.1.1 Rozdělení podle umístění v paměti:

- rezidentní
- nerezidentní

4.1.1.1 Rezidentní viry

Rezidentní viry se vyskytují v systémové paměti a zároveň běží na pozadí operačního systému. Jejich samotná aktivace probíhá ve dvou rovinách. Buď při prvním zavedení napadeného souboru, kdy se jedná o souborový virus, a nebo při prvním

[1] Malware – výraz vznikl složením ze dvou anglických slov malicious a software a jedná se o souhrnné označení škodlivého programu
[2] Infiltrace - programy vnikající do počítače, bez vědomí vlastníka

zavedení operačního systému z infikovaného boot sektoru , kdy se jedná o boot virus. Hlavní charakteristikou těchto virů je, že jsou aktivní až do chvíle, kdy nastane vypnutí celého systému. [3]

4.1.1.2 Nerezidentní viry

Tyto viry jsou pravým opakem virů rezidentních a velmi často se označují jako tzv. viry přímé akce. Jsou charakteristické tím, že se aktivně neinstalují do paměti počítače, ale jejich načítání probíhá při zavedení hostitele, kde po předání obsluhy hledají příslušné objekty k napadnutí. Po spuštění infikují převážně jen hrstku souborů, ale existují i výjimky, které dokáží napadnout všechny dostupné soubory. Úspěšnost těchto virů je závislá především na pozici hostitele. Z tohoto důvodu jsou efektivnější v oblasti síťového prostředí. Vzhledem k jejich snadnému stvoření na mnoha platformách je největší skupina počítačových virů původem právě virů přímé akce.

4.1.2 Rozdělení podle napadených oblastí:

- boot viry
- souborové viry
  - přepisující viry
  - připojující viry
  - parazitické viry
  - dutinové viry
  - komprimující
- multipartitní viry
- makroviry

4.1.2.1 Boot viry

Mezi první oblasti v počítači, která byly v minulosti napadány počítačovými viry patřily tzv. boot sektory disků. Dnes se však tento typ infekce už neužívá. Hlavní charakteristikou boot virů je, že dokáží napadnout počítač, aniž by brali ohled na operační systém, který je na něm nainstalovaný. Využívají se při spouštění osobního počítače. Převážná většina počítačů nemá operační systém uložen v paměti ROM[3], ale načítá tento

[3] ROM – jedná se o zkratku anglického označení Read-Only Memory a jedná se o pamět určenou pouze pro čtení

systém z pevného disku. V minulosti ovšem nebyl určen postup zavedení operačního systému popsán, a tak se počítač snažil vždy zavádět systém z disketové mechaniky, což vedlo k tomu, že mohlo dojít k infikaci počítačovými viry ještě před spuštěním operačního systému. Docházelo k tomu například u prvních počítačů firmy IBM, kde nebyl tento proces zaznamenán a počítač se tak snažil zavádět systém přímo z diskety. Na základě těchto poznatků se doporučuje nastavit zaváděcí proces tak, aby první zavedení pocházelo z pevného disku, čímž se zamezí existenci boot virů. [1]

4.1.2.2 Souborové viry

Charakteristické jsou tím, že se přidávají ke spustitelným souborům nebo mění jejich určitou část, která se nazývá programový kód. Aktivují se spuštěním napadeného souboru. Tyto soubory mají nejčastěji tyto koncovky: exe, bat, sys, com a dll. V závislosti na těchto koncovkách se souborové viry rozdělují na jednotlivé podkategorie. [3]

4.1.2.2.1 Přepisující viry

Přepisující viry jsou viry, které přepisují nebo úplně nahrazují původní soubor. Mezi jejich hlavní charakteristiku patří, že napadené soubory nelze vyléčit některou ze známých technik, ale takto napadené soubory musí být kompletně smazány z disku. Později však lze tyto soubory obnovit ze zálohy počítače. Tyto viry vynikají technikou velké šiřitelnosti hlavně v případech, kdy dochází k jejich šiřitelnosti pomocí počítačové sítě. Takovým příkladem je například vir VBS/LoveLetter.A@mm , který pomocí elektronické pošty rozesílá své kopie na jiné systémy. Dalším případem přepisujících virů je způsob, kdy vir nemění velikost hostitele, ale v souboru si náhodným způsobem najde určitou oblast, na kterou se zapíše. Vir není za každou cenu aktivován spolu se spuštěním svého hostitele, ale tento hostitel je již nenávratně poničen a může vykazovat známky havárie i před samotným spuštěním. Největší problém tvoří přepisující viry pro scenery, jelikož musejí prozkoumat celý obsah hostitele, a to je náročné jak z výkonového hlediska, tak z hlediska časového.

4.1.2.2.2 Připojující viry

Samotný název je odvozen od umístění virového kódu, který se připojuje na konec hostitele. Klasickým případem připojujících virů je infekce DOSových COM souborů, při které se vkládá skoková instrukce JMP na počátek hostitele. Skoková instrukce JMP se někdy nahrazuje instrukcemi, které vykazují podobné vlastnosti jako JMP. Například se jedná o instrukce CALL nebo PUSH. Zajímavostí je existence určitých virů, který před samotnou infikací převádějí EXE soubory na COM soubory. Příkladem jsou například viry Vascina. Funkce viru spočívá v tom, že v době otevření postiženého programu vir načte hostitele do paměti, aby následně skoková instrukce přesměrovala vykonávání do těla viru, kde dochází k vyhledání dalších souborů, které jsou vhodné k infikování. Tento způsob připojování je použitelný pro jakýkoliv spustitelný soubor, který má například přípony EXE, NE, ELF aj. Každý takový soubor má v sobě hlavičku obsahující adresu počátečního bodu, který je následně nahrazen vstupním bodem , který obsahuje počátek virového kódu napojeného na konec hostitele.

Kromě vkládání virového kódu na konec hostitele existují i viry, které se připojují na počátek hostitele. Tyto viry bývají často označovány jako
tzv. prependery. I přes svoji jednoduchost se jedná o velmi účinné viry, které byly použity na různých operačních systémech. Prependery jsou psány pomocí programovacích jazyků C++, Pascal nebo Delphi. Vzhledem ke struktuře spustitelného souboru jsou tyto virové kódy složitější v porovnání s případy COM souborů.

4.1.2.2.3 Parazitické viry

Příkladem parazitického viru byl například vir Virdem od autora Ralfa Burgera, který se považoval za jeden z prvních souborových virů. V zásadě se jedná o variantu infekce typu připojení na začátek souboru. Tyto viry nahradí počátek hostitele svým kódem a uloží ho na konec hostitelského souboru. Při léčení takto zavirovaných souborů dochází k mnoha problémům, které vychází především z vícenásobné infekce, tedy ze situace, kdy je soubor infikován opakovaně.

4.1.2.2.4 Dutinové viry

Tato skupina virů je charakteristické tím, že nijak nemění velikost svého hostitele, ale místo toho si najde v souboru určitou oblast, do jaké se přepíše. Detekování dutinových virů vychází z obsahu zaváděné rutiny, která je uložena v určité části kódu. Mezi nejčastěji napadané oblasti patří skupiny binárních souborů obsahující nuly. Dutinové viry jsou především pomalu šiřitelné DOS infektory, mezi které patří například vir bulharského původu Darth Vader, který vzhledem ke svému pomalému rozvoji nezpůsoboval velké škody. Program infikoval až v době, kdy se tento program sám zapsal. Největší problém dutinových virů je ten, že obsah přepsaných programů nejde dokonale obnovit do stoprocetního stavu před přepsáním. To je způsobeno tím, že po léčení souboru neodpovídají jeho kryptografické kontrolní součty.

4.1.2.2.5 Komprimující viry

Jedná se o specifickou techniku virů využívající komprimaci obsahu hostitelských souborů. Mezi jejich hlavní rozpoznávací znaky patří zkomprimování svého hostitele vice, než jeho zvetšení, čímž znatelně ušetřuje volné místo na pevném disku. Komprimační techniky patří mezi velice oblíbené, a proto také lákají virové útočníky, které je využívají pro zkomprimování počítačových červů, virů apod. na co nejmenší celky, aby byly co nejméně rozpoznatelné. První vir využívající tuto techniku se nazýval Cruncher a patřil do kategorie DOSových virů.

4.1.2.3 Multipartitní viry

Tyto viry vznikly jako spojení boot virů a souborových virů. První příklad multipartitního viru objevil v roce 1989 Fridrik Skulason a pojmenoval ho Ghostball. Jednalo se o první vir, který byl schopen napadnout jak COM soubory, tak i zároveň boot sektory. Další následoval virus Tequila, který uměl napadnout kromě EXE souborů systému DOS i sektory pevných disků. Jeden z hlavních a zároveň i prvních virů, který mohl napadnout současně COM i EXE soubory systému DOS byl vir označený jako Virus Memorial. Mezi základní vlastnost multipartitních virů patří jejich obtížné odstraňování. V minulé době se multipartitní viry využívaly především k infikacím u systému DOS. U systémů Windows se snimi lze také setkat, ale v podstatně menší míře než je tomu u uvedených systémů DOS. [1]

4.1.2.4 Makroviry

Jedná se o viry, které jsou tvořeny makry. Tyto makra jsou vytvářena pomocí vyšších programovacích jazyků, které jsou schopny pohybovat s daty aplikace a zároveň i s danými makry, které jsou s těmito daty propojeny. Makro s možností překopírovat sebe samo z jednoho souboru do druhého, a to i vícenásobně se nazývá makrovirem. Mezi hlavní podmínky úspěšného šíření makroviru patří časté užívání dané aplikace a musí docházet k přenosům dat, a tedy současně i maker, mezi jednotlivými uživateli. Tyto podmínky nejvíce naplňují produkty od firmy Microsoft s označením Microsoft Word a Microsoft Excel, které jsou součástí balíčku Microsoft Office. Princip je založen na neukládání makra do specifického souboru, ale do totožného souboru ve kterém se nacházejí i uložená vlastní data. Speciální vlastností makrovirů je jejich funkčnost na různých typech počítačů a zároveň i na odlišných operačních systémech. [5]

4.1.3 Rozdělení podle chování

- stealth viry
- polymorfní viry
- retroviry
- tunelující viry
- armored virus

Poslední tři typy rozdělení virů retroviry, tunelující viry a armored virus patří do kategorie tzv.obranné strategie virů. Slouží k popisu různých technik obrany, které mají za cíl co nejdelší setrvání virů na systémech i v případě, že jsou systémy chráněny antivirovým programem pro monitorování virů.

4.1.3.1 Stealth viry

Jedná se o viry, které se před uživatelem ukrývají jako například metodou zamaskováním velikosti souborů aj. Jejich oblast působnosti se nachází v operační paměti.

4.1.3.2 Polymorfní viry

Dokáží pomocí zašifrování pozměnit strukturu svého těla. Jejich odhalení bývá velmi obtížné, jelikož umožňují pozměnit svůj kód ve spojitosti s určitou situací. Vzhledem k jejich odhalení musí moderní antiviry obsahovat mechanismy na detekci šifrování. První vir, který se mohl řadit do této skupiny byl Virus 1260 zhotovený Markem Wasburnem. Tento vir užíval dva klíče, aby dosáhl zdekódování vlastního těla a výhodu měl v tom, že se mohl v závislosti na vložených instrukcí zmenšovat či zvětšovat. [6]

4.1.3.3 Retroviry

Retroviry patří do kategorie počítačových virů, které se snaží obelstít nebo vyřadit funkčnost antiviru, firewallu[4] nebo ostatní bezpečnostní složky počítače. Mnoho počítačových virů odstraňuje procesy v počítači z paměti a pevného disku, které přísluší antivirovým programům, jelikož většina uživatelů systému Windows mají na svém počítači nastavená práva administrátora. Retroviry umožňují pozměňovat cestu pro již zámé viry, které by v normálním případě byly zachyceny antivirovým programem. Tvůrci těchto virů ve velkém množství případů užívají techniku reverze v inženýrství pro vyhledání postupů, které by sloužily k deaktivaci antivirového programu.

Činnost retrovirů se dá charakterizovat těmito body :

- deaktivují nebo vypnou antivir z počítačové paměti nebo pevného disku
- deaktivují firewall
- zničí programy a soubory, které slouží pro zjištění integrity dat
- pomocí antivirového programu provedou virový kód
- napadnou antivirovou databázi pomocí vnoření trojského koně
- při spuštění antiviru poničí určitá data
- zabraňují napadeným systémům ve stáhnutí aktualizací pro antivirové databáze

[4] Firewall – jedná se o zařízení sloužící k ovládání a zabezpečení počítačových sítí

- některé retroviry mají i vlastnost, ve které neútočí jen na antivirové programy, ale i na nástroje pro jejich analýzu

Aby se moderní antivirové programy více chránily před jednotlivými počítačovými viry, musí obsahovat speciální ochranu před útoky typu rušení procesů.

4.1.3.4 Tunelující viry

Tunelující viry se řadí do kategorie paměťově rezidentních virů. Tato kategorie často užívá právě tunelovací techniky, aby se vyhnuly systémům, které sledují zvláštní chování. Jejich funkce spočívá ve vyhledání prvotního článku zavolání přerušení, čímž se vyhnou ostatním aplikacím. Tímto druhem volání přerušení dokáží obejít i antivirový software.

4.1.3.5 Armored virus

Samostnatný název armored virus přineslo oddělení New Scotland Yard, které mělo na starost kriminalitu kolem počítačové terminologie. Tato skupina virů obsahuje špatně analyzovatelné a detekovatelné viry. Jednotlivé části se rozdělují do několika metod.

Metoda obrany proti disassemblování pojednává o počítačových virech sepsaných v programovacím jazyku assembler. Nejčastější útoky, které se týkají disassemblerů, se zaměřují na matoucí techniky kódu jako jsou například polymorfismus nebo metamorfismus.

Metoda obrany proti ladění se týká útočníků, který znesnadňují proces ladění. Mnoho technik je závislých na jednotlivých platformách, jelikož proces ladění je úzce spojen s počítačovým hardwarem.

Metoda obrany proti heuristické analýze patří mezi kategorie, které hledají známé i neznámé viry pomocí dynamických a statických metod. Dynamická metoda využívá emulování kódu k simulaci procesů. Statická metoda využívá analýzu určité části kódu a souborového formátu. Jako první generace se tato metoda objevila u detektorů pro systém Win32, která využívala statickou metodu. Tato metoda dokázala rozpoznat podezřelé části PE souborů s velmi vysokou úspěšností detekce. Vysokou úspěšností byly zaskočeni i samotní tvůrci virů, avšak postupem času dokázali vytvořit různé metody útoku, které heuristickou analýzu prolomily. Dokonce se našli i tvůrci, kteří vytvořili techniky proti nejsložitější části antivirového softwaru – emulátoru počítačového kódu.

Metoda obrany proti emulaci vznikla na popud tvůrců virů, kteří se dověděli, že určité druhy scenerů využívají pro detekci 32 bitových Windows virů emulaci. Zaměřili se proto s vytvářením útoků na počítačovou součástku scenerů tzv. emulátor[5].

4.2 Trojské koně

Trojský kůň je druh škodlivého programu, který se na první pohled jeví uživateli jako užitečný a vybízí uživatele k jeho spuštění. Pomocí trojského koně poté ovládá útočník infikovaný počítač.

Jeden z nejznámějších představitelů trojského koně je AIDS TROJAN DISK, který byl pomocí diskety rozeslán přibližně na 7000 adres různým výzkumným institucím po celém světě. Ten po nahrání do systému rozházel všechny názvy souborů a obsadil všechny volné pozice na pevném disku. Zpětné vrácení dat do původního stavu bylo nabízeno za finanční kompenzaci. Autorem viru byl Dr. Joseph Popp, který pracoval jako zoolog ve městě Cleveland.

4.3 Počítačoví červi

Samotný název charakterizuje viry šířící se pomocí počítačové sítě. Jedná se o samostatné programy, které narozdíl od počítačových virů nevyžadují svého hostitele. Spuštěny bývají ve většině případu bez asistence uživatele. Výjimku však tvoří červi, kteří se šíří pomocí e-mailové pošty, ty zásah uživatele vyžadují. [1]

4.3.1 Historie

První zmínky o počítačových červech sahají do roku 1998, kdy se obejvil Morrisův počítačový červ, který vytvořil zprávy jenž měli za následek několika denní zpomalení celého internetu. V dnešní době se už útoky na systémy Unix nevyskytují tak často jako dřív, jelikož záměr vetšiny autorů počítačových červů je soustředěn hlavně na systémy Windows. Příčin tohoto zaměření by se dalo najít mnoho, ale mezi hlavní patří především velká oblíbenost systému Windows mezi koncovými uživateli. Od Morrisova červa se dnešní červi liší tím, že nestahují a nepřekládají zdrojové kódy, ale zaměřují se pouze na určité architektury.

[5] Emulátor – jedná se o určíty druh softwaru, který umožňuje chod počítačových programů na jiném operačním systému, než pro který byl původně navržen

Hlavní vlna moderních červů přišla až s objevením paměťově rezidentního červa Code Red v roce 2001, který využil náchylnosti webového serveru od Microsoftu s označením IIS k napadnutí webových stránek. Tohoto viru se objevilo několik variant, kde novější varianta vycházela z předchozí a byla doplněna o další prvky. Některé z těchto variant se vyskytují ve světě internetu dodnes.

Po těchto červech přišli další jako například Nimda, jehož charakteristická vlastnost byla, že zabraňoval antivirové produkty na napadnutých systémech. Vzhledem k tomu, že tato vlastnost zabraňovala detekci červa, je hojně využívána dnešními tvůrci červů. Dalším byl v roce 2003 červ Slammer, jenž byl uložen v jednom paketu a jeho hlavní předností byla rychlá šiřitelnost. Vzhledem k tomu, aby se zamezilo dalšímu útoku, se musela vytvořit záplata, která odstraňovala tuto bezpečnostní díru. Mezi další známější červi by se dali zařadit i Blaster a Welchia, které stáli u zrození nakažlivých variant počítačových červů. V budoucnu se dají očekávat mnohem dokonalejší a nakažlivější červi, hlavním úkolem zůstává práce na vyvoji nástrojů pro jejich detekci, aby způsobily co nejméně škod nejen na podnikové úrovni. [4]

4.3.2 Chobotnice

Chobotnice se řadí do rodu počítačových červů. Samotný nápad chobotnice pochází z novely Shockwave Rider od autora Johna Brunnera. Jedná se o červa, který je vytvořen větším množstvím programů, které jsou rozděleny na více počítačích v síti. Funkci lze popsat tak, že se jednotlivé části programu nainstalují na odlišné počítače a následně provádějí určitou funkci pomocí vzájemné komunikace. V současné době nemá velkou působnost, avšak s jejím uplatněním se počítá hlavně do budoucna.

4.3.3 Králík

Jedná se o specifický typ počítačového červa. Tento typ se v každém okamžiku vyskytuje právě v jedné kopii, která putuje po počítačích zapojených ve společné síti. Samotný termín je využíván odborníky pro škodlivý software, který se spouští do doby, než zabere celou paměť. Velké problémy vyvolává hlavně u aplikací, které musejí pracovat s malým paměťovým rozpětím. [1]

4.4 Adware

Jde o produkty znepříjemňující práci s počítačovou reklamou. Mezi hlavní příklady patří tzv. pop-up[6] okna nebo banner[7]. Většina adware je doprovázena pomocí licence, kdy musí uživatel potvrdit instalaci tohoto adwaru. Nevýhodou je, že nás tato nepopulární reklama provází během celé práce s daným programem.Výhodou ovšem zůstává, že zároveň nabízí větší množství různých funkcí, které se ve verzi bez reklamy nevyskytují.[5]

4.5 Spyware

Spyware je druh programu využívající internet k rozesílání dat z počítače bez souhlasu jeho uživatele. Do počítače se může dostat i legální cestou, jelikož s jejich aktivací může uživatel souhlasit v rámci licenční dohody. Tvůrci spyware se ospravedlňují tím, že se pouze pokouší zjistit potřeby a zájmy uživatele, aby je následně mohli využít pro efektivní reklamu. Důležitým znakem je šiřitelnost spywaru s plno sharewarovými programy jejichž tvůrci jsou s touto skutečností narozdíl od uživatelů srozumněni. Důsledky spyware spočívají v radikálním nárustu spotřeby výkonu počítače, což se projevuje jeho značným zpomalením. Dále může zjišťovat navštívené internetové stránky, hesla apod. Mezi další negativní vlastností spyware patří přesměrování na internetové stránky, které mají většinou pornografické zaměření. Velmi kritická závada nastává v situaci, kdy spyware pozmění nastavení vlastností registrů počítače nebo přenastaví systémové složky. Největší ochranou před spyware je neinstalovat podezřelé programy, nenavštěvovat podezřelé internetové stránky a používat antispyware. [6]

5 Antivirová ochrana

V obecném měřítku se antivirový software používá jako ochrana uživatelů před útoky počítačových virů. Hlavní funkce spočívá v technice antivirových scenerů.
V dnešní době se rozlišují dva typy scenerů. První scener se nazývá on-demand, jehož skenování probíhá na uživatelský příkaz a může se spouštět při startování operačního systému. Druhý scener se nazývá on-access a jeho poznávací charakteristikou je, že je stále rezidentní v paměti a jeho nahrání se provádí pomocí jednoduchých aplikací.

[6] Pop-up – neboli vyskakující okna, která spouštějí různé webové stránky k vyobrazení reklamy
[7] Banner – jedná se o typ reklamy využívaný na internetu, často má tvar obrázku či animace

Tyto aplikace jsou vytvořeny jako ovladače zařízení, které se napojují na souborové systémy. [1]

5.1 Hlavní činnosti antivirové ochrany

Mezi hlavní činnosti antivirových programů patří :

- vyhledávání
- skenování
- heuristická analýza
- kontrola integrity

Vyhledávání je charakterizováno tím, že antivirus obsahuje jednotlivé znaky virů a při nalezení nějakého programu, který se shoduje s danými charakteristikami, označí jako vir. Metoda je úspešná především u velmi známých virů, u kterých jsou známy jejich podrobné vlastnosti. U modifikovaných virů není tak úspěšná nebo má dlouhé trvání. Neznámé viry s novými charakteristikami ovšem odhalit nedokáže.

Skenování se vyznačuje výrazně rychlejším vyhledáváním virů, jelikož při vyhledávání virů se nepoužívají tak podrobné charakteristiky jako u vyhledávání, ale pouze ty základní. Velkou nevýhodou ovšem u této metody zůstává fakt, že nedokáže rozpoznat co se za vir označit dá a co už ne. V případě, že program obsahuje řetězec, který je totožný s řetězcem v databázi antivirového programu, je tento soubor brán jako infikovaný. I přes nutnosti častých aktualizací a drobná negativa je tato metoda vysoce spolehlivá.

Heuristická analýza pojednává o rozebrání virového kódu, kde antivirus prozkoumává jiný program od jeho počátku a v případě nalezení podezřelé instrukce tento program označí jako zavirovaný. Výhodou této metody je možnost objevení neznámých virů, které ostatní metody nevyhledají. Značnou nevýhodou ovšem zůstává velké množství poplašných zpráv.

Kontrola integrity porovnává stavy před případnou nákazou a stavem po nákaze. Princip fungování spočívá v tom, že antivirus čeká na dobu, kdy se virus projeví určitou vlastností. Například se může jednat o nárust u velikosti souboru. Nevýhodou této metody je skutečnost, že vir dokáže pouze najít, ale nedokáže ho zničit. [6]

5.2 Skenery první generace

K objevení počítačového viru je možné dojít několika způsoby. V této kapitole se zaměřím na podrobnější rozebrání příkladů metod identifikace a detekce.

5.2.1 Skenování řetězců

Tento způsob patří k nejzákladnějším u metody detekování. Funkce spočívá v tom, že se užije řetězec bajtů charakteristický pro konkrétní počítačový vir. Tyto řetězce jsou uloženy v databázích, které jsou využívány skenery při procházení oblastí souborů. Jsou uspořádány tak, aby v čase, který je vyhrazený pro skenování, dokázali detekovat počítačové viry. Řetězce musejí mít délku alespoň 16 bajtů, aby byly schopny bezpečně detekovat vir a nedocházelo k rizikům falešných poplachů. Výjimku tvoří například 32 bitové počítačové viry, u kterých je k úspěšné detekci vyžadována větší velikost řetězce než již zmiňovaných 16 bajtů. Ke komplikacím dochází v případě chybné detekce viru, kdy se antivirový skener snaží infikovaný objekt vyléčit. Může tak docházet k řadě problémům, jelikož jsou postupy léčení, například u dvou podobných virů, zcela odlišné.

5.2.2 Zástupné znaky

Jedná se o znaky, které mají možnost přeskočit určité rozsahy bajtů. Znaky jsou využívány pro půlbajty, které umožňují lepší srovnání skupin instrukcí. Při srovnávání dvou řetězců od počátku je k nalezení neshody potřeba sedmi srovnání. Naopak při srovnání dvou řetězců od konce se rozdíl projeví už při prvním pozorování. Tato technika byla převážně úspěšná u prvotních virů jako například polymorfních virů.

5.2.3 Neshody

Tato metoda byla vynalezena pro IBM Antivirus. Umožňují libovolnost N bajtů, které jsou obsaženy v řetězci bez ohledu na rozmístění uvnitř řetězce. Přínosné jsou především při utváření generických řešení při detekování počítačových virů. Velkou nevýhodou algoritmu ovšem zůstává nízká rychlost při skenování.

5.3 Skenery druhé generace

Využívají přesnější identifikaci, která zlapšuje detekování složítějších počítačových virů a ostatního škodlivého softwaru.

5.3.1 Chytré skenování

Bylo objeveno v době výskytu prvních počítačových virů založených na speciálním enginu. Tyto enginy pracovaly se zdrojovým kódem programovacího jazyka assembleru tak, že do něho zasouvaly bezpředmětné intrukce NOP. Překompilovaný vir ovšem vykazoval odlišné vlastnosti, než měl jeho originál, jelikož došlo ke změnám velkého množství offsetů[8]. Chytré skenování umožňuje tyto instrukce NOP v programu přeskakovat a zároveň i neukládat. Tato technika je také velice úspěšná pro viry vyskytující se v textové formě jako jsou například makroviry.

5.3.2 Detekce struktury

Tato technika je zaměřena především na detekci makrovirů a vynalezl ji pan Eugen Kaspersky. Skener vybere místo prostého řetězce makra řádek po řádku a vynechá všechny zbytečné příkazy včetně prázdných znaků.
Na konci zůstane pouze hlavní struktura makra, která je tvořena pouze nepostradatelným škodlivým kódem, který se vyskytuje v makrovirech. Tyto informace jsou poté využity k efektivnější detekci počítačových virů.

5.3.3 Přesná identifikace

Jedná se o jediný způsob, jak bezpečně zajistit správnou identifikaci viru. Často je slučována s technikami skenerů první generace. Funkce spočívá v tom, že využívá největší možný počet rozsahů, který je potřebný k výpočtu kontrolního součtu všech bitů. Je zapotřebí odstranit všechny proměnlivé bajty, aby se dosáhlo velké přesnosti a mohla být vytvořena mapa pro všechny konstatní bajty. Tato metoda se vyznačuje velkým množstvím výhod. Nevýhodou ovšem zůstává fakt, že skenery využívající přesnou identifikaci, jsou při skenování infikovaného souboru mnohem pomalejší než jednoduché základní skenery. To je způsobeno zejména dlouhotrvajícím mapováním všech konstatních rozsahů.

[8] Offset – adresa ukazující na místo v paměti u pc x86 se skládá ze segmentu a offsetu, offset je tedy část adresy

5.4 Algoritmické metody skenování

Algoritmické skenování se využívá při implementaci nového specifického algoritmu pro detekci v momentě, kdy si klasické algoritmy skeneru nedokážou poradit s určitým virem. Jde o nepostradatelnou vlastnost každého moderního antivirového softwaru. Jednotlivé viry mají detekované rutiny sepsané v programovacím jazyce C, Assembleru nebo Java. Tyto rutiny jsou následně překompilovány do databáze uložené ve skeneru.

5.4.1 Filtrování

Tento způsob se stále využívá u skenerů druhé generace. Funkce je založena myšlence, že počítačové viry ve většině případech napadají pouze určitou sadu typů objektů. V praxi to pro skenery znamená velkou výhodu, jelikož se jednotlivé části mohou zaměřit pouze na určité skupiny.

Například části, které mají na starost boot viry se mohou zaměřit pouze na boot sektory stejně jako části EXE útoků se mohou zaměřit pouze na EXE soubory. Skenovací algoritmy jsou z velké části závislé na filtrech, které mohou být například spustitelné soubory, část kódu s podezřelými příznaky nebo identifikační značka viru. Nevýhodou ovšem zůstává, že existuje několik počítačových virů pro které se technika filtrování nedá využít.

Pro správné filtrování existuje celá řada kontrol :

- v místě předpokládaného výskytu viru přepočítat počet nulových bajtů v souboru
- překontrolovat počet změn příznaků a velikostí sekce
- některé druhy virů nanapadají například konzolové aplikace nebo DLL knihovny, a proto je potřeba zkontrolovat jednotlivé příznaky souboru

5.4.2 Statická detekce decryptoru

Skenovací rychlost je závislá na velikosti skenovaných sekcí. Samostatný význam má tato techniky téměř nulový, jelikož dokáže opomíjet infikované soubory a hlásí ve velké množství poplašných zpráv. Vzhledem k nedekódování virového kódu neumožňuje

ani léčení. Statická detekce decryptoru je ovšem velmi rychlá pokud se použije společně s nějakým filtrem. Využití tato detekce nachází například u polymorfních virů.

5.4.3 Rentgenová metoda

Jako rentgenové skenování se myslí zaútočení na zakódování kódu. Autorem byl Frans Valdmen, který rentgenové skenování vytvořil pro svůj projekt TBSCAN. Princip rentgenování spočívá ve využití všech základních metod kódování a realizuje se na předem zvolených místech v souboru. I přes nižší rychlost skenování má tato technika výhodu ve své všeobecné použitelnosti. Mezi další výhody patří například celkové zdekódování virového kódu. Nevýhoda se projeví ve chvíli, kdy není k nalezení počátek těla viru a útok proti decryptoru musí být proveden na velké oblasti programu.

5.5 Emulace kódu

Jedná se o vysoce efektivní metodu detekce počítačových virů. Činnost emulace kódu je založena na virtuálním stroji skeneru, který implementuje simulaci počítače a předstírá vykonávání škodlivého kódu. Ve skutečnosti se ovšem virový kód na procesoru ani nespustí. Základním stavebním kamenem je tedy simulace skupiny instrukcí procesoru s využitím virtuálních komponent. Softwarová emulace byla prvně použita v antivirovém programu F-PROT, jehož autorem byl pan Skulason. Novější verze vycházející z F-PROTU už obsahovaly integrované emulátory pro náročnější polymorfní viry. Detekování polymorfních virů se provádí prohledáváním obsahu paměti pomocí virtuálního stroje. Vzhledem k vlastnosti polymorfních virů dekódovat samy sebe je důležité odhadnout čas, kdy se má zastavit emulace virového kódu. Řešení nabízí tyto tři klasiké metody :

- **sledování aktivních intrukcí** - jedná se o intrukce, které mění bitovou hodnotu v paměti virtuálního stroje
- **sledování decryptoru s užitím profilů** - využití speciálního profilu pro všechny polymorfní decryptory
- **zastavení s pomocí breakpointů** – pomocí tzv. breakpointů dokáží intrukce zastavit emulaci v případě, že nastane spuštění dekódovaného těla počítačového viru

Tento způsob detekce je podstatně rychlejší než rentgenové skenování. Rychlost je závislá na počtu opakování dekódovací smyčky. Samotné dekódování počítačového viru ve virtuálním stroji může být dlouhé i několik minut.

6 Obrana na síťové úrovni

Předchozí stránky byly zaměřené na detekování a principu obrany s přihlédnutím k hostitelovi. V této kapitole se zaměřím na jednotlivé techniky obrany a chování počítačových červů v počítačové síti. Mezi hlavní techniky obrany patří firewally, systémy pro detekci průniků do sítě, honeypoty, metody protiútoků a systémy včasného varování. Podrobněji se budu v této kapitole věnovat technikám jako jsou firewally, honeypoty a metody protiútoku.

6.1 Firewally

Základní funkcí firewallů je ochrana před infekcí počítačovými červy. Jako hlavní prvek k ochraně před červy slouží blokování portů. Ve vetšině případů se k zamezení útoku využívá zablokování síťových portů. Existují ovšem výjimky jako například červ s názvem Witty, který vyžaduje i zablokování zdrojových portů. K dostatečné ochraně osobního počítače ovšem samostatný firewall nestačí, jelikož počítačový červ s využitím retro-útoku umožňuje zlikvidovat kompletní software daného firewallu. Proto je velmi důležité spojit firewall s další bezpečnostní ochranou. Firewally se rozdělují do třech základních skupin :

- stavové
- nestavové
- proxy

Stavové firewally srovnávají stav síťového spojení a bezpečnostní politiky. I přes lepší výkon nemohou stavové firewally pracovat se zabezpečením na aplikační úrovni. Nestavové firewally se vyznačují vlastností, že neukládají informace o síťovém připojení a nemohou tedy využívat informace o protokolech. Nejvíce bezpečné jsou proxy firewally, ale zároveň jsou nejvíce citlivé vůči parsovaným protokolům.

6.2 Systém honeypotů

Jedná se o systémy, které mají vlastnost nalákat útočníka k jejich bezprostřednímu napadnutí. Jejich zabezpečení proti útoku je nastaveno na velmi nízkou úroveň, aby bylo možno je lépe napadnout. Při napadnutí mají honeypoty tu vlastnost, že útok udrží a další šíření útoku je velmi obtížné. Důvodem honeypotů je získání motivů a taktiky útočníků.

Mezi nejznámější autory zabývající se touto technikou obrany patří Lance Spitzner, který je autorem titulu Know your enemy. Spitzner rozděluje honeypoty na dva základní typy – s vysokou a nízkou mírou interakce. S nízkou interakcí mají za úkol simulovat síťové služby. Mezi jejich přednosti patří možnost zachycení určité části útoku. Honeypoty s vysokou interakcí jsou zranitelné systémy , které pracují na odlišných operačních systémech. V případě průniku počítačového červa do systému může být v případě zachycení zaslán do analytického centra na prozkoumání. Honeypoty neplní pouze funkci nástrahy na počítačové červy, ale užívají se také jako nástroj pro boj se spamy.

6.3 Protiútoky

Další technikou obrany je zahájení protiútoku proti infikovanému systému s cílem tento systém vyléčit. Nemnoho úspěšná byla snaha některých profesionálů, kteří se snažili zpětným útokem počítačového červa odstranit systém útočníka, jelikož za takovéto pokusy byly ve velkém měřítku odsouzeni. V případě techniky obrany pomocí protiútoků musí mít uživatel souhlas administrátora sítě nebo být sám administrátorem. Uživatel musí mít také na paměti, že u této metody může snadno dojít k poškození nebo úplné ztrátě dat.[1]

7 Výběr antivirového programu

Pro srovnávací test antivirů jsem zvolil čtyři antivirové programy, které jsou v dnešní době nejvíce oblíbeny u uživatelů domácího počítače. Při porovnávání se u jednotlivých druhů zaměřím na jejich celkovou cenu v závislosti na počtu licencí, na systémové požadavky, které kladou na osobní počítač při instalaci, na množství poplašných zpráv, na procentuální úspěšnost detekce škodlivého softwaru a na skenovací rychlost jednotlivých antivirů. Ke srovnávacímu testu jsem zvolil poslední dostupné verze jednotlivých antivirových programů.

Jedná se o :

- Eset NOD 32 Antivirus 4
- AVG Anti-Virus 2011
- Avast! Pro Antivirus 6
- Kaspersky Anti-Virus 2011

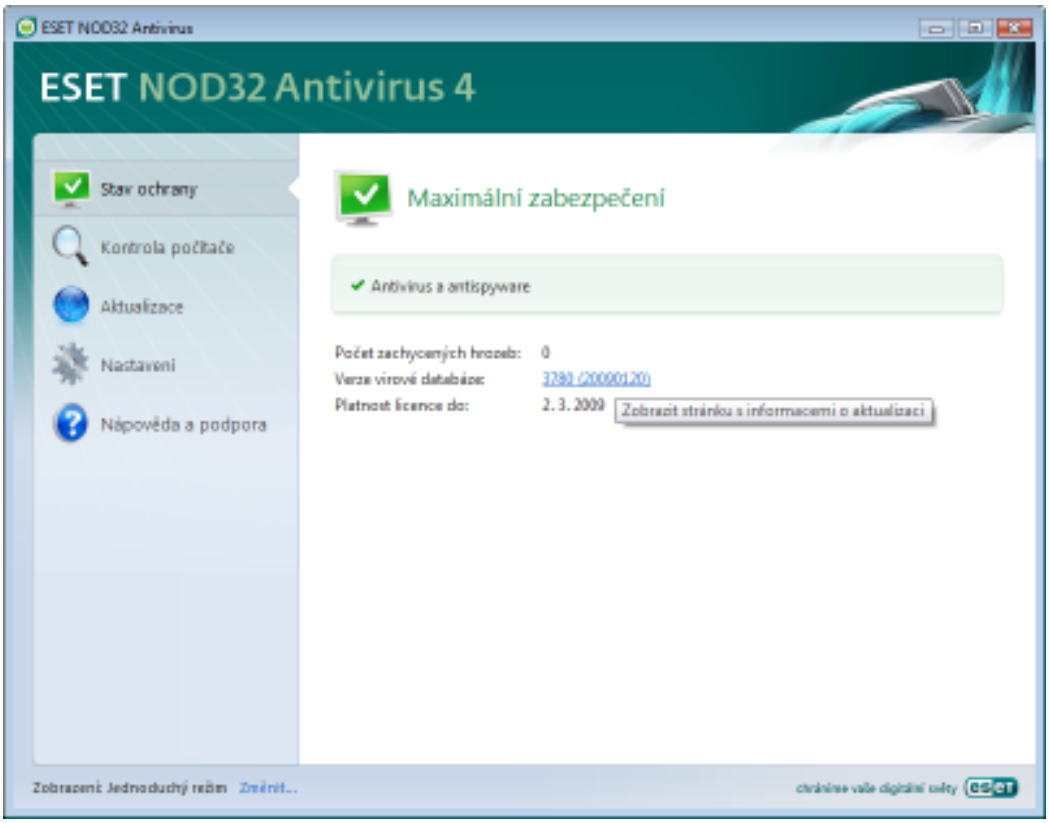
7.1 Požadavky domácího uživatele

Převážná většina domácích uživatelů upřednostňuje při koupi antivirového programu hlavně tyto požadavky :

- nejmenší pořizovací cena
- nejmenší systémové požadavky
- nejvyšší % úspěšnosti detekce
- nejmenší množství poplašných zpráv
- nejvyšší skenovací rychlost

V následujících srovnávacích tabulkách budou bodově hodnoceny jednotlivá kritéria. Hodnocení jsem zvolil v rozsahu bodů 1-5, kde 1 označuje nejnižší hodnocení a 5 označuje nejvyšší hodnocení. V závěru bakalářské práce zrekapituluji konečné výsledky a doporučím domácímu uživateli vítězný antivir.

7.2 Eset NOD 32 Antivirus 4



Obrázek 1. – Eset NOD 32 Antivirus 4

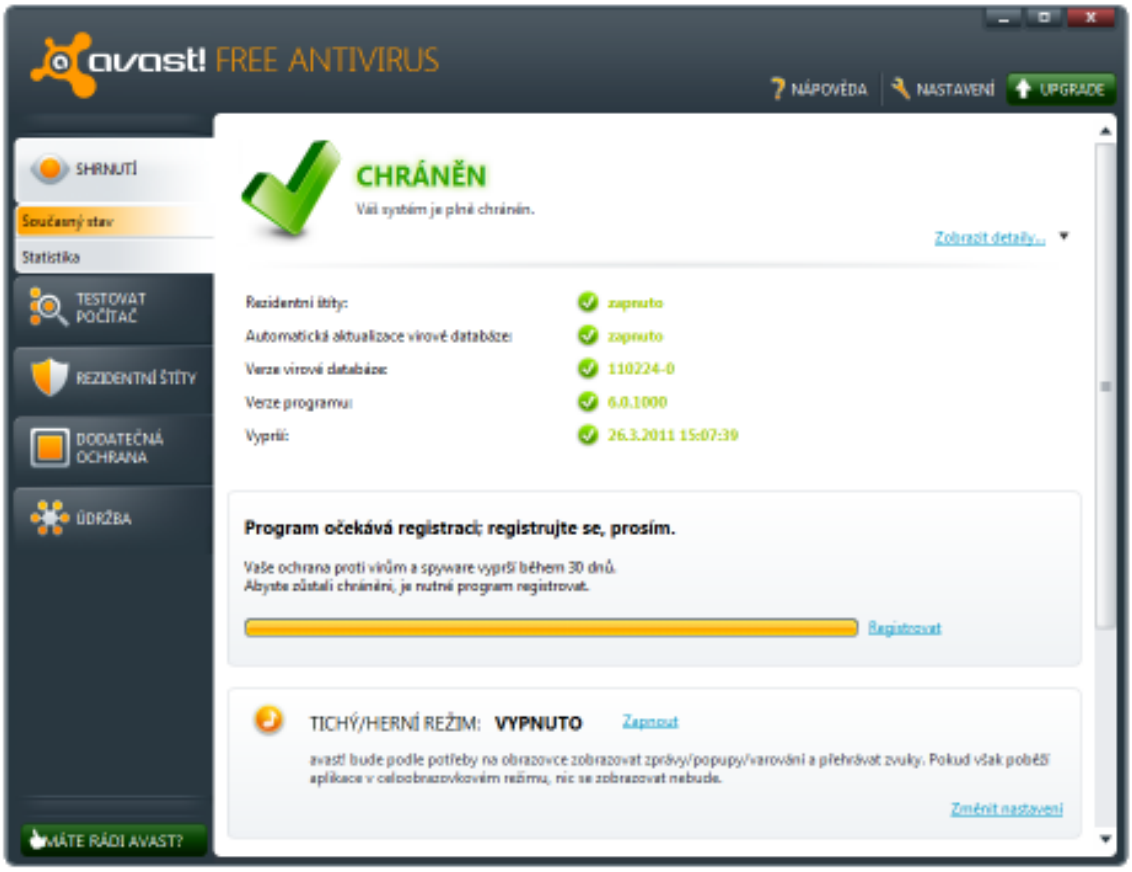
Mezi hlavní výhody tohoto produktu patří technologie ThreatSense, která zaručuje nepřetržitou ochranu v reálném čase. Dále nabízí automatickou kontrolu při připojení přenosných médií. Vyznačuje se také velmi vysokou úsporností energie, jelikož při napájení pomocí baterie je automaticky přepnut do úsporného režimu bez ohledu na úroveň zabezpečení PC. Mezi jeho přednosti patří i nejvyšší ochrana zabezpečení bez předchozího nastavení, což nejvíce uvítají méně pokročilí uživatelé. [7]

7.3 AVG Anti-Virus 2011

Obrázek 2. – AVG Anti-Virus 2O11

Revoluční novinkou tohoto antiviru je aplikace AVG social Networking Protection, která uživatele ochraňuje na stále více populárních sociálních sítí. Ochrana je založena na automatické kontrole zasílaných odkazů prostřednictvím sociální sítě. Stejně jako u NOD 32, i zde je ochrana v reálném čase pomocí aplikace AVG LinkScanner, která rozpozná škodlivé stránky před jejich otevřením. [8]

7.4 Avast! Pro Antivirus 6



Obrázek 3. – Avast! Pro Antivirus 6

Obsahuje unikátní systém skenování, který vyčistí počítač od nežádoucích vlivů před zavedením samotného operačního systému Windows. Mezi další výhody patří zablokování škodlivého kódu určeného pro krádeže při načítání operačního systému v době, kdy je neviditelný pro ostatní prostředky k detekci. Aplikace avast! WebRep umožňuje poskytnutí informací o spolehlivosti jednotlivých internetových stránek na základě hodnocení ostatních uživatelů produktu avast!. Velmi výhodná je i funkce SafeZone, která vytvoří na počítači speciální prostor neviditelný pro ostatní aplikace ve kterém lze bezpečně nakupovat a užívat online banovnictví. [9]

7.5 Kaspersky Anti-Virus 2011

Obrázek 4. – Kaspersky Anti-Virus 2011

Umožňuje instalaci antiviru i na zavirovaný počítač. Novinkou je možnost přehledu o bezpečnosti systému v postraním panelu systému Windows. Pomocí heuristické analýzy blokuje podezřelé soubory v operačním systému. Jinak má vylepšené všechny standartní funkce jako kontrolu webových stránek nebo ochranu proti virům v reálnem čase. [10]

7.6 Srovnání jednotlivých antivirů

Většina domácích uživatelů se při výběru antivirového programu zajímá v první řadě o celkovou cenu produktu. V následujících srovnávacích testech uvedu nejčastější kritéria, které by měl domácí uživatel sledovat při nákupu antivirového programu. K porovnání jsem si zvolil pro každou kategorii váhy, na základě kterých jsem poté jednotlivé antiviry bodově ohodnotil. Jednotlivé váhy a bodové hodnocení pro daná kritéria jsou zobrazena v následující tabulce.

Kritéria / Body	1	2	3	4	5
Cena 1 rok	1001-1100	901-1000	801-900	701-800	601-700
Cena 2 roky	1401-1500	1301-1400	1201-1300	1101-1200	1001-1100
Paměť RAM	601-750	451-600	301-450	151-300	0-150
Místo na disku	801-1000	601-800	401-600	201-400	0-200
Faleš.poplachy	35-44	27-35	18-26	9-17	0-8
Skenovací rychlost	4-6,9	7-9,9	10-12,9	13-15,9	16-17,9
Detekce (%)	97,6-98	98,1-98,5	98,6-99	99,1-99,5	99,6-100

Tabulka 1. – Kritéria a bodové ohodnocení

7.6.1 Srovnání podle ceny

Jednotlivé ceny uvedených antivirů jsou uvedené bez dph a pro jeden osobní počítač. Cenové hodnoty byly nashromážděny na domovských stránkách produktů, které jsou označeny v seznamu literatury čísly [7 – 10]. V následující tabulce jsou popsány jednotlivé ceny závislé na době trvání licence antiviru a jejich bodové ohodnocení na základě stanovených vah.

Licence	NOD 32	AVG	Avast!	Kaspersky
1 rok	999 kč	726 kč	820 kč	705 kč
2 roky	1499 kč	1079 kč	1025 kč	1128 kč
Body	2+1	4+5	3+5	4+4
Celkem	**3**	**9**	**8**	**8**

Tabulka 2. – Porovnání cen antivirů

Z uvedené tabulky je patrné, že v případě jednoroční licence je cenově nejvýhodnější Kaspersky. Za menší nevýhodu bych bral absenci zakoupení licence na tři roky, i když nabízí možnost prodloužení končící licence. Jako nejdražší volba bez ohledu na délku licence vyšel produkt společnosti Eset NOD 32. Nejlevnější volba bez ohledu na dobu trvání licence je antivir AVG.

7.6.2 Srovnání podle systémových požadavků

Kromě ceny je při výběru antiviru důležitý aspekt systémových požadavků. Projevuje se především v domácnostech, kdy hodně záleží na finančních prostředcích uživatele vložených do osobního počítače. Antivir nainstalovaný na počítač, který nesplňuje minimální požadavky na instalaci, by nemusel plnit všechny zabezpečovací funkce jako v případě kompatibilního počítače.

Následující tabulka ukazuje minimální požadavky jednotlivých antivirů při instalaci. V obecném měřítku uživatel upřednosťnuje co nejmenší obsazené místo na pevném disku a co nejmenší paměť.

Sys.požadavky	**NOD 32**	**AVG**	**Avast!**	**Kaspersky**
Paměť RAM	60 MB	512 MB	128 MB	512 MB
Místo na disku	230 MB	750 MB	100 MB	480 MB
Body	5+4	2+2	5+5	2+3
Celkem	**9**	**4**	**10**	**5**

Tabulka 3. – Porovnání požadavků antivirů

Z uvedené tabulky z hlediska paměťové náročnosti vyčnívá NOD 32, který je se 60 MB v porovnání s AVG a Kaspersky bezkonkurenční. V porovnání zabrané velikosti na pevném disku při instalaci antiviru vyšel nejhůře AVG, který zabírá velikost 0,75 GB. Tato velikost je v porovnání s ostatními antiviry nezvykle vysoká.

7.6.3 Srovnání podle úspěšnosti detekce

Hlavní činností antivirových programů je detekce a ochrana před škodlivým softwarem. Pro domácího uživatele je tedy tato vlastnost nezbytná při rozhodování o koupi antivirového programu. V praxi platí, že čím vyšší je rychlost detekce, tím je antivir výkonější. Hodnocení detekce je prováděno v procentuálním zastoupení úspěšnosti detekování škodlivého softwaru. Vnásledující tabulce jsou uvedeny hodnoty detekcí v procentech s příslušným bodovým ohodnocením podle nastavených vah.

Detekce	NOD 32	AVG	Avast!	Kaspersky
Úspěšnost (%)	98,6	98,3	99,3	98,3
Body	**3**	**2**	**4**	**2**

Tabulka 4. – Porovnání úspěšnosti detekce [12]

Z hlediska úspěšnosti detekce jsou všechny antiviry poměrně vyrovnané a všechny patří v této kategorii ke světové extratřídě.

7.6.4 Srovnání četností detekce falešných poplachů

Všechny antivirové programy byly v testu podrobeny zkoumání na totožných počítačových souborech. Jako výsledek testu byly sledovány falešné poplachy, které antiviry hlásili v domnění nálezu škodlivého softwaru. Posuzovacím měřítkem je množství výskytu takových poplachů, kde čím méně jich daný antivir ohlásí, tím lépe je hodnocen. Následující tabulka znázorňuje výsledky testu zkoumání četností detekce falešných poplachů u jednotlivých antivirů.

Falešné poplachy	NOD 32	AVG	Avast!	Kaspersky
Počet poplachů	6	19	9	44
Body	**5**	**3**	**4**	**1**

Tabulka 5. – Porovnání počtu poplachů [11]

Z uvedené tabulky nejvíce vyčnívá antivir Kaspersky, který měl ze všech testovaných antivirů největší množství falešných poplachů a získal tedy nejméně bodů.

7.6.5 Srovnání skenovací rychlosti

U většiny antivirových programů záleží nejen na detekci samotné, ale i na skenovací rychlosti, kterou je antivir schopen dosáhnout. Tato rychlost je měřena v jednotkách MegaBytu/sekundu a platí zde, že čím je rychlost vyšší, tím je antivirový program výkonější. Následující tabulka znázorňuje nejvyšší dosažené rychlosti u jednotlivých druhů antivirů.

Skenovací rychlost	NOD 32	AVG	Avast!	Kaspersky
Rychlost (MB/sec)	9,5	13	17,2	9,8
Body	**2**	**4**	**5**	**2**

Tabulka 6. – Porovnání skenovací rychlosti [12]

Z tabulky vyplívá, že nejvyšší skenovací rychlost má z pozorovaných antivirů Avast!. V poměru s Nod 32 a Kaspersky je tato rychlost téměř dvojnásobná.

8 Závěr

V praktické části mé bakalářské práce jsem se snažil doporučit domácímu uživateli nejvhodnější antivir. K výběru jsem využil metodu vícekriteriální analýzy, kdy jsem si zvolil pro daná kritéria váhy včetně bodového ohodnocení. K porovnání jsem zvolil pět základních kritérií a to cena produktu, systémové požadavky, úspěšnost detekce, množství poplašných zpráv a skenovací rychlost. K testu jsem využil poslední verze čtyř nejoblíbenějších antivirů mezi uživateli: NOD 32, AVG, Avast! a Kaspersky.
V následující tabulce jsou uvedeny dílčí výsledky pro jednotlivá kritéria včetně konečného hodnocení.

Celkové hodnocení	NOD 32	AVG	Avast!	Kaspersky
Licence	**3**	**9**	**8**	**8**
Sys.požadavky	**9**	**4**	**10**	**5**
Falešné poplachy	**5**	**3**	**4**	**1**
Skenovací rychlost	**2**	**4**	**5**	**2**
Detekce	**3**	**2**	**4**	**2**
CELKEM	**22**	**22**	**31**	**18**

Tabulka 7. – Celkové zhodnocení

Z celkové tabulky vyšel vítězně antivir Avast! Pro Antivirus 6, který ve sledovaných kritérií ani v jednom nepropadl. K příznivé pořizovací ceně a nízkým instalačním požadavkům přidal nejvyšší skenovací rychlost s největším procentem úspěšnosti a je tedy vítězem zaslouženým. Ostatní antivirové programy by se pro své

výborné vlastnosti daly také doporučit, ale jako nejvhodnějšího kandidáta pro domácího uživatele doporučuji koupi antiviru od společnosti Avast!.

Seznam literatury

[1] SZOR, Peter. Počítačové viry – analýzy útoku a obrana. Brno : Zoner Press 2006. 608s. ISBN 80-86815-04-8

[2] Technet.cz [online]. Datum citace 2011-2-17. Dostupné z: http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A0411035285981bezpecnost

[3] Svethardware.cz [online]. Datum citace 2011-2-18. Dostupné z: http://www.svethardware.cz/art_doc4013E34C24856B88C125755900501965.html

[4] ENDORF, Carl. Detekce a prevence počítačového útoku. Praha : Grada 2005. 355s. ISBN 80-247-1035-8

[5] Eset.cz [online]. Datum citace 2011-2-23. Dostupné z: www.eset.cz/cz/podpora/rejstrik

[6] KRÁL, Mojmír. Bezpečnost domácího počítače. Praha : Grada 2006. 334s. ISBN 80-247-1408-6

[7] Eset.cz [online]. Datum citace 2011-3-10. Dostupné z: http://www.eset.cz/cz/domacnosti/produkty/antivirus/

[8] Avg.com [online]. Datum citace 2011-3-10. Dostupné z: http://www.avg.com/cz-cs/buy-antivirus,

[9] Avast.com [online]. Datum citace 2011-3-10. Dostupné z: http://www.avast.com/cs-cz/pro-antivirus,

[10] Kaspersky.cz [online]. Datum citace 2011-3-10. Dostupné z: http://www.kaspersky.cz/produkty/domaci-uzivatele/kaspersky-anti-virus/

[11] av-comparative.org [online]. Datum citace 2011-3-22. Dostupné z: http://av-comparatives.org/images/stories/test/fp/avc_fp_aug2010.pdf

[12] av-comparative.org [online]. Datum citace 2011-3-22. Dostupné z: http://av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf