Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

KII

Bakalářská práce

Viry a antiviry

Jitka Těšínská

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Viry a antiviry" jsem vypracovala 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. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 29.3.2010 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Markovi Píckovi za konzultace a pomoc při vypracování bakalářské práce.

Viry a antiviry

Virus and antivirus software

Souhrn

Bakalářská práce se zabývá hodnocením jednoho z nejvyužívanějších antivirových programů. Úvodem se zabývá charakteristikou základních hrozeb pro počítač a historickým vývojem virů a jejich účinky. Následuje popis současných virů a antivirů. Dále se zabývá detailním rozborem vybraných typů antivirových programů z hlediska dostupnosti, funkcí a možností. Závěrečná část je věnována hodnocení antivirových programů a doporučení uživatelům.

Klíčová slova:

Viry, antiviry, antivirový program, základní hrozby

Summary

This Bachelor‘s thesis deals with the assessment of one the top antivirus software. The first part describes the basic threats for computers and tries to define the evolution of viruses and their actual effect followed by the description of present viruses and antivirus softwares. The bachelor‘s thesis also lays out a detail analysis of a chosen antivirus programs in terms of the availibility, function and possibility. The last part focuses on the assesment of these antivirus programs and also the recommendations for the customers.

Key words:

Virus, antivirus, antivirus software, basic threats

1.Úvod

Internet se v poslední době stal nedílnou součástí nejen mnoha domácností. Možností setkat se s internetem je několik - ve školách, v knihovnách, na úřadech, v zaměstnání a v neposlední řadě doma. Nejčastěji je využíván k rychlému získávání informací. K tomu, aby se uživatel cítil bezpečně, je důležité používat antivirové programy.

Antivirové programy by měly být součástí každého počítače či notebooku. V současné době existuje na trhu nepřeberné množství takových programů, a tak si každý uživatel může vybrat podle osobních preferencí (cena, vlastnosti, aktualizace apod.). Existují antiviry pro domácí využití i pro potřebu společností. Jenže samotný program bezpečnou funkci počítače nezaručí. Je třeba dodržovat jisté další bezpečnostní opatření. Vybrat si pro počítač ten nejvhodnější antivir nemusí být vždy lehké. Proto vznikla tato práce s cílem vyhodnotit vybrané antivirové programy a usnadnit tak rozhodnutí.

2. Cíl práce a metodika

2.1 Cíl práce

Cílem předkládané bakalářské práce na téma ,,Viry a antiviry‘‘ je především srovnání možností vybraných antivirových programů a jejich následné hodnocení. Dílčí cíle práce jsou:

1. Charakterizovat hrozby pro počítač v internetu.
2. Shrnout vývoj virů a antivirů.
3. Charakterizovat viry a antiviry.

Část práce je věnována popisu základních pojmů, vývoji virů a antivirů, vysvětlení funkcí antivirových programů a jiných podobných bezpečnostních softwarů. Praktická část se zabývá hodnocením vybraných typů antivirů podle jejich prezentace na webu. Práce se dále věnuje základním prvkům ochrany počítače a zásadám bezpečnosti, které by měl běžný uživatel dodržovat. V závěru práce je doporučení uživatelům a vyhodnocení vybraných antivirů.

2.2 Metodika

Vývoj virů a antivirů a jejich charakteristika bude popsána na základě získaných informací, čerpaných ze zdrojů, které jsou uvedeny v seznamu literatury. Budou vylíčeny základní typy virů a antivirů, jejich projevy a principy činnosti antivirových programů. Dále bude charakterizováno pět druhů antivirových programů a na základě sumarizovaných údajů bude sestavena hodnotící tabulka. Budou použity screeny pro

lepší představivost o vzhledu vybraného antivirového programu. Pro výběr nejlepšího antiviru bude použita metoda váženého průměru, která se používá v případě, že hodnoty v pozorovaném souboru mají různou důležitost. Bude vybráno 5 ukazatelů, které bývají směrodatné pro uživatele při volbě vhodného antiviru. Každé kategorii budou přiřazeny váhy tak, aby jejich součet byl 100%. Dále bude přidělena známka v rozmezí od 1 do 5, přičemž číslo pět představuje nejlepší hodnocení. Odůvodnění přidělených bodů bude popsáno pod hodnotící tabulkou.

Pro výpočet výsledných hodnot bude použit vzorec váženého průměru:

$$\bar{x} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$$

3.Hrozby pro počítač v internetu

Hrozba počítačových virů se v dnešní době neustále zvětšuje. Jedním z faktorů je i větší množství používaných počítačů nebo notebooků, není to ale jediný faktor..

V literatuře se lze často setkat s různými soubory programů, pod společným označením viry. Definici viru ani leckteré z nich neodpovídají (nemají systém sebereprodukce a podobně). Zde je uveden jejich souhrnný přehled: [1]

Softwarové bomby [1, 2] jsou programy, které když docílí určitých podmínek, zpravidla po určitém čase, něco zničí – důležitá data, programy, v krajní situaci i technické vybavení počítače. Bomba však není virem, protože nesplňuje základní podmínku viru – nerozmnožuje se.

Trojský kůň [1, 2, 3] funguje obdobně jako bomba. Vypadá spíše jako bomba v dárkovém balení. Trojský kůň je program, který nabízí nějakou zajímavou a většinou uživateli vítanou službu (často bývají trojskými koni diskové utility, nebo programy kreslící na monitoru spoře oděné slečny v kompromitujících pozicích), kterou mohou někdy i vykonat, vzápětí ale vpustí do systému to škodlivé, co obsahuje – virus, bombu či špiona.

Virem nebývá ani *špion* [1, 3]. Podstatou tohoto programu je přinést svému stvořiteli nějakou zprávu, kterou běžně používanými nástroji nelze odhalit. Charakteristickou úlohou těchto špionů bývá zjišťování hesel. Dobrý špion se po vykonání úkolu vymaže, takže se jeho činnost po nějakém časovém intervalu stane nedohledatelnou . Pokud dojde ke spojení špionů a trojského koně, stane se tato kombinace velmi silnou zbraní hackerů.

V praxi je možné se setkat také s označením *neškodné viry* [2, 3]. Pojem neškodný je samozřejmě diskutabilní. I ten nejneškodnější virus se může stát nebezpečným, pokud se například začne v síti množit tak rychle, až ji úplně zaplní.

Trpaslík [3, 4] je vir, který nepáchá nic zlého, naopak může pomoct třeba při pakování dat při zápisu na disk, takže se jich tam vejde potom mnohem víc. Nebo *skřítek*, který už není tak přátelský jako trpaslík a uživatele počítače může všelijak potrápit– například tím, že po obrazovce leze brouk , který si občas pochutná na nějakém tom písmenku, ale skutečně vážnou škodu nenadělá.

Vyskytují se samozřejmě i neškodní *červi* [4], ale na základě Murphyho zákona jejich neškodnost musí být pouze podmíněná. Je znám příklad červa, který měl za úkol popřát všem uživatelům sítě BITNET veselé vánoce. Červ se však množil tak rychle, že během krátké doby síť úplně zahltil. V důsledku zahlcení sítě musela být dána mimo provoz a s vynaložením určitého úsilí od červa vyčištěna.

V případě prostoupení systému profesionálem (většinou jde o proniknutí do objemných systémů, které se používají ve finančnictví) obsahuje obvykle počítač komplikovaný systém vzájemně se podporujících programů a nástrah (zvaných někdy také *miny* [1]), které mohou při neopatrném pohybu – tj. snaze odstranit nebo jen popsat infiltraci – „explodovat“ a smažou za sebou všechny stopy (často taky varují svého tvůrce, který si včas vybere miliónové konto a pro jistotu se vydá na cestu kolem světa). Při výbuchu se mohou ztratit i některá důležitá data, typickým případem to ale není – profesionálové, až na výjimky, nebývají škodolibí.

Nakonec zmínka o *krmítku* [1, 4]– prostředku, který se občas v literatuře doporučuje jako zbraň proti některým skřítkům. Jak bylo již řečeno, oblíbeným trikem skřítků totiž je otravovat uživatele s prosbou o něco (nejčastěji nesplnitelného). Skřítek čas od času prohlásí ‚I want a cookie‘ a očekává že uživatel napíše cookie. Princip krmítka spočívá v existenci rezidentního programu, který po stisknutí určitých kláves (např. ALT-I) nakrmí skřítka tak, že simuluje vypsání slova cookie.

Vlastní virus v užším slova smyslu je program, který cizopasí na jiných programech, anebo na vlastním operačním systému, je s nimi přenášen na další počítače, na kterých se samozřejmě dál množí. [1]

4.Vývoj virů a antivirů

Viry (stejně jako jiné programy) vytvářejí lidé. A to buď přímo nebo k tomu využívají nástroje speciálně určené pro tyto účely. První dokumentovaný virus pochází z roku 1983. Tehdy byl virus určený pro studijní účely. Byl vytvořen pro přednášku o počítačové bezpečnosti.[3, 4]

Člověk ale chybuje a také se může mýlit, a proto může vytvořit dílo obsahující chybu, popřípadě chyby. Přesněji řečeno jen málokdy se podaří vytvořit dílo chyby neobsahující. Pohromu proto může způsobit i napohled neškodný vir, a to kvůli neúmyslně vytvořené chybě. K podobné situaci dohází i díky vývoji operačního systému a podpůrných programů. Daný vir mohl být v dřívější verzi operačního systému naprosto neškodný a v jeho nové verzi nemusí fungovat (to je ta příjemnější věc), nebo se naopak může stát katastrofou. [4, 5]

Jelikož jsou tvůrci virů různí, liší se od sebe také viry. Nové viry [4] jsou často vytvořeny výkonným programátorem, který má k naprogramování takového díla předpoklady. Naštěstí tito programátoři mají natolik vysokou inteligenci, tudíž vir neobsahuje žádnou výrazně destruktivní jednotku. Autor totiž ví, co znamená ztráta dat. Tyto viry disponují mechanismem, který umožňuje autorovi vir předem identifikovat a poté zastavit. I zde samozřejmě existují nebezpečné viry. Jejich počet je ovšem nižší. Změna některých instrukcí v těle viru s cílem znemožnění identifikace známým antivirovým programem společně se změnou v chování viru vede k přepracování virů. Tyto změny navíc nezaberou mnoho času, tudíž je možné vytvořit několik nových mutací za poměrně krátký časový interval.

Očkování, neboli vakcinace [6] slouží k ochraně před viry. Termín vakcína se používá i v počítačové terminologii a je to program sloužící k odhalení virů, omezení jejich činnosti a případně také k jejich odstranění.

První antivirový software se objevil v roce 1988 [5] a vytvořil indonéský programátor. Tento software uměl najít virus Brain, odstranit ho a zajistit imunitu

počítače před dalším útokem stejného viru. Na to vznikl velký počet specializovaných systémů na ochranu počítačů před napadením viry. Vznikly také firmy, které se zabývají tímto specifickým odvětvím počítačových programů. Dodnes existuje názor, že v případě opadávajícího zájmu o výrobky těchto firem prostě nějaký ten vir pustí do světa. Tyto firmy pak se zpožděním několika hodin oznámí, že mají patřičný antivir a poté ho zařadí do své antivirové databáze.

V roce 1989 spatřil světlo světa nebezpečný virus Dark Avenger [5], který rychle napadl programy, ale škody napáchané tímto virem probíhaly poměrně pomalu, takže na počítačích bez antivirových ochran zůstal dlouhou dobu skryt. V té době přichází na trh IBM s prvním komerčním antivirovým programem a je zahájen intenzivní antivirový výzkum. Jak se hned v roce 1990 ukazuje, mělo to svůj důvod, protože na svět přicházejí nové a vyvinutější formy virů, které nazýváme polymorfními (dovedou se při šíření modifikovat) a viry mnohostranné, které zamořují různé oblasti v počítači.

Rok 1991 byl pro vznik nových virů obzvláště důležitý, neboť na Virus-exchange boards [5, 6] se začaly objevovat konstrukční soupravy, díky kterým bylo umožněno vytvořit si vlastní vir komukoliv, kdo některou ze souprav zkusil. Zatímco na začátku roku mělo zkušenosti s napadením virem asi jen 9% firem, na konci stejného roku už to bylo 63%. O rok později se začal rychle šířit virus Michelangelo, který se aktivoval 6. března, tedy v den, kdy se slavný umělec narodil, a přepsal úseky napadených pevných disků. V důsledku toho vzrostla poptávka po antivirových programech a společnostem, které se zabývaly antiviry, začaly žně.

5.Viry a antiviry

Virem bývá mezi počítačovou veřejností obecně nazýván každý program, který se do počítače dostane bez vědomí jeho uživatele a tropí uvnitř nějakou neplechu. Podle [1] by pokus o přesnější definici by mohl vypadat např. takto:

Počítačový virus je program nebo součást programového kódu, který má schopnost sebereprodukce (šířit se) a více nebo méně škodlivé účinky.

Druhá část definice je samozřejmě trochu problematická. Lepší by nejspíš bylo vymezit virus jako program, který do systému prostupuje bez vědomí uživatele (k tomu právě poslouží jeho schopnost sebereprodukce).

Užívání odborného termínu virus, převzatého z biologie, nabízí řadu dalších výrazů převzatých z biologie, které dostatečně pasují i pro počítače a do hojné míry se vskutku vžily:

Program, který není napaden žádným virem, nebo program, který byl napaden, ale je již vyléčen, je zdráv [7]. Program, který virem napaden je, je nakažený. Pravděpodobně to na něm nějakou chvíli po napadení bude ještě znát, protože dosud neproběhla inkubační doba, po které se virus teprve začne projevovat. V průběhu inkubační doby, a samozřejmě i po jejím vypršení, můžeme virus v programu či jinde v systému odhalit provedením řady testů, kterým se kupodivu obvykle neříká diagnóza, ale detekce. Podařilo-li se virus detekovat, můžeme začít léčbu., tj. odstraňování viru ze systému. Může se při tom stát, že leckterý program bude mrtev – díky působení viru nepracuje a nelze jej již obnovit. Některé viry mohou dokonce vytvořit zombie – mrtvé programy, které nicméně při pokusu o spuštění virus stále šíří.

Při podrobnějším pohledu na vir je možné zjistit,že je zpravidla možné programy uspořádat, někdy také očkovat takovým stylem, že virus na ně již nezaútočí. Nejhojnější metodou je „obalamucování“ viru tak, aby odhalil, že program je již napaden – což

samozřejmě není pravda. Je to však velmi působivé, protože snad žádný virus nezaútočí na jeden program vícekrát. Úspěšný očkovací program se stává proti viru odolný. [1, 7]

5.1 Klasifikace počítačových virů podle rychlosti šíření

Podle [8] je klasfikace počítačových virů z hlediska rychlosti následující:

Rychlé viry se vyznačují rychlým napadáním všech programů, které jsou v danou chvíli otevřeny. To vede k napadení všech spustitelných souborů na disku. Pro své napadení mohou i aktivně vyhledat na disku soubory, které jsou podle nich vhodné.

Pomalé viry v paměti odkládají svou činnost. Ukáží se teprve tehdy, kdy se s daným programem pracuje a přitom se zvolna množí, aniž by to uživatel zpozoroval. To jim dává čas na nakažení všech přístupných paměťových médií.

Viry vzácně napadající napadají soubory po splnění určitých podmínek (např. každý pátý soubor). Snižují pravděpodobnost odhalení.

5.2 Stavba viru

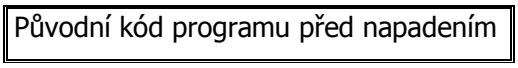
Každý virus se skládá alespoň ze tří samostatných částí [9]: *rozmnožovací systém*, jehož úkolem je kopírování viru do dalších programů a *záškodnickou jednotku* , která provádí destruktivní akce viru a to na pokyn *spouštěcího mechanismu*. Může se stát, že některá z těchto částí může chybět, ale jen ve výjimečných případech. Další podsložkou je *systém utajení*, díky kterému se virus stane těžko odhalitelným. Celé to může být doplněno i aktivní obranou.

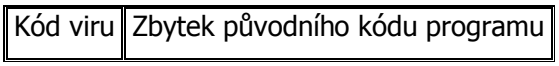
5.2.1 Rozmnožovací systém

Rozmnožovací systém vlastně dělá virus virem. Zajišťuje šíření viru a to jak uvnitř napadeného systému tak i na další dosud nenapadené počítače. Obě úlohy jsou zpravidla zajišťovány stejným mechanismem. [9]

Nejjednodušší rozmnožovací systém mají viry vytvářející zombie. Podstatou je, že takový virus prostě vyhledá spustitelné programy a přepíše jejich začátek sám sebou (začátek – necelý kód) proto, že běžný virus je mnohem kratší než naprostá většina běžných programů. Nevýhoda tohoto systému je, že při prvním spuštění napadeného programu dochází k aktivaci daného virus , ale pak se buď nestane vůbec nic nebo naopak se zhroutí systém. Díky tomu se zombie pozná na první pohled a s jeho analýzou se virus dá snadno vypátrat. [6, 9]

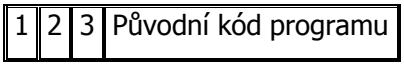
5.2.1.1 NAPADENÍ PROGRAMU PŘEPISUJÍCÍ VIREM

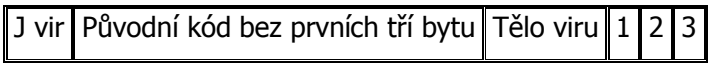




U naprosté většiny viru se shledáme s vyvinutějším systémem rozmnožování. Pokud je program napaden, není přepsán , ale je upraven takový stylem, že pokud se spustí, aktivuje se namísto programu virus. Ten mezitím provede co provést chce a nakonec obnoví v paměti původní program a spustí jej. Uživatel občas tedy ani neví o tom, že uvnitř jeho systému řádí virus, dokud ho na to neupozorní nějakým velmi nepříjemným způsobem – například ztrátou dat na celém pevném disku. Napadený program lze na první pohled poznat, a to podle jeho délky, protože je větší právě o délku viru. Musíme ovšem znát jeho původní délku. [6, 9]

5.2.1.2 NAPADENÍ PROGRAMU NEPŘEPISUJÍCÍ VIREM





Některé viry tento způsob rozmnožování přivedou k dokonalosti ještě tím, že uvnitř programu najdou neinicializovaná data, nebo že kód programu nějakým způsobem pakují, aby velikost programu zůstala i po napadení stejná. Dalším velmi rozšířeným způsob rozmnožování virů je napadení operačního systému počítače tak, že při běžných úkonech (jako je kupříkladu zápis na disketu) se účastní i rozmnožovací systém viru. Takové viry, které se nějakým způsobem připojují ke spustitelným programům, nazýváme link viry (anglicky to link – připojit). Viry napadající operační systém však většinou patří do velké skupiny tzv. boot virů. [9]

5.2.2 Spouštěcí mechanismus

Spouštěcí mechanismus se vlastně může zařadit mezi systémy utajení. Takový virus, který by bezmyšlenkovitě ničil vše na co přijde, by byl pravděpodobně brzy odhalen. Proto většina viru má nějakou inkubační dobu, ve které se pouze množí. Páchat škody začne teprve tehdy, když je jeho kopií opravdu plný systém. Nejjednodušším typem spouštěcího mechanismu je časový mechanismus. Je množství virů, které se aktivují zásadně v pátek třináctého nebo prvního dubna. Zvláště škodolibé viry si vybírají 24. prosince. Jiným spouštěcím mechanismem je tzv. jednoduchý čítač. Virus se aktivuje poté, co se mu podařilo napadnout předem určený počet programů. Často se to děje na základě nějakého náhodného algoritmu – jeden virus může zjistit systémový čas , a je-li počet vteřin dělitelný osmi, zaútočí. [9]

5.2.3 Záškodnická jednotka

Znakem záškodnické jednotky je provádění něčeho, co uživatele příliš nepotěší. Nejjednodušší přepisující viry záškodnickou jednotku vůbec nemají a jejich nevítaná činnost spočívá v ničení napadených programů, ze kterých se, jak již bylo uvedeno, stávají nevyléčitelní zombie. Velká část virů má záškodnickou jednotku neškodnou – jedná se o žertíky, které se projevují „padajícími“ písmenky na obrazovce, převracením pohybu myši (táhneme-li myš nahoru, pohybuje se kurzor směrem dolů), nebo se simulací hardwarových chyb (včetně zcela absurdních oblíbených hlášení typu „Voda v disketové mechanice.“, nebo „Odpoj myš, v okolí jsou kočky.“). Tyto viry jsou sice nepříjemné, ale nepředstavují významnější ztráty (nevoláme-li ovšem zbytečně drahého opraváře kvůli viru simulující hardwarové chyby). Mnohem větší škody napáchají viry, které ničí data. [10]

Předejít tomuto napadení dat [9] můžeme mazáním souborů nebo formátováním disku. Kromě toho existují rafinovanější viry, které pouze zničí logickou strukturu disku (efekt je víceméně srovnatelný s přeformátováním, ale jde to mnohem rychleji), nebo které na náhodná místa v datových souborech ukládají náhodné nesmysly. Takto se nám snadno může stát, že nepoužitelná jsou nejen nejnovější data, ale také všechny záložní kopie.

5.2.4 Systém utajení

Každý virus se pochopitelně snaží zůstat co nejdéle „neviditelný“. Tvůrce viru samozřejmě také chce, aby ani po odhalení nebylo lehké činnost viru pochopit a tak se proti němu napříště účinně bránit.

Naprosto nejzákladnějším (a přesto kupodivu u některých virů nedodrženým) způsobem utajení je ochrana před jakoukoli chybou zápisu – virus, který by se například pokoušel napadnout program na disketě, chráněné proti zápisu, a vyvolal tak na obrazovku patřičné systémové hlášení by byl asi brzy odhalen. Virus proto musí zjistit, není-li soubor, který chce napadnout, označen jako read-only, a případně toto označení

zrušit. Podobně musí virus umět korektně reagovat na takové případy, jako je plná disketa nebo disketa chráněná proti zápisu.

Velmi rozšířeným způsobem utajení u link virů je již zmíněná nedestruktivita, kdy napadený program pracuje stejně, jako kdyby napaden nebyl, jen se přitom „přiživí“ virus. Vyšším stupněm utajení u link virů pak je zachovávání délky napadeného programu, případně zachovávání různých pomocných příznaků. Velká většina link virů může před napadením také zjistit, jestli je daný program dosd zdráv. Je to proto, poněvadž několikanásobné napadení snižuje efektivitu dalšího množení viru a zvyšuje riziko odhalení viru.

Další viry využívají tzv. skrýše, které se nacházejí uvnitř systému. Klasickou metodou je uložení virů na disk, který je označen jako vadný. Tato činnost může být doprovázena dělením viru. Důsledkem je obrovské množství viru a tato metoda znesnadňuje analýzu nalezeného viru. [9]

5.2.5 Aktivní ochrana

Některé viry se mohou bránit i aktivně. Viru se sice můžeme zbavit, ale protože jsme neměli šanci jej analyzovat, zůstáváme proti němu i nadále bezbranní. [1]

5.3 Nejběžnější typy počítačových virů

5.3.1 Boot vir

Boot vir byl historicky první typ PC viru (Brain, 1986), který byl už v roce 1987 následovaný velmi rozšířeným virem Stoned [4]. Některé viry tohoto typu zaznamenaly vlivem zabudovaní destrukční akce poměrně velkou popularitu – vzpomeňme například vir Michelangelo nebo J&M. Na svůj přenos využívá boot sektor (případně i několik dalších sektorů) diskety zasunuté v mechanice A:, kde nahrazuje původní boot sektor

(bez ohledu na to, zda šlo o bootovatelnou disketu nebo ne). Kód viru po svojí aktivaci (nabootování ze zavirované diskety ponechané úmyslně nebo ze zapomnětlivosti v mechanice) obvykle přenese svoje tělo do Boot sektoru logického disku C: nebo častěji Master Boot [6] sektoru pevného disku(případně i několik dalších sektorů). Při nejbližším bootu z pevného disku se tedy virus spouští po BIOSu jako první (ještě před samotným operačním systémem) a záleží jen na typu viru, jak této skutečnosti využije. Obvykle se stává vir paměťově rezidentním a od tohoto momentu infikuje všechny proti zápisu nechráněné diskety zasunuté do počítače.

Za připomenutí stojí, že samotným zasunutím zavirované diskety do mechaniky A: nedochází k zavirování počítače, musí se z ní nabootovat. Dnes je tento druh virů vzhledem ke snižujícímu významu disket, na ústupu. [9]

5.3.2 Souborový vir

Do příchodu makrovirů to byl nejběžnější typ virů, který na svojí replikaci využívá tělo jiného programu. Prvním experimentálním PC virem tohoto typu byl Burger [4,9] pocházející z roku 1986, prvním virem tohoto typu v terénu byl virus Lehigh (1987) následovaný viry Jerusalem, Vienna, Cascade a dalšími. Vir se nejčastěji připojuje na konec těla hostitelského programu , čímž způsobuje jeho prodloužení. Existují ale viry, které neprodlužují hostitelský soubor, což dělají tak, že začátek nakaženého programu jednoduše přepíší (čímž ho zničí) nebo využívají díry v kódu programu, které zaplní svým kódem (tak funguje např. vir CIH, napadající 32bitové Windows EXE soubory). Po spuštění nakaženého souboru se vytvoří nejdříve kód viru, který buď uskuteční přímou akci (infikování dalších souborů podle vhodné strategie), ale častěji se virus stane paměťově rezidentním a následně infikuje další spustitelné soubory (nejčastěji při jejich spuštění, ale i při kopírování, prohlížení, komprimaci a jiné manipulaci s nimi). V závislosti na splnění určité podmínky (čas, datum, počet spuštění) přitom může vir strategii svého šíření obměňovat, případně vykonávat i jinou (související se samotnou replikací), např. destrukční akci. Po vykonání celého kódu viru se zabezpečí aktivace samotného hostitelského programu. Samotným kopírováním, prohlížením či jinou manipulací s nakaženým souborem nedochází k zavirování

počítače – na to je potřeba zavirovaný program spustit.

5.3.3 Makrovir

Makrovir je dnes jednoznačně nejrozšířenějším typem viru. První experimentální vir tohoto typu vznikl v roce 1994 (makrovir DMV) [6,9] a v terénu se makrovir poprvé objevil v roce 1995 (Concept). Jde o viry, jejichž činnost je řízená makrojazykem příslušné aplikace, přičemž jsou v tomto smyslu vázané na konkrétní formát dokumentu – makrojazyk Word Basic a dřívější verze MS Word, respektive dnes nejčastěji Visual Basic ve spojení s novějšími verzemi MS Word, MS Excel, MS Access, MS Power Point, MS Project, ale už i CorelDraw a dalšími aplikacemi. V tomto smyslu jsou nezávislé na samotném operačním systému počítače (Win9x, WinNT/2000 i MacOS) nebo na jeho hardwarové platformě (Intel, Alpha a MAC). Vzhledem na jednotný typ makrojazyka existují i viry, které napadají dokumenty dvou i tří různých aplikací ze stejného kancelářského balíku (např. MS Word, MS Excel a MS Power Point z balíku Office 97).

Standardní způsob šíření makroviru spočívá v následujícím postupu – po načtení zavirovaného dokumentu příslušná aplikace interpretuje makra viru, která při různých doprovodných akcích zabezpečí napadnutí globální šablony. Zavirovaná makra šablony se potom vkládají do dalších otevíraných dokumentů a tím je infiltrují. Je třeba zdůraznit ještě jednou, že makrovir se aktivuje již samotným prohlédnutím dokumentu v příslušném editoru (který má používání maker povolené), což je zřejmý rozdíl proti souborovým virům. K aktivaci makrovirů však nedochází při kopírování nebo jiné manipulaci se zavirovanými dokumenty.

Z výše jmenovaných tří nejběžněji se vyskytujících druhů virů se makroviry nejjednodušeji programují (rozdíl v náročnosti zvládnutí programovacího jazyka Word Basic nebo Visual Basic a assembleru je značný) a navíc se také nejsnadněji šíří vzhledem na to, že výměna dokumentů mezi uživateli je mnohem častější jak výměna spustitelných souborů. Když k tomu přidaly nové možnosti šíření kanálem elektronické služby (e-mailem), nedalo se v budoucnosti v tomto směru očekávat nic pozitivního. [1]

5.4 Škody způsobované viry

Klasifikace škod způsobovaných viry podle [11] je následující:

Škody, které způsobí viry, můžeme rozdělit do dvou kategorií, a to na škody přímé a nepřímé.

Přímé škody jsou na pohled viditelnější a řadíme mezi ně např. náklady na odstranění viru, náklady na kontrolu napadených dat či na novou instalaci softwaru, náklady na znovuvytvoření ztracených dat. Dále sem můžeme zařadit i poškození zdraví v důsledku používání poškozeného programu.

Nepřímé škody si uživatel mnohdy neuvědomí, protože se měří v celosvětovém měřítku a některé jsou i složitěji vyčíslitelné. Patří sem náklady na nákup a provoz antivirového software, dále např. školení. Můžeme sem zařadit i náklady na ztráty a z omezení činnosti.

5.4.1 Solomonova klasifikace škod způsobených viry

Solomonova klasifikace škod způsobovaných viry podle [8] je následující:

Tato klasifikace vychází z ničivých částí viru a sleduj se zde doba od přítomnosti viru v systému až do jeho odstranění.

Triviální – čas, který potřebujeme k odstranění viru. Většinou se jedná o minuty a vir nemá destrukční část a nepřepisuje.

Malé – dochází k obnovení všech záložních kopií, čili k reinstalace programů. Jedná se o desítky minut.

Střední – v tomto stádiu dochází ke ztrátě práce i za půl dne. Data se musí obnovit ze záloh.

Velké – dochází k postupnému ničení dat a virus je objeven až za několik dní. Ztracená data za několik dní.

Kruté – virus je objeven s velkým zpožděním a dochází k velkému ničení dat.

5.5 Antivirové programy

Při koupi antivirového programu uživatele ovlivní různé parametry - nízká cena, dostupnost na trhu, spolehlivost dodavatele, cena a frekvence aktualizace,lokalizace produktu (jazyk). Při testování a recenzích antivirových programů by tyto parametry měly být porovnávány společně s provozními parametry.

5.5.1 Principy činnosti antivirových programů

5.5.1.1 DETEKCE

Detekce virů [12] je základní funkce antivirových programů. Antivirové programy díky tomu mohou odhalit vstup virů do systému , objevit uložené viry, aktivované viry a funkční projevy viru.

Vstupující viry jsou detekovány na základě porovnávání signatur s kódem viru, analýzou kódu spustitelného programu (heuristická analýza, podpora porovnávání řetězců).

Uložené viry jsou detekovány na základě porovnávání části řetězce kódu viru, analýzou kódu spustitelného programu , zjišťování přítomnosti změn spustitelných souborů.

Aktivované viry jsou instalovány v paměti , kde lze vyhledat jejich kód pomocí signatur, analyzovat způsob instalace do paměti.

Funkční projevy virů souvisí s jejich replikací a destrukční činností. AV může

blokovat provádění neobvyklých příkazů – formátování pevného disku, analýzu souboru pro napadení, nevyžádaný přístup na disk apod.

5.5.1.2 PREVENCE

Prevence [12] úzce souvisí s detekcí virů (včasná detekce virů je její součástí). Do prevence však patří další úkony – autorizace přístupu k počítači, ochrana proti bootování z neautorizované diskety, ochrana proti zápisu na disk, zálohování systémových oblastí disku, možnost podrobného prohlížení všech oblastí disku uživatelem apod.

5.5.1.3 ODSTRANĚNÍ ŠKOD

Při dobrém antivirovém programu by se odstraňování škod vůbec nemělo dít. Existují však uživatelé, kteří odhalí přítomnost viru ve svém počítači až po zjištění škod - ztráta důležitých dat. K obnově napadených souborů slouží informace o známých virech , dodatečné informace uložené o každém souboru, heuristické čištění. [12]

5.5.2 Nejběžnější typy antivirových programů

5.5.2.1 ESET NOD 32 ANTIVIRUS

ESET NOD 32 Antivirus [13] představuje světovou špičku antivirových programů . Obsahuje účinnou heuristickou technologii, schopnost odhalit nové, dosud neznámé, viry. Je nabízen pro mnoho různých operačních systémů. Stal se držitelem významných ocenění pro svoji vyjímečnou detekci, rychlost a nízkou spotřebu systémových zdrojů. Je k dostání od 1 999 Kč s licencí na jeden rok, zpoplatněna je i verze pro domácí využití.

5.5.2.2 AVG TECHNOLOGIES

Již řadu let má AVG [14] přední postavení v poskytování antivirové ochrany. Důkazem je 80 miliónů uživatelů po celém světě. Je k dostání od 720 Kč s licencí na jeden rok pro komerční účely, pro domácí využití je k dispozici zdarma.

5.5.2.3 MCAFEE

Produkty společnosti McAfee [15] jsou nabízeny jak pro domácí tak pro komerční využití a nabízejí dlouhodobě výbornou kvalitu a vysokou úspěšnost. Společnost McAfee patří již řadu let mezi světovou špičku mezi producenty bezpečnostních produktů, které jsou kladně hodnoceny nejen odborníky, ale i širokou veřejností. K dostání je od 1 199 Kč s licencí na jeden rok, zpoplatněna je i verze pro domácí využití.

5.5.2.4 KASPERSKY

Kaspersky vyvíjí, produkuje a distribuuje bezpečnostní řešení chránící zákazníky před IT hrozbami a minimalizuje bezpečnostní rizika ve velkých firmách. Dle nezávislých expertů má Kaspersky [16] celosvětově nejrychlejší reakce proti novým hrozbám. Je k dostání od 705 Kč s licencí na jeden rok.

5.5.2.5 AVAST ANTIVIRUS

avast! [17] s vyspělou vícevrstvou rezidentní ochranou nabízí vysoký stupeň zabezpečení před všemi typy nebezpečných kódů. Je založen na pokročilé testovací technologii ALWIL Software, nabízené již od roku 1988. Jeho kvalitu dokazuje již 19 ocenění za 100% úspěšnost detekce v časopisu VirusBulletin. Pro domácí využití je poskytován zdarma, pro komerční účely je k dostání od 899 Kč s licencí na jeden rok.

6. Výběr a hodnocení konkrétního typu antiviru

6.1 ESET Smart Security 4

Tento antivirový program je volně dostupný na internetové adrese www.eset.cz. Registrace není nutná. Program byl cíleně navržen pro méně než 5 počítačů, pro studenty, domácnosti a živnostníky. Pro větší počet počítačů je určen ESET NOD32 Antivirus 4. Mimo jiné obsahuje i antispyware, firewall a antispam, který chrání počítač před hackery, nevyžádanou poštou a útoky z internetu. Není tedy nutné tyto komponenty zvlášť dokupovat. Výborná je schopnost detekce zcela nových virů. Antispyware, firewall i antispam je možné vypnout. ESET Smart Security 4 je zpoplatněný antivirový program jak pro komerční, tak i pro domácí využití. Výhodou je, že je poskytován ve zkušební verzi na 30 dnů od instalace, poté je nutné zakoupit licenci, nebo program odinstalovat. Licenci na 1 rok lze pořídit již od 1499 Kč včetně 20% DPH, prodloužení licence pak stojí 1049 Kč včetně 20% DPH. Velké pozitivum je možnost poskytnutí slev. Studentům vlastnícím kartu ISIC je program poskytován s 50% slevou na jeden počítač s licencí na jeden rok. Slevy mohou také uplatnit subjekty veřejné správy – 20%, 50% pro zdravotnictví, 50% pro školství, 50% pro držitele průkazu ZTP, ZTP/P, TP a poživatele plného invalidního důchodu a 50% pro neziskové organizace.

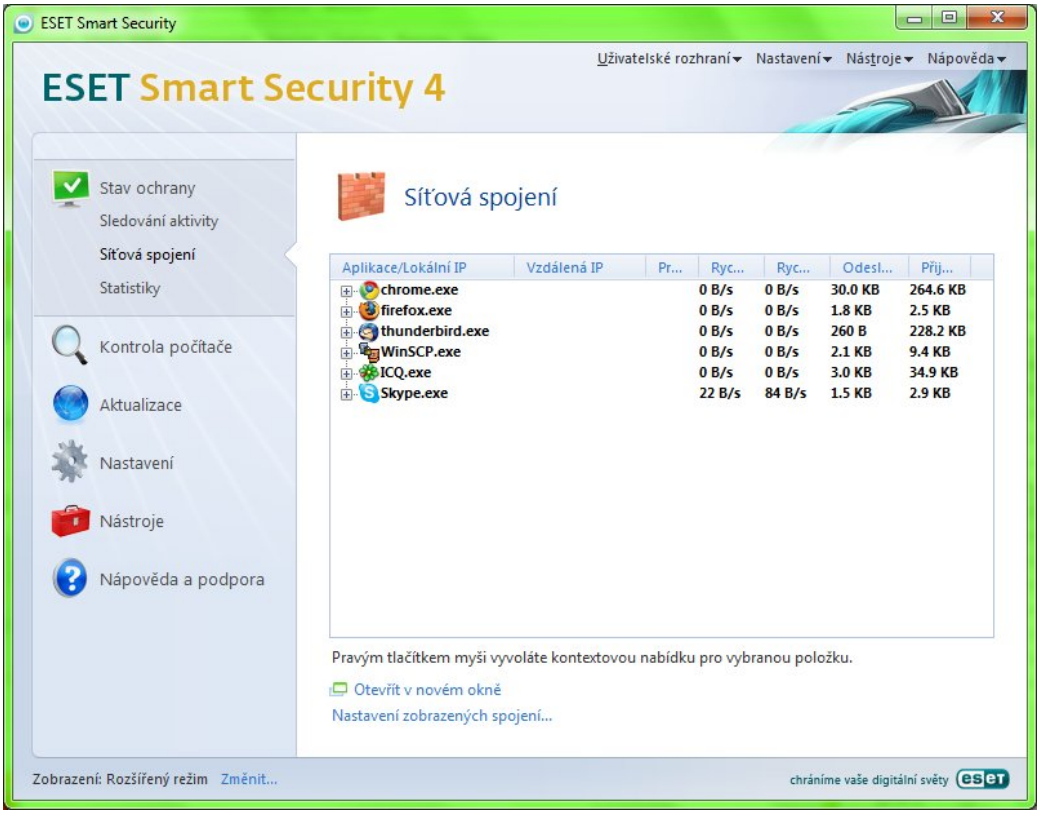
Celý program je k dispozici v šestnácti jazycích, mimo jiné disponuje i češtinou. Pro stažení produktu musí být na disku 34MB volného místa, pro instalaci pak 130 MB. Při instalaci jsou nabídnuty možnosti od začátečníka až po pokročilého, tudíž je instalace velmi jednoduchá.

Podporovanými procesory jsou Intel® nebo AMD® x86 a x64 a operačními systémy Microsoft® Windows® 7, Microsoft® Windows® 2000, Microsoft® Windows® XP a Microsoft® Windows Vista®.

ESET Smart Security sám rozpozná, jestli běží na stolním počítači nebo na notebooku a upozorní uživatele před stažením většího updatu, kvůli úspoře baterie.

K aktualizacím dochází automaticky. Jsou k dispozici i několikrát denně a probíhají na pozadí počítače.

V případě nespokojenosti má uživatel právo od smlouvy odstoupit ve lhůtě 14 dnů od převzetí.



[18]

6.2 avast!Home Antivirus 4.8

avast!Home Edition 4.8 představuje nejdostupnější verzi antivirové ochrany pro nekomerční využití, protože je poskytován zdarma. Je dostupný v několika jazycích a uživatel si může vybrat jazykovou verzi podle vlastních preferencí. Velikost České

verze činí 40MB, cizojazyčné 44MB. Nechybí spyware. Umí detekovat známé viry, zejména trojské koně. Bohužel neobsahuje firewall ani antispam.

Pro stažení je potřeba 100 MB volného místa na disku. Kompatibilní je s procesorem Pentium 3 a operačním systémem Microsoft 2000, XP a Vista. Stažení a uložení programu netrvá dlouho. Instalace sestává z překlikávání několikrát po sobě „Další“. Instalace zabere maximálně 10 minut (bez restartování počítače) a je jednoduchá. Zvládl by ji každý, kdo již někdy něco instaloval. Uživatel má již nastavené parametry na optimum, což ocení zejména ti, kteří by si v nastavení jednotlivých komponent nevěděli rady.

Program avast!Home Edition 4.8 je sice zdarma, nicméně uživatelé si ho zaregistrovat musí. Registrační formulář je k dispozici na internetové adrese http://www.avast.com/cze/home-registration.php . Po vyplnění daného formuláře bude odeslán licenční klíč, který je nutné vložit do požadovaného okna. Registrace není nutná ihned a program lze vyzkoušet v Demo verzi na 60 dní. Další registrace je možná kdykoliv během 60 dnů. Pokud si uživatel program avast! nezaregistrujete ani během 60 dnů, na obrazovce se zobrazí varovná zpráva o vypršení licence.

Licenční klíč uživatel obdrží po vyplnění formuláře na webových stránkách firmy avast!. Na svých stránkách uvádí firma obdržení klíče do 24 hodin. Z vlastních zkušenostní mohu uvést, že jsem klíč obdržela vzápětí po odeslání formuláře. Po vložení klíče bude program aktivován na 12 měsíců a po vypršení lhůty opět požádá o vložení nového licenčního klíče.

Avast! poskytuje dva typy ochrany. Tou první je Rezidentní ochrana, která probíhá neustále a aktivuje se po instalaci programu. Tou druhou je Test na vyžádání. Při tomto testu se volí oblast, která bude sloužit k testování.

Rezidentní ochranu je možné pozastavit nebo úplně ukončit. Po znovuzapnutí počítače bude opět aktivována, což zabraňuje jejímu nechtěnému vypnutí. Rezidentní ochrana sestává z několika podsložek, např. Instant Messaging sloužící např. k ochraně programů jako ICQ či Skype, dále Internet Mail, který chrání email, Síťový štít blokuje útoky internetových červů. Dalšími složkami jsou ještě Outlook/Exchange, P2P štít, Script blocking, Standartní štít a Webový štít.

Při testu na vyžádání se před spuštěním testu musí vybrat oblast, která bude testována. Může se provést test lokálních pevných disků, všech médií nebo zvolených

adresářů. Lze také nastavit citlivost testu. Volbou testu lokálních pevných disků se otestují jednoduše všechny soubory v počítači. V testu lokálních pevných disků se navolí možnost Diskety nebo CD/DVD , případně obojí. Zvolením možnosti testu zvolených adresářů se navolí přímo adresář (složka), která se bude testovat.

Lze nastavit také úroveň testování. Na výběr je rychlý test, standardní test a důkladný test. Rychlý test testuje ty soubory na základě jejich přípony, tzn. , že neodhalí v souboru ty viry, které pro daný soubor nejsou typické. Důkladný test testuje všechny soubory na všechny viry a trvá nejdéle. Při testu je lepší dialogové okno s testem zavřít, protože by mohl výrazně zpomalovat činnost počítače. Pokračovat v práci je ale nadále možné. Pokud nebyl nalezen virus, po skončení testu se zobrazí okno s informacemi o počtu testovaných souborů a délce testu.

[19]

V avastu! je možnost zvolit z několika možností aktualizace. Automatické aktualizace lze nastavit po různých intervalech. Dále je možné provádět aktualizace ručně nebo si nastavit, aby docházelo k upozornění na nejnovější dostupné verze programu. O aktualizaci programu pravidelně upozorňuje modré okénko, které se

oběvuje v pravém dolním rohu a obsahuje informaci o aktualizované verzi a délce času již proběhlé aktualizace.

Aktualizace probíhají několikrát do týdne a uživatel ani nepozná, že na nich počítač právě pracuje. Na webu jsou k dispozici při epidemii nové aktualizace i několikrát denně. Jednotlivá informační okna, která vyskakují ať už při instalaci nebo při nastavení jednotlivých komponent jsou jednoduchá a přehledná. Nabízí uživateli jasné postupy a řešení. Oproti nejnovější verzi Avast Free Antivirus 5 nejsou však dialogová okna příliš atraktivní. Hlavní změnou jsou barvy a velikost dialogových oken. Z původních modrošedých oken se stala oranžovočerná a jejich velikost se značně zvětšila.

6.3 AVG Anti-Virus Free Edition 9.0

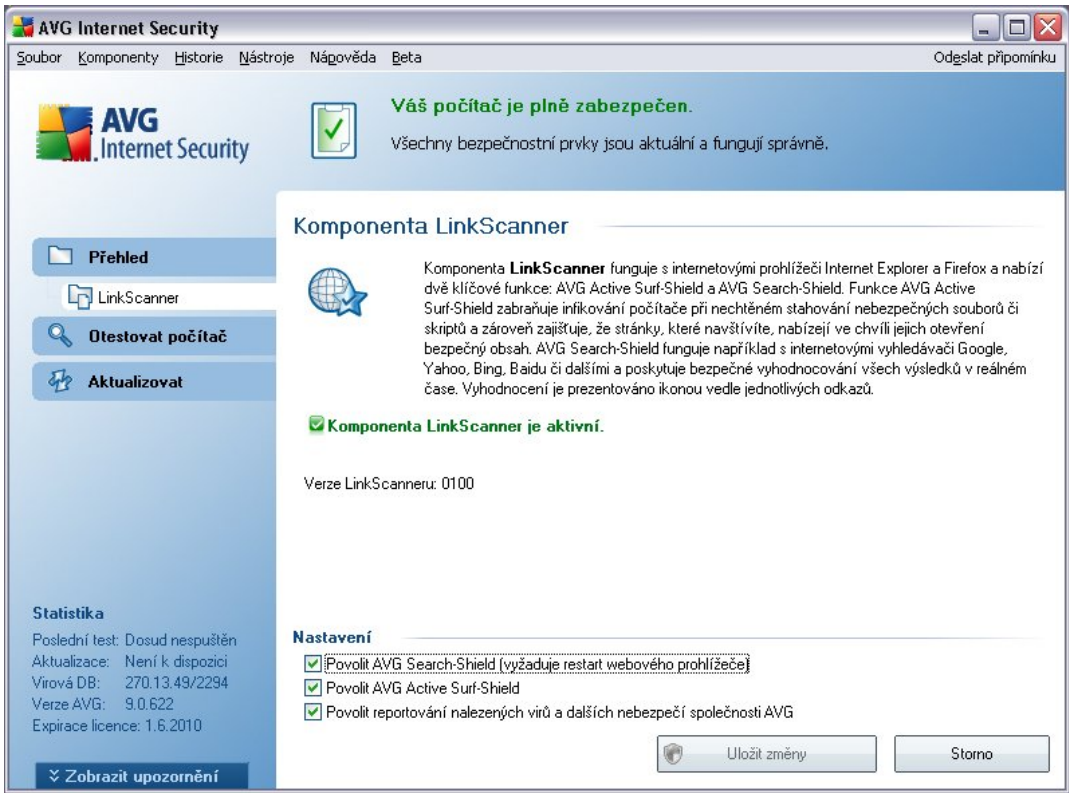
AVG Antivirus je dalším z antivirů, které jsou k dispozici zdarma pro domácí využití na webové adrese www.avg.com. Pro používání programu je nutná registrace. Uživatel obdrží prodejní/licenční číslo. AVG Antivirus obsahuje spyware, ale jinak poskytuje jen základní ochranu. Schopnost detekce se vztahuje pouze na známé viry. Chybí firewall, antispam a webový štít, takže počítač není chráněn před útoky hackerů, nevyžádanou poštou a před krádeží osobních údajů. To se jeví jako veliký problém např. při vstupu do elektronického bankovnictví, kdy je bezpečnost velice důležitá. K tomu aby ochrana počítače byla dostatečná je nutné výše vyjmenované složky k programu doplnit. Pro komerční účely jsou k dispozici AVG Anti-virus a AVG Internet Security, které již disponují větší ochranou. Pro vyzkoušení programu je k dispozici třicetidenní zkušební verze.

AVG je původně český antivirový program, takže je dostupný i v češtině, která je jedním z dvaadvaceti podporovaných jazykových verzí programu. Pro instalaci je nutné mít na disku 512 MB volného místa. Kompatibilní je s operačními systémy MS Windows XP, MS Windows Vista a MS Windows 7. Podporovaným procesorem je Intel Pentium, 1,8 GHz. Po instalaci je nutné vložit licenční klíč.

K aktualizacím dochází automaticky a vše se děje na pozadí monitoru. Uživatel je informován o stavu aktualizací i výsledcích testů. Ani zde nechybí možnost testu na vyžádání.

Svým zákazníkům program nabízí možnost předčasného prodloužení licence a tím získání slevy na nákup další licence. Je poskytována sleva pro školství a zdravotnictví. V současné době mohou zákazníci při nákupu dvou licencí získat třetí zdarma.

Program je doručen buď na zadanou emailovou nebo dodací adresu. Při dodání fyzického balení je k ceně účtován manipulační poplatek, tudíž je výhodnější si program stáhnout z internetu.



[20]

6.4 McAfee Antivirus Plus 2010

McAfee Antivirus Plus je nejzákladnější způsob ochrany rodiny McAfee. Obsahuje spyware i malware, firewall a schopnost detekce je na výborné úrovni, bohužel chybí antispam, tudíž se uživatel nevyhne přeplnění schránky nevyžádanou poštou. Podporuje následující operační systémy: Windows XP, Vista a 7 a Procesor I GHz a vyšší. Na disku musí být alespoň 200 MB volného místa a 256 MB paměti RAM.

McAfee Antivirus Plus je zpoplatněným antivirem a k dostání je za 1 199 Kč včetně DPH. Pro používání programu si uživatel musí založit účet na stránce www.home.mcafee.com. Z daného účtu si poté může stáhnout požadovaný program. Na uvedené stránce je možno program rovnou stáhnout nebo zvolit fyzickou dodávku. Dále je možné objednat roční nebo měsíční předplatné. K dispozici je v české verzi. Uživatel může využít bezplatnou zkušební verzi po dobu třiceti dnů. Aktualizace jsou k dispozici téměř každý den a počítač nezpomalují.

Zákazník má možnost třicetidenní záruky vrácení peněz, pokud s produktem není spokojen.

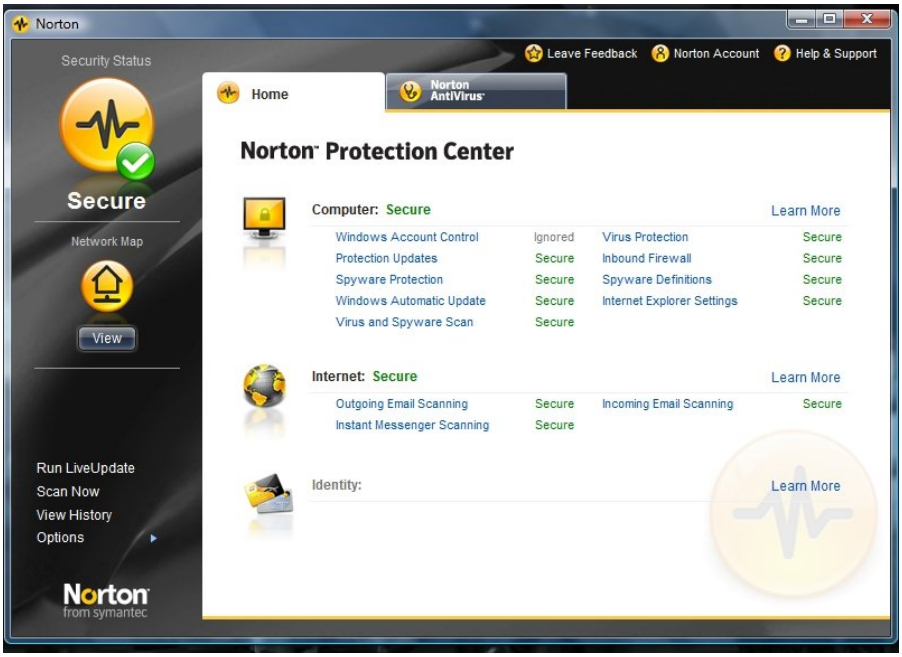
[21]

6.5 Norton Antivirus

Norton Antivirus společnosti Symantec jako jediný ze jmenovaných není možné stáhnout přímo z internetu, ale lze objednat pouze prostřednictvím České pošty. K jeho spuštění je nutná registrace. Je kompatibilní s operačními systémy Windows XP, Vista a s procesorem 300 MHz nebo výkonnější. Vyžaduje min 200MB místa na volném disku a 256 MB RAM. Pořídit ho lze za 1 164 Kč včetně DPH, prodloužení licence za 900 Kč. Součástí balíčku je ochrana před spyware a antirootkit a chrání např. před programy zaznamenávající klávesové úhozy. Vyniká schopností detekce červů. Chybí antispam a firewall. Program neumí blokovat přístup hackerů do počítače. Dostupný je také v české verzi. Zkušební doba antiviru je 15 dní.

Pokud zákazníkovi nevyhovuje, má možnost produkt do 14 dnů od nákupu bez

udání důvodu vrátit.



[22]

6.6 Výsledky

Tabulka č. 1.

Antivir → Vlastnost ↓	**ESET Smart Security 4**	**McAfee Antivirus Plus 2010**	**Norton Antivirus**	**Avast! Home Antivirus 4.8**	**AVG Anti-Virus**
cena	1 499 Kč	1 199 Kč	1 164 Kč	zdarma	zdarma
slevy	ano	ne	ne	-	-
velikost	130 MB	200 MB	200 MB	100 MB	512 MB
čeština	ano	ano	ano	ano	ano
antispam	ano	ne	ne	ne	ne
firewall	ano	ano	ne	ne	ne
antispyware	ano	ano	ano	ano	ano
automatické aktualizace	ano	ano	ano	ano	ano
stažení z internetu	ano	ano	ne	ano	ano
zkušební verze	30 dní	30 dní	15 dní	60 dní	30 dní

Tabulka č. 2. Metoda výpočtu pomocí váženého průměru

Antivir → ***Vlastnost ↓***	**Váha známky**	**ZNÁMKA (1→ 5)**				
		ESET Smart Security 4	**McAfee Antivirus Plus 2010**	**Norton Antivirus**	**Avast! Home Antivirus 4.8**	**AVG Anti-Virus**
Schopnost detekce	30%	3	5	4	2	1
Zabezpečení ***(firewall,antispam, antispyware)***	30%	5	3	2	2	2
Čeština	20%	5	5	5	5	5
Cena	10%	3	3	4	5	5
Velikost	10%	3	2	2	4	1
CELKEM	100%	**4 (80%)**	**3,9 (78%)**	**3,4 (68%)**	**3,1 (62%)**	**2,5 (50%)**

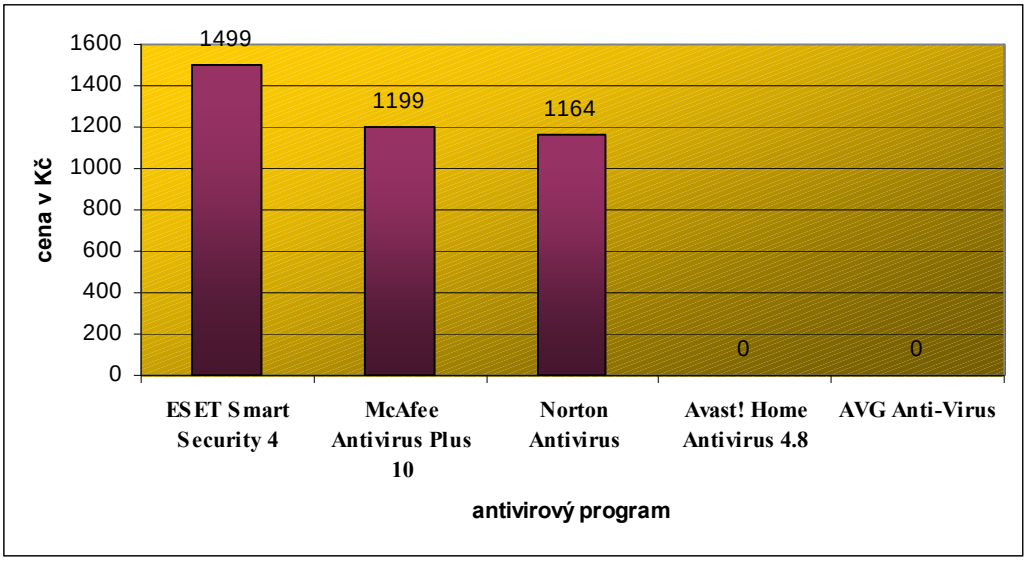
Pro kategorii Schopnost detekce a Zabezpečení byla vybrány váhy 30%, protože jsou to nejdůležitější vlastnosti dobrého antivirového programu. Čeština, vzhledem k stále se zmenšující jazykové bariéře, tvoří 20% a zbývající Ceně a Velikosti byly přiřazeny váhy v hodnotě 10%, protože by neměly být hlavním kritériem pro výběr antiviru (důležitá je především ochrana dat).

K určení bodů za kategorii Schopnost detekce posloužily zahraniční srovnávací testy antivirů [http://www.av-comparatives.org]. Konkrétně se jedná o Retrospective/Proactive test, který se zaměřuje na výkonnost metod detekce. Test probíhal následovně: Byly nainstalovány a zaktualizovány jednotlivé antiviry a byly zmraženy (tzn. dále neprobíhala aktualizace). V následujících třech měsících byla zachycována nová havěť, která by měla být pro antiviry neznámá. V závislosti na kvalitě detekce a nově získané havěti se vypočítá úspěšnost detekce. Výsledky byly

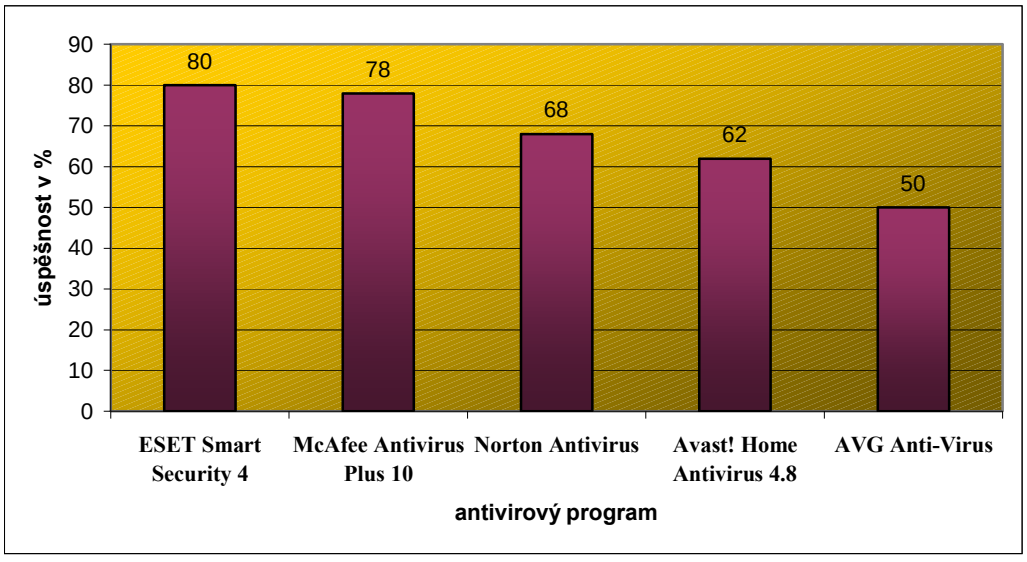
následující: McAfee 98,9%, Norton 98,6%, ESET 97,2%, avast! 97,3% a AVG 94,2%. Na základě těch výsledků byly přiřazeny body do výše uvedené tabulky.

Za zabezpečení by bylo uděleno nejvyšší ohodnocení, pokud daný antivir obsahuje všechny tři výše uvedené složky. McAfee Anvitivur Plus získal tři body, protože chybí antispam. Zbývající Norton, avast! a AVG získali po dvou bodech z důvodu nepřítomnosti firewallu a antispamu. Všechny programy jsou dostupné v češtině, tudíž získali pět bodů. Pět bodů za cenu bylo uděleno, pokud je antivir poskytován zdarma. Norton Antivirus získal čtyři body, protože je nejlevnější ze tří uvedených programů. ESET Smart Security a McAfee Antivirus Plus dostaly po třech bodech. Za velikost by byl udělen plný počet bodů, pokud by byla menší než 100 MB, proto avast! získal čtyři body, ESET Smart Security tři body, McAfee a Norton obdržely dva body a zbývající AVG získal jeden bod.

Graf č. 1: Cena jednotlivých antivirových programů



Graf č.2: Úspěšnost jednotlivých antivirových programů



7. Doporučení uživatelům

Ať už si uživatel vybere placenou verzi programu, nebo dá přednost té bezplatné, samotná přítomnost antiviru v počítači mu bezpečnost nezaručí. Zde je uvedeno několik tipů pro uživatele

Důležité je udržovat antivirový program stále aktualizovaný, protože i ten sebelepší antivir je k ničemu, pokud je v zastaralé verzi. Každý den vznikají nové kódy, a proto jsou aktualizace k dispozici ke stažení i několikrát denně. Dále je dobré vědět, co všechno antivir umí a neumí. Leckteré programy mají v nastavení možnost jednotlivé komponenty vypnout, což někdy nemusí být na škodu, protože někdy není nutné denně kontrolovat něco, co už bylo dávno zkontrolované nebo napsané. Tato činnost může výrazně zpomalit počítač.

Co se týče bezpečnosti na webu, nevyplatí se otevírání emailových příloh, o kterých uživatel nic neví. Takové emaily prozradí např. anglický text. V dnešní době pochází tři čtvrtiny útoků prostřednictvím elektronické pošty. Dále platí neklikat na internetu na vše, co se dostane pod kurzor myši, jako např. stahování mp3 souborů ze stránek typu „mp3 zdarma“. Vyplatí se také vyhnout tzv. řetězovým emailům.

Není na škodu mít přehled o tom, kolik lidí se u jednoho počítače střídá. Platí zásada čím více lidí u počítače, tím větší riziko hrozí. Dále je důležité před použitím CD ho otestovat, než se potom trápit nad zavirovaným počítačem.

Dalším pravidlem je opatrně nakládat s každým novým souborem. Dnes neplatí, že soubor stažený od důvěryhodného zdroje, je neškodný. I instalační cédéčko může obsahovat vir. Vyplatí se kombinovat více způsobů antivirové ochrany, jako např. firewall, antispam či antispyware. Leckterých antivirů jsou tyto balíčky již součástí, jinde se musí zvlášť dokoupit. Jako prevence poslouží zálohování. Pravidelné zálohování umožňuje minimalizaci škod způsobených napadením virem.

V případě napadení virem není třeba podléhat panice a v případě, že si uživatel neví rady, je tu ještě možnost svěřit PC do rukou odborníka. Takováto investice je mnohdy menší než ztracená data.

8. Závěr

V současné době existuje několik způsobů, jak napadnout bezpečí počítače. Ať už se jedná o červy či trojské koně, vždy se dovnitř počítače dostanou přes jeho nedostatečnou ochranu. S vývojem takovýchto hrozeb přicházely na trh antivirové firmy, které se zabývají virovou problematikou. Na trhu jsou k dostání antivirové programy jak pro domácí, tak pro komerční účely. Nabízejí širokou škálu služeb. Daný antivirový program je možné stáhnout přímo z internetu, popřípadě koupit ve specializovaných obchodech, nebo si ho nechat doručit až domů.

Z předložené bakalářské práce vyplývá, že všechny hodnocené antivirové programy jsou dostupné i v českém jazyce. Jejich součástí je i spyware a mají možnost automatické aktualizace. Úspěšnost jednotlivých antivirových programů je znázorněna v grafu č.2.

Nejlepšího hodnocení dosáhl ESET Smart Security 4 s 80% a s výbavou antispamu, firewallu a spyware. Nevýhodou je cena, kterou je možné snížit, protože vybraným subjektům je nabízen se slevou, což ocení zejména studenti.

Na druhém místě skončil McAfee Antivirus (78%) Plus 2010, který je zpoplatněn konečnou cenou 1 199 Kč bez možnosti využití slevy. Na disku zaujímá 200 MB. Ve výbavě chybí antispam a uživatel má možnost využít bezplatnou zkušení verzi na třicet dní.

Třetí místo zaujímá Norton Antivirus s 68%, který je ze tří zpoplatněných antivirů ten nejlevnější. Je k dispozici i ve zkušební patnáctidenní lhůtě. Na disku zabere 200 MB a chybí mu firewall a antispam.

Na čtvrtém místě se umístil avas!Home Antivirus 4.8 s 62%, který je k dispozici zdarma a na disku zabírá nejméně místa (100 MB). Nulová cena je ovšem vykoupena nepřítomností antispamu a firewallu.

Na pátém místě se umístil bezplatný AVG Antivirus, který získal 50%. AVG Antivirus na disku zabírá nejvíce místa a to 512 MB a do výbavy mu schází firewall a antispam.

Z výsledků dále vyplývá, že nejlepším placeným antivirovým programem se stal ESET Smart Security 4 a z neplacených antivirů se na lepší pozici umístil avast!Home Antivirus. Cena jednotlivých antivirů je znázorněna v grafu č.1.

9. Literatura

[1] ČADA, Ondřej. *Ochrana proti počítačovým virům*. Praha : Plus, 1991. 155 s. ISBN 80-85297-15-9.

[2] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti* [online]. Brno : CP Books, 2005. 52 s. ISBN 80-251-0574-1.

[3] HÁK, Igor; ZELENKA, Josef. *Ochrana dat : Škodlivý software*. Vyd. 1. Hradec Králové : Gaudeamus, 2005. 211 s. ISBN 80-7041-594-0.

[4] ODEHNAL, Petr; ZAHRADNÍČEK, Petr. *Praktická sebeobrana proti virům*. Vyd. 1. Halíčkův Brod : Grada, 1996. 115 s. ISBN 80-7169-363-4.

[5] KOCMAN, Rostislav; LOHNINSKÝ, Jakub. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd. 1. Brno : CP Books, 2005. 148 s. ISBN 80-251-0793-0.

[6] HEINIGE, Karel. *Viry a počítače*. Brno : Mobil Media, 2001. 80 s. ISBN 80-86593-02-9.

[7] BITTO, Ondřej. *Jak zabezpečit domácí a malou síť Windows XP : účty, práva, firewally, antiviry a další nástroje* . Brno : Computer Press, 2006. 216 s. ISBN 80-251-1098-2.

[8] HÁK, Igor; ZELENKA, Josef. *Ochrana dat : škodlivý software*. Vyd. 1. Hradec Králové : Gaudeamus, 2005. Klasifikace počítačových virů podle rychlosti šíření, s. 211. ISBN 80-7041-594-0.

[9] JALŮVKA, Josef. *Moderní počítačové viry : podstata, prevence, ochrana*. 2. aktualiz. vyd. Praha : Computer Press, 2000. 223 s. ISBN 80-7226-402-8.

[10] SZOR, Peter. *Počítačové viry : analýza útoku a obrana*. Brno : Zoner press, 2006. 608 s. ISBN 80-86815-04-8.

[11] BAUDIŠ, Pavel; ZELENKA, Josef. *Antivirová ochrana*. Praha : Plus, 1996. Škody způsobované viry, s. 183. ISBN 80-251-0793-4.

[12] BAUDIŠ, Pavel; ZELENKA, Josef. *Antivirová ochrana*. Praha : Plus, 1996. 183 s. ISBN 80-85297-74-4.

[13] *ESET NOD32 Antivirus 4* [online]. Www.antivirovecentrum.cz. Dostupné z WWW: <http://www.antivirovecentrum.cz/nod32-antivirus-system.aspx>.

[14] *AVG Anti-Virus a Internet Security : Profil společnosti* [online]. - [cit. -]. Www.avg.com. Dostupné z WWW: <http://www.avg.com/cz-cs/profil-spolecnosti>.

[15] *McAfee - Internet Security Suite 2008, VirusScan Plus a SiteAdvisor, Total Protection* [online]. - [cit. 2010-03-17]. Www.antivirovecentrum.cz. Dostupné z WWW: <http://www.antivirovecentrum.cz/mcafee.aspx>.

[16] *Kaspersky Lab - O nás* [online]. - [cit. 2010-03-17]. Www.kaspersky.cz. Dostupné z WWW: <http://www.kaspersky.cz/pages/o-nas-r53>.

[17] *Avast! : O společnosti* [online]. - [cit. 2010-03-17]. Www.avast.com. Dostupné z WWW: <http://www.avast.com/cs-cz/about>.

[18] *Stopvir* [online]. - [cit. 2010-03-18]. Www.stopvir.cz. Dostupné z WWW: <http://www.stopvir.cz/_obchody/stopvir.shop5.cz/soubory/ESET_Smart_Security_4/ESET_Smart_Security_4_sitova_spojeni_screenshot.png>.

[19] *Avast!* [online]. - [cit. 2010-03-18]. Www.avast.cz. Dostupné z WWW: <http://download612.avast.com/files/manuals/user-manual-home-cze.pdf>.

[20] *AVG free* [online]. - [cit. 2010-03-18]. Www.extrawindows.cnews.cz. Dostupné z WWW: <http://extrawindows.cnews.cz/files/obrazky/2009/05May/avgfree.png>.

[21] *Virus, Spyware, Virus Scan Software | VirusScan Plus | McAfee* [online]. - [cit. 2010-03-18]. Www.home.mcafee.com. Dostupné z WWW: <http://home.mcafee.com/store/PackageDetail.aspx?pkgid=276>.

[22] *Norton-Antivirus* [online]. - [cit. 2010-03-18]. Www.sosej.cz. Dostupné z WWW: <http://www.sosej.cz/screenshots/Norton-Antivirus_15.5.0.23.jpg>.