Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Počítačové viry a antiviry

Michal Martinek

vedoucí: Ing. Marek Pícka, Ph.D.

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Akademický rok 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Martinek

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název práce: **Počítačové viry a antiviry**

Osnova bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Historie počítačových virů a jejich rozdělení
4. Prevence před viry a důvody jejich vzniku
5. Antivirové programy a jejich možnosti
6. Porovnání vybraných antivirových programů
7. Závěr
8. Seznam použitých zdrojů
9. Přílohy

Rozsah hlavní textové části: 30 - 40 stran

Doporučené zdroje:

SZOR, Peter. Počítačové viry - analýza útoku a obrana. 1.vydání. Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.

HÁK, I. - ZELENKA, J. Ochrana dat: škodlivý software. 1.vydání. Gaudeamus, 2005. 211 s. ISBN 80-7041-594-0.

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

KRÁL, Mojmír. Bezpečnost domácího počítače. 1.vydání. Grada, 2006. 336 s. ISBN 80-247-1408-6

Vedoucí bakalářské práce: **Ing. Marek Pícka, Ph.D.**

Termín odevzdání bakalářské práce: březen 2012

.....
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

.....
Děkan

V Praze dne: 13. 2. 2012

Evidováno děkanátem PEF pod č.j.: KII-099-11B

Čestné prohlášení

Tímto čestně prohlašuji, že jsem BP na téma „Počítačové viry a antiviry“ zpracovával samostatně, pouze s použitím uvedené literatury, metod a zdrojů.

V Praze, dne 29.3.2012 ……

Poděkování

Tímto bych rád poděkoval vedoucímu práce Ing. Markovi Píckovi, Ph.D. za rady a konzultace při vypracování této bakalářské práce. Dále bych chtěl poděkovat mé trpělivé rodině a přátelům, kteří mi poskytli další cenné rady vedoucí k lepší úrovni této práce.

Počítačové viry a antiviry

Souhrn

Tato bakalářská práce se zabývá hodnocením několika antivirových programů a doporučením jednoho z nich.

První část práce je zaměřena na charakteristiku škodlivých programů, jejich rozdělení a stručnou historii. V další části se práce podrobněji zaměřuje na kategorii počítačových virů. Zkoumá, proč viry vznikají a rozděluje je na několik nejběžnějších typů. Následně jsou rozebírány antivirové programy a jejich činnosti.

V poslední části práce je srovnáváno několik antivirových programů a na základě metody váženého součtu je vybrán nejvhodnější z nich.

Klíčová slova

Počítačové viry, antivirový program, malware, trojský kůň, počítačový červ

Computer viruses and antiviruses

Summary

This bachelor thesis deals with evaluation of some antivirus software and tries to recommend one of them.

The first part of the thesis is focused on description of malware, its division and brief history. The next part focuses on the computer viruses category in detail. It examines why the viruses are created and divides them into several most common types. After that the antivirus software is discussed and also its operation.

In the final part of the thesis, several types of antivirus software are compared and the best one is chosen on the basis of Weighted Sum Approach method.

Key words

Computer viruses, antivirus software, malware, trojan horse, computer worm

Obsah

1 Úvod

V dnešní době je počítač, respektive internet, součástí téměř každé domácnosti. Připojit se k internetu je nyní možné prakticky odkudkoliv, ať už je to škola, knihovna, kancelář či autobus. Každý počítač, který je připojen, je však zároveň vystaven několika hrozbám. Jednou z nich jsou počítačové viry, a proto je velmi důležité, aby byl počítač chráněn některým z antivirových programů.

Antivirové programy zajišťují uživateli alespoň základní ochranu před počítačovými viry. Na trhu můžeme nalézt celou řadu antivirových programů a každý člověk nebo firma si může vybrat podle svých požadavků. Jejich vlastnosti velmi často závisí na ceně, ale existují i takzvané free edice, které jsou v současné době velmi kvalitní a pro běžného uživatele zcela dostačující.

2 Cíl práce a metodika

2.1 Cíl práce

Prvotním cílem bakalářské práce na téma „Počítačové viry a antiviry“ je srovnání několika antivirových programů a následné doporučení jednoho z nich, který vyjde z testu nejlépe. Jedním z dalších cílů je charakterizovat škodlivý software a správně ho pojmenovat. Dále se část práce věnuje historií virů a má za cíl objasnit, proč počítačové viry vznikají a jak jsou rozděleny. V neposlední řadě je úkolem práce popsat základní činnosti antivirových programů a představit několik firem, které se na tyto produkty zaměřují. V závěru se nachází údaje o vybraných antivirových programech, které jsou srovnávány.

2.2 Metodika

Informace, které budou použity při psaní bakalářské práce, jsou získány z internetu, skript a odborné literatury, zabývající se danou tématikou. Všechny tyto zdroje budou uvedeny v seznamu použité literatury v závěru práce. Jejich pomocí bude popsána základní charakteristika a rozdělení počítačových hrozeb a principy antivirových programů.

V závěru práce budou charakterizovány a porovnávány čtyři placené antivirové programy. Bude zvoleno a definováno pět kritérií, které jsou rozhodující pro výběr vhodného antivirového programu. Následně se vypočítají užitkové hodnoty antivirových programů pomocí metody váženého součtu a sestaví se tabulky pro jejich výpočet. Nejvyšší užitková hodnota stanoví optimální antivirový program, který bude doporučen pro ochranu počítače před škodlivým kódem.

3 Počítačová havěť a další škodlivé programy

Počítačový virus definoval v roce 1983 Frederick Cohen následovně: „Počítačový virus je počítačový program, který může infikovat jiný počítačový program takovým způsobem, že do něj zkopíruje své tělo, čímž se infikovaný program stává prostředkem pro další aktivaci viru“ [1, s. 4].

Mnohá literatura nabízí celou řadu programů, které jsou označovány pod pojmem viry, ale některé z nich neodpovídají jejich definici. V následujícím textu je nazýváme malware [1, 2, 3].

3.1 Klasifikace malware

Název malware pochází z anglického MALicious softWARE. V překladu to znamená škodlivý software.

3.1.1 Klasifikace podle způsobu šíření

Klasifikovat malware je někdy velmi obtížné, jelikož mohou mít velmi podobné vlastnosti. Lze je třídit do několika skupin:

- **Červy**, které bývají označovány jako síťové viry, a které se primárně šíří pomocí sítí, anebo pomocí aplikačních programů, například e-mailem.
- **Počítačové viry**, jejichž šíření a replikace probíhá pomocí souborů a oblastí pevného disku.
- **Trojské koně**, které využívají oklamání uživatele a spolupracují s červy a viry.

Mnohdy se však tyto třídy překrývají, a tak záleží, do jaké skupiny je daný odborník zařadí [2].

3.1.2 Klasifikace podle typu škodlivé činnosti

- **Špionážní software** (spyware) se zakládá na získávání statistických údajů jako je přehled instalovaných programů nebo navštívených stránek, ale i na získávání hesel a dalších údajů.
- **Zadní vrátka** (backdoor) jsou programy, které útočníkovi umožní přístup do systému.
- **Další typy škodlivých činností** jsou páchány programy pro přesměrování připojení nebo programy pro útok na dostupnost zdrojů [4].

3.2 Počítačové viry

Asi nejčastější definice počítačového viru je, že virus je část programového kódu, který je bez vědomí uživatele šířen pomocí systémových oblastí nebo souborů a zároveň je schopen se dále rozmnožovat [4].

Jejich kopie nemusí být identické s originálem, ale obvykle mají stejné vlastnosti a mohou se dále množit. Od běžných programů se viry vyznačují škodlivou činností, jako například formátováním disku nebo mazáním určitých souborů [4].

Počítačové viry byly dlouhou dobu nejčastější nákazou počítačových systémů až do velkého rozšíření červů. Jejich vlastnosti odpovídají vlastnostem biologických virů. Jsou schopny se rozmnožovat bez cizí pomoci a to za přítomnosti hostitelů, kterými mohou být spustitelné soubory nebo systémové oblasti disku [4].

3.3 Počítačové červy

Šíření počítačových červů je zpravidla postaveno na vyhledání a zneužití bezpečnostních děr v systému a následné infekci. Jejich hlavní charakteristikou je, že se šíří pomocí sítí a na vzdáleném počítači jsou schopny se spustit bez jakékoliv intervence uživatele. Další možností jsou červy šířící se pomocí e-mailových zpráv, ale ty obvykle vyžadují pomoc koncového uživatele a jsou mnohými odborníky spíše považovány za

počítačový virus než za červa. Počítačové červy jsou tedy zpravidla programy, které nemají potřebu infikovat soubory a šíří se samostatně [2, 4].

3.4 Trojské koně

Trojský kůň je obecně považován za jeden z nejjednodušších druhů škodlivých programů. Je to program, který se snaží tvářit užitečně a zároveň obvykle slibuje nějaké zajímavé služby. Jeho cílem je, aby jej uživatel spustil a on mohl napáchat škody [3].

Asi nejznámějším typem trojského koně byl AIDS TROJAN DISK, jenž se rozšiřoval pomocí disket, které byly rozeslány do nejvýznamnějších výzkumných organizací bojujících proti AIDS a po jeho zavedení do systému středisek měl za úkol zpřeházet názvy souborů a zaplnit zbývající místo na disku. Napravení způsobených škod bylo poté nabízeno za úplatu [2].

Počet trojských koňů se zvětšil v době, kdy začaly být přidávány do některých virů a tak se úspěšně šířily do dalších počítačů. Přesto je jejich počet v porovnání s červy či viry velmi nízký a pohybuje se okolo 4% veškerého malware [4].

3.4.1 Trojský kůň typu zadní vrátka

Trojský kůň umožňuje přes počítačovou síť vzdálený přístup k systému. Po spuštění vyčkává na připojení útočníka a ten má pak volnou cestu do systému oběti. Tento způsob je asi nejčastější funkcí trojského koně a je velmi rozšířený mezi hackery [2].

3.4.2 Trojští koně s funkcí hledání hesel

Trojští koně s funkcí hledání hesel jsou primárně zaměřeny na zjištění a hledání hesel, které jsou využity pro přístup k systému oběti. Často bývají doplněny programy pro zaznamenávání stisků kláves, což může velmi ulehčit cestu k odhalení potřebných hesel. Zjištěná hesla bývají automaticky odesílána na e-mailové adresy útočníků [2, 4].

3.4.3 Destruktivní trojské koně

Spuštění takové formy trojského koně může způsobit smazání souborů na disku nebo jeho kompletním zformátováním [4].

3.4.4 Trojský kůň typu dropper

Tento typ trojského koně nese ve svém těle ještě jiný škodlivý kód, obvykle virus, který se po spuštění tohoto trojského koně dostane do systému [4].

3.5 Další typy malware a škodlivých aktivit

3.5.1 Logické bomby

Logické bomby jsou škodlivé naprogramované chyby programu, jejichž cílem je páchat neplechu po splnění určitých podmínek. Napadený program se například může smazat z disku po několikerém otevření nebo po určitém čase [2].

3.5.2 Stahovače

Stahovač se často vyskytuje jako příloha e-mailových zpráv. Po spuštění může stahovat škodlivá data pomocí internetu a poté tyto data spustí [2].

3.5.3 Dialery

Dialery byly velmi populární v době vytáčeného připojení k internetu. Jejich záměrem bylo připojování k jiným telefonním číslům, které poskytovaly připojení za velmi vysoké ceny. Objevovaly se obvykle na stránkách s pornografickým obsahem, kde byl

uživatel upozorněn, že bude pro spojení používáno odlišné telefonní číslo, ale už nebyla uvedena cena připojení [2].

3.5.4 Kity

Kity jsou generátory nových virů či červů, které jsou produkovány na základě voleb uživatele. Proto jsou přístupné i pro nováčky, kteří nepotřebují větší odborné znalosti.

Velice známým červem, vytvořeným generátorem, je červ Anna Kournikova. Jeho stvořitel, v té době dvacetiletý Holanďan, neuměl programovat, ale mnoho lidí chtělo vidět fotografii známé tenistky i modelky a neváhali kliknout. Místo toho byl spuštěn červí skript a červ se začal rychle šířit [2].

3.5.5 Snímače stisku kláves

Programy na snímání stisků kláves předávají útočníkům informace, které zpravidla obsahují osobní údaje i jiná citlivá data a útočník jich může využít pro svou potřebu. Tyto programy jsou na počítačích instalovány bez vědomí uživatele a velmi těžko si jich oběť všimne [2].

3.5.6 Hoax

Hoax je zpráva, která motivuje příjemce k jejímu dalšímu rozeslání, např. jeho přátelům a dalším lidem. Jejich šíření je závislé pouze na uživatelích, kteří jsou ovlivněni výhradně negativním obsahem této poplašné zprávy. Nejčastěji jde o varování před novou formou počítačového viru, kde se autor Hoaxu odvolává na známé autority (například Microsoft, IBM, FBI) a vyzývá k dalšímu rozeslání [4].

3.5.7 Spam

Spam je obecně považován za nevyžádanou poštu, obvykle s reklamním sdělením. Ke spamu může být připojen trojský kůň, který je například schopen instalovat do systému propojení na několik pornografických stránek a případně je i automaticky otevírat.

Spam se vyznačuje i falšováním e-mailových adres odesílatele, které jsou nalezeny na internetových stránkách. Svým ohromným množstvím obtěžují příjemce, a proto jsou vytvářeny různé programy, které filtrují příchozí zprávy a podle určitých pravidel se je snaží rozlišovat [4].

3.5.8. Adware

Adware, neboli také reklamní programy, se dostávají do počítače instalací různých freeware programů. Poté jsou schopny přesměrovat domovskou stránku internetového prohlížeče anebo předkládat různé reklamy [4].

3.5.9 Spyware

Spyware je program, který získává data a odesílá je bez vědomí uživatele. Obvykle se jedná o statistická data, kde se uvádí, jaké stránky uživatel navštěvuje nebo jaké programy používá. Autoři tyto programy odůvodňují tím, že se pouze snaží zjistit zájmy uživatele a data pak mohou použít pro cílenou reklamu nebo pro boj s nelegálním softwarem. Řadí se sem ale i programy, které odcizují citlivá data, jako jsou hesla, certifikáty a podobně [4].

3.2 Stručná historie

Již v roce 1949 popsal John Von Neuman program, který měl schopnost vlastní replikace. První virům podobné programy se však začaly objevovat až na začátku 60. let minulého století. Tehdy skupina programátorů vytvořila hru Core Wars, která se při

každém novém spuštění reprodukovala a zabírala tak místo na disku dalším hráčům. Tvůrci zároveň naprogramovali prvního předchůdce antivirových programů, který sloužil k tomu, aby vzniklé kopie této hry odstranil [11].

První virus, který se začal veřejně šířit, byl virus Joe na počítačích Apple Macintosh v roce 1981. Ovšem až rok 1983 je považován za začátek éry počítačových virů. Hlavním důvodem bylo rozšiřování operačního systému MS-DOS. V tomtéž roce byl na semináři o počítačové bezpečnosti poprvé použit výraz vir Frederickem Cohenem, který ho následně definoval [4, 5].

Rok 1986 přinesl první větší hrozbu pro počítače IBM PC a tou se stal virus Brain, jenž byl vytvořen dvěma bratry z Pákistánu a následně distribuován pomocí disket s nelegálním softwarem, který si od nich kupovali cizinci. V témže roce se také objevil jeden z prvních trojských koňů [4, 11].

O rok později se objevily první souborové viry v čele se známým virem Jerusalem a také červ Christmas worm, který se na svou dobu šířil neobvyklou rychlostí a dokázal za jednu hodinu vytvořit okolo půl milionu kopií [11].

Na trhu se poté začaly objevovat první antivirové programy jako McAfee VirusScan, Dr. Solomon AVTK nebo dokonce první československý antivir AVAST! [4, 5].

V listopadu roku 1988 byl vypuštěn Morrisův červ, který vytvořil student Robert Morris. Tento červ napáchal škody za 100 miliónů dolarů a to i proto, že pronikl do jednoho oddělení NASA. To zčásti zapříčinilo vznik organizace CERT, která měla podobným útokům zabránit [2, 11].

Na přelomu 80. a 90. let se začínaly objevovat tzv. polymorfní viry, které se díky odlišnosti každého exempláře velmi dobře bránily detekcím antivirových programů. Tvůrci antivirových programů tedy museli hledat stále nové metody detekce virů [11].

Okolo roku 1992 se začaly objevovat první programy na vytváření nových virů. Stačilo jen zadat parametry a program byl schopen vytvořit virus podle přání [2, 11].

Popularita virů rostla a začínala se o ně zajímat i média. Prvním virem, o kterém se hromadně informovalo, byl virus Michelangelo [11].

S rozšířením internetu a e-mailu však začala nová éra virů. V roce 1995 vznikl první makrovirus, který využívá speciálního jazyka v aplikacích firmy Microsoft. Jedním z prvních byl Concept, který byl dlouhou dobu těžko detekovatelný antivirovými programy. Roku 1999 se poprvé hromadně začaly šířit viry pomocí e-mailových zpráv. Známý je především vir Melissa nebo Loveletter (I Love You), který se šířil obrovskou rychlostí [2, 4, 11].

V roce 2003 přišel drtivý návrat červů, které využívaly bezpečnostních děr v operačních systémech Microsoft. Běžný antivirový program nedokázal zamezit infekci a bylo potřeba instalovat bezpečnostní záplaty. Nejznámějším červem, který napadl obrovské množství počítačů bez bezpečnostních záplat, byl červ Blaster [2, 4].

Vývoj nelze zastavit a to platí i pro škodlivý software. V současné době pokračuje šíření malware pomocí elektronické pošty, dále šíření spyware, adware a podobně. Velmi žádaným zbožím jsou pro tvůrce virů hesla a čísla kreditních karet. Jedna věc je ale jistá, antivirové programy budou vždy o krok pozadu oproti tvůrcům virů, kteří se snaží vymýšlet stále nové a dokonalejší techniky pro šíření malware [12].

4 Počítačové viry

4.1 Nejčastější důvody vzniku virů

Velmi často si lidé mylně myslí, že tvůrci virů jsou převážně hackeři. Není vyloučeno, že hackeři jsou zároveň tvůrci virů, ale rozhodně to není pravidlem. Pro hackery je hlavní motivací výzva. Jsou hnáni touhou dostat se tam, kde se nacházejí utajované informace. Nejčastějším cílem hackerů se stávají uživatelské účty [6].

Tvůrci virů, na rozdíl od hackerů, mají v úmyslu škodit. Zatímco po hackerech zpravidla nezůstává ani stopa, po činnosti virů tomu je naopak. Počítačový vir dokáže zničit důležitá data na disku.

4.1.1 Touha po slávě

Sen každého programátora je, že jeho program bude hromadně používán. Virus je možnost, jak tohoto snu dosáhnout i bez souhlasu samotných uživatelů. Tvůrci virů bývají motivováni pouhou představou, že jednoho dne budou číst zprávu o tom, jak jejich virus řádí ve světě [6].

4.1.2 Prostředek seberealizace

Pro některé programátory může být tvorba viru jakýmsi testem jejich schopností. Antivirové prostředky a operační systémy bere tvůrce viru jako určitou výzvu. Jako je pro někoho potřeba např. sportovat, tak pro tohoto programátora, který sedí od rána do večera u svého počítače, je seberealizačním prostředkem tvorba viru [6].

4.1.3 Lidská zvědavost

Časté zmiňování virů ve sdělovacích prostředcích je důsledkem toho, že lidé bývají zvědaví, jak viry vůbec fungují. Z tohoto důvodu si programátor může nějaký ten vir zkusit napsat a v horším případě u toho zůstane [6].

4.1.4 Snaha škodit, ničit, ublížit

Snaha někoho poškodit nebo se mu pomstít je jedním z nejhlavnějších důvodů tvorby virů. Známé bývají případy, kdy se bývalí zaměstnanci firmy chtěli nějakým způsobem pomstít firmě, která je propustila, a jedním z těchto způsobů byl počítačový virus. Dalším důvodem je boj mezi počítačovými experty. Na jedné straně může stát fanatický tvůrce virů a na straně druhé antivirový expert, na kterého jsou útoky směřovány [6].

4.1.5 Ekonomický zisk

Na existenci počítačových virů asi nejvíce vydělávají antivirové firmy. Proto se také občas objevují názory, že tyto firmy viry vytváří. Je logické, že čím bude ve světě více virů, tím budou mít antivirové firmy větší zisk. Na druhou stranu je velice málo pravděpodobné, že by se některá z těchto firem k takovému činu snížila. V případě odhalení by se na trhu naprosto znemožnila a dost pravděpodobně by to znamenalo konec a krach takovéto firmy.

Existuje však tvorba virů na zakázku, kde si člověk, který se chce někomu pomstít, najme programátora a ten může být motivován vidinou slušného výdělku [6].

4.2 Klasifikace virů podle umístění v paměti

Virus má zpravidla dvě možnosti na provedení své činnosti. Buď vykoná jednorázovou akci, například infikuje další soubory, a poté přenechá řízení svému hostiteli anebo setrvávají v paměti, kde čekají na to, aby mohly udeřit [4, 6].

4.2.1 Nerezidentní viry

Tato skupina virů je také nazývána viry přímé akce. Virus přebere řízení programu, provede svoji činnost, zpravidla sebereplikaci, a poté přenechá řízení opět hostitelskému programu. Tento typ virů se v současné době příliš nevyskytuje [4, 6].

4.2.2 Rezidentní viry

Hlavním znakem těchto virů je, že se snaží setrvat v paměti. Ještě než dokončí svoji činnost, zajistí, že část jeho těla bude nadále aktivní i po předání činnosti operačnímu systému. Typickým příkladem rezidentního programu je ovladač myši a programy, které se aktivují po stisku tlačítka myši. Viry ovšem provádějí svojí činnost bez vědomí uživatele [4, 6].

4.3 Klasifikace virů podle rychlosti šíření

- **Rychlé viry** aktivní v paměti napadají všechny programy, které jsou otevřeny. Prohledávání disku, například antivirovým programem, může vést k infekci všech spustitelných souborů.
- **Pomalé viry** aktivní v paměti čekají, až bude spustitelný soubor regulérně pracovat a pomalu se rozmnožují. Běžný uživatel si této činnosti jen těžko všimne a virus má dostatek času pro infikaci všech potřebných paměťových médií.

- **Viry zřídka napadající** útočí na spustitelné soubory jen při splnění nějakých podmínek, například každý desátý spustitelný soubor. Tím snižují pravděpodobnost odhalení, ale zároveň je jejich rychlost šíření velice nízká [4, 5].

4.4 Klasifikace virů podle chování, způsobu vzniku a možnosti detekce

Všechny viry v současné době využívají pokročilé metody, které jim umožňují alespoň dočasně se skrývat před antivirovými programy.

- **Stealth viry** monitorují činnosti systému, případně falšují údaje a poté napadají soubory při jejich kopírování a spouštění.
- **Kódované viry** kódují části svého těla a tím znesnadňují svou detekci před antivirovými programy.
- **Polymorfní viry** mění svůj kód a tím se liší od předchozích generací virů. Jednou z metod kódování je rozdělení viru do malých částí a ty volně zpřeházet uvnitř kódu viru tak, aby nedošlo ke změně funkce viru.
- **Viry napadající antivirové programy** (Retroviry) jsou záměrně zaměřeny proti některým antivirům. Mohou mazat soubory z antivirového programu, zastavit jeho činnost, anebo při spuštění antivirového programu konají škodlivé akce.
- **Viry vyhýbající se antivirovým programům** obsahují knihovnu s názvy nejznámějších antivirových programů, které záměrně nenapadají a tím tak oddalují svou detekci. Většina antivirových programů totiž využívá samokontrolu integrity, která okamžitě zjistí a nahlásí své napadení [4, 5].

4.5 Škody způsobované viry podle Solomona

Toto rozdělení škod způsobených viry vychází z jejich destrukčních vlastností a doby, která uplyne mezi přítomností viru v systému a jeho detekcí [4].

- **Triviální** – virus není přepisující a nemá destrukční části. Pár minut na napravení škod.

- **Malé** – potřeba obnovit některé nebo všechny spustitelné soubory ze záložních kopií, může trvat desítky minut.
- **Střední** – virus zformátuje HDD, případně zakóduje disk, náprava může trvat půl dne.
- **Velké** – virus objeven až po několika dnech a postupně zničil důležitá data, která musí být obnovena ze záloh, pokud existují. Je třeba reinstalovat software. Pokud je možná náprava, může trvat i několik dní.
- **Kruté** – virus, který ničí data je objeven s velkým zpožděním. Obnova je velice obtížná, neboť virus mohl dříve napadnout i data, která si uživatel zálohoval [4].

4.6 Viry pro MS DOS

Nejstarší skupinou počítačových virů jsou viry pro operační systém MS DOS. Ten byl i přes svá dílčí vylepšení více než vhodným pro šíření virů. Neexistovala jakákoliv ochrana jádra operačního systému, systémových oblastí a souborů proti napadením virů, které se tak mohly velmi úspěšně šířit. MS DOS byl navíc ve své době nejrozšířenějším operačním systémem na světě a Microsoft se při vývoji dalších verzí snažil, aby všechny stávající programy byly spustitelné i v novějších operačních systémech. To ovšem zamezovalo využití nejnovějších prvků ochrany proti virům [4].

4.6.1 Boot viry

Boot viry ukládají své tělo do boot sektoru diskety či pevného disku. Boot sektor má každá disketa či každý logický disk pevného disku (pevný disk se dělí na několik logických disků, které si jsou navzájem nezávislé). Virus se přenáší pomocí boot sektoru diskety zasunuté v počítači. Po nabootování (zavedení operačního systému) ze zavirované diskety zapomenuté v mechanice se virus aktivuje a přenese svoje tělo do boot sektoru logického disku. Tam se virus při dalším bootu z pevného disku spustí ještě před naběhnutím operačního systému a velmi často nakazí každou nechráněnou disketu vloženou do počítače. Tyto viry mohou způsobovat například formátování disku či jiné

nevyžádané akce. Stojí ovšem za připomenutí, že k napadení diskety dochází až při jejím nabootováním, nikoliv při pouhém vložení do počítače. V současné době jsou tyto viry prakticky mrtvé, souvisí to hlavně s vymizením disket jako média pro přenos dat [1, 4, 6].

4.6.2 Souborové viry

Tato skupina virů byla ve své době bezesporu nejrozšířenější a, jak už z názvu vyplývá, napadá spustitelné soubory operačního systému. Nejčastěji se jedná o přímo spustitelné programy s příponou COM a EXE, ale mohou být napadeny také soubory s příponou BAT, SYS a další. Podle metody infekce a umístění viru v souboru se dají rozdělit do několika skupin [4].

4.6.2.1 Přepisující viry

Přepisující viry se vyznačují tím, že původní kód programu je zničen (přepsán) a při spuštění souboru dojde pouze k aktivaci viru. Napadený program se nespustí a spustí se pouze virus, který se bude snažit rozmnožovat. Nevýhodou těchto virů je, že jsou snadno odhalitelné díky nefunkčnosti napadeného programu [1, 4, 6].

4.6.2.2 Parazitické viry

Tyto viry mají schopnost zkopírovat své tělo nejčastěji na konec napadeného programu, aniž by původní program poškodily. Při spuštění infikovaného programu nejprve dochází k aktivaci viru a po dokončení jeho činnosti se spustí původní program. U těchto virů uživatel nemusí poznat, že je program infikován [1, 4, 6].

4.6.2.3 Doprovodné viry

Doprovodné viry napadají EXE soubory takovým způsobem, že vytvoří nový soubor se stejným názvem, kde je uloženo tělo viru, ale s rozdílnou příponou COM. Při zadání příkazu ke spuštění souboru nalezne operační systém nejprve soubor s příponou COM a jeho spuštěním dojde k aktivaci viru. Poté zpravidla dochází ke spuštění původně volaného programu, čímž se odvede pozornost od činnosti viru [1, 4, 6].

4.7 Viry pro operační systémy Win32

Nejčastější formou virů jsou v současné době viry pro operační systémy Win32, mezi které patří Windows 9x, Me, NT (2000, XP a další). Velké množství virů pro operační systém MS DOS nebylo schopno v tomto novém prostředí správně fungovat, a tak se jejich autoři museli přizpůsobit a vymýšlet nové typy virů. Jejich funkčnost zajišťuje Win32 API, množina funkcí operačních systémů 9x a NT. Win32 API se poprvé objevilo ve Windows NT a v menším rozsahu i v řadách Windows 9x a až poté se objevil nový spustitelný formát souborů - PE (Portable Executable). První Win32 virus byl vytvořen pro operační systém Windows 95, ale díky kompatibilitě operačních systému fungoval i na Windows 98 a Windows 2000, ačkoliv tyto operační systémy v té době ještě neexistovaly a autor viru ho na těchto systémech nikdy netestoval. Z hlediska virů se stala kompatibilita Win32 systémů pro Microsoft zlým snem [2, 4].

4.8 Makroviry

Dlouhou dobu přetrvával názor, že se viry mohou rozšiřovat pouze pomocí spustitelného kódu. To se ale s příchodem makrovirů změnilo. Tyto druhy virů mohou být nebezpečné ve všech programech podporujících makrojazyk, jako jsou například kancelářské programy Microsoft Office. „Makrojazyk je interní soubor instrukcí dané aplikace, vytvořený za účelem efektivnějšího využití pracovního prostředí“ [6, s. 41].

Pro své šíření využívají makra, což jsou programy, které si uživatel v některých aplikacích vytvoří pro usnadnění práce a to například pomocí příkazů příslušného jazyka.

Makra jsou obvykle uložena dohromady s dokumentem v jednom souboru a tím se změní dokument z datového souboru v soubor, který je za vhodných podmínek interpretován, což je jedna z podmínek pro fungování počítačového viru. V aplikaci Microsoft Word je nejčastějším místem, kde bývá napadán, globální šablona NORMAL.DOT. Tato šablona se automaticky otevře při každém startu aplikace, a když jí virus napadne, tak má kontrolu nad celým Wordem ihned po jeho spuštění.

Velká většina makrovirů byla napsána pro aplikace společnosti Microsoft a to souvisí hlavně s rozšířeností těchto aplikací. Vzhledem k tomu, že se dokumenty šíří mezi lidmi více než programy, je tento druh virů velice rozšířený a oblíbený. Neméně zajímavá je i vlastnost makrovirů, že mohou úspěšně fungovat na různých operačních systémech i různých programech z jednoho kancelářského balíku Microsoft Office [1, 4, 6].

4.9 Skriptové viry

S příchodem Microsoft Internet Exploreru 5.0 zároveň přišel i Windows Script Host. Tento modul umožňuje vykonávat jak Java Scripty, tak i Visual Basic Scripty, a to stejně jednoduše jako u klasických spustitelných souborů, pouhým poklepáním myší na ikonu [4].

Zde se objevil podobný problém jako u makrovirů. Skriptovací jazyk nabízí spoustu možností, jak vytvořit úspěšně se šířící virus a to nejčastěji pomocí elektronické pošty. Dále mohou být tyto skripty přímo vloženy do HTML kódu internetových stránek a při nesprávném nastavení internetového prohlížeče může docházet k jejich spuštění a tím k aktivaci viru. Některé internetové prohlížeče mají toto nesprávné nebo nevhodné nastavení jako standardní a bohužel dochází velmi často k napadení počítače, především u Microsoft Internet Exploreru [4].

4.10 Speciální skupiny virů

4.10.1 Multiplatformní viry

Pokud nepočítáme makroviry, tak jsou multiplatformní viry ojedinělou a neobvyklou skupinou počítačových virů. Již podle názvu je patrné, že se jsou schopny rozšiřovat pod různými platformami, čímž jsou myšleny různé operační systémy.

Jeden ze způsobů šíření těchto virů je pomocí takzvaných emulátorů, které jsou schopny pod operačním systémem Linux spouštět aplikace Win32 a tím i viry [4].

4.10.2 Multiparitní viry

Toto označení virů se nejčastěji objevuje v souvislosti s viry operačního systému MS DOS, které kombinovaly několik metod pro jejich replikaci. Nejčastěji šlo o takové viry, které se dokázaly rozšiřovat pomocí souborů, ale zároveň byly i boot viry, tudíž se dokázaly usadit v oblasti pevného disku [4].

4.10.3 HLL viry

S nástupem operačních systémů Windows se zvýšil i počet takzvaných High Level Languages virů. Tyto viry jsou vytvářeny ve vyšších programovacích jazycích, jako C++, Pascal, Delphi a mnoho dalších. Na rozdíl od ostatních virů jsou tyto viry mnohem větší, co se týče velikosti binárního souboru, a proto musí být obvykle komprimovány [4].

5 Prevence proti škodlivému kódu

Dodržením několika jednoduchých pravidel obrany proti škodlivému kódu můžeme značně minimalizovat riziko nákazy počítače a zamezit případné ztrátě dat.

5.1 Pravidelná záloha

Pravidelná záloha všech důležitých dat nám může zaručit možnost vrátit se k již ztraceným nebo poškozeným souborům. Zálohovat by se mělo velmi často a hlavně pravidelně, aby bylo možné data v případě ztráty obnovit [7, 8].

5.2 Ignorace dat z cizích zdrojů a emailových příloh

Dříve představovaly nejčastější zdroj nákazy diskety. Dnes se viry a další škodlivý software šíří hlavně pomocí internetu a počítačových sítí. Tyto komunikační kanály jim dávají možnost infikování mnoha počítačů po celém světě za velmi krátkou dobu.

Při surfování na internetu na nás může vyskočit nové okno, které zdarma nabízí stažení nějaké skvělé aplikace, jejíž jméno pravděpodobně nikdo neslyšel. Velice často se pod touto aplikací skrývá nějaký škodlivý kód, pro který je to snadná cesta k nakažení počítače. Podobně je to i s přílohami emailových zpráv od neznámých autorů. Ty se doporučují neotvírat a směle ignorovat. Stále se ale najde velmi mnoho lidí, kteří jsou schopni otevřít přílohu emailové zprávy typu VTIP.EXE, která může například způsobit nakažení počítače a rozeslání zpráv všem lidem, na které tento škodlivý software nalezne emailovou adresu v počítači [8].

5.3 Používání specializovaných aplikací a jejich aktualizace

Asi nejlepší způsob, jak se vyhnout škodlivému kódu v našem počítači, je pořízení specializovaných programů. Moderní antivirové programy jsou schopny odhalit a odstranit

viry ještě předtím, než se zahnízdí v počítači a vykonají nějaké škody. Jejich výrobci ale musejí neustále vydávat aktualizace, které dokážou rozpoznat i nejnovější hrozby. Tyto aktualizace si program může stahovat sám, ale je třeba dbát na to, aby byl příslušný antivirový program dobře nastaven a plně funkční [8].

5.4 Používání firewallu

Nezbytným bezpečnostním doplňkem každého počítače by měl být firewall. Operační systémy Windows obvykle obsahují základní verzi firewallu, který dokáže zabránit řadě síťových hrozeb. Je ale třeba znovu dbát na správné nastavení [8].

5.5 Přemýšlet a nepanikařit

V mnoha případech je to uživatel sám, kdo nechtěnou akci spustí. Proto je lepší přemýšlet a pozorně číst, než spustit nějakou aplikaci, která může poškodit počítač.

Když už ale uživatel zjistí, že je počítač napaden, měl by zachovat chladnou hlavu a nepanikařit. Mnohdy není potřeba přeinstalovat operační systém z důvodu, že antivirový program nedokázal odstranit škodlivý software. Některé antivirové firmy dokonce vydávají jednoúčelové utility, které jsou schopny odstranit danou hrozbu, s kterou si neporadil antivirový program [8, 9].

6 Antivirové programy

Nainstalovat antivirový program je jednou z nejjednodušších možností, kterou uživatel může udělat, aby ochránil svůj počítač před škodlivým softwarem.
Z uživatelského hlediska jsou důležitými parametry cena, možnosti aktualizace, lokalizace, spolehlivost detekce a spousta dalších. V dnešní době existuje řada antivirových programů, které se dají zdarma stáhnout z internetu a není nic jednoduššího než je nainstalovat, pravidelně aktualizovat a mít tak alespoň základní ochranu počítače [4].

6.1 Základní činnosti antivirového programu

6.1.1 Vyhledávání

Všechny význačné znaky virů má v sobě antivirový program naprogramován, a jestliže nalezne v počítači nějaký program s charakteristikami, které už zná, prohlásí ho za virus. Metoda je to velmi účinná v případě, je-li podoba viru přesně známa. V opačném případě, kdy je virus nějakým způsobem upravený, je tato metoda příliš zdlouhavá a nákazu nemusí odhalit [9].

6.1.2 Skenování

Antivirový program porovnává řetězce souborů se svou databází. Pokud je shodný s řetězcem ve své interní databázi, pak je tento soubor označen jako zavirovaný. Metoda je to velmi rychlá a spolehlivá, ale mnohdy se stává, že je soubor prohlášen virem, i když jím není [9].

6.1.3 Heuristická analýza

Heuristická analýza je metoda, kdy antivirový program provádí rozbor kódu souboru a krok po kroku hledá nějakou podezřelou instrukci. Metoda dokáže zachytit

činnosti programů, které jsou obvyklé pro viry a tím je možné odhalit i ty, které dosud nebyly známé [4, 5, 9].

6.1.4 Kontrola integrity

Při napadení souboru se virus nějakým způsobem projeví, například změnou velikosti. Kontrola integrity porovnává stav před možným nakažením se stavem po nakažení a to na základě těchto změn. Dokáže dokonce zachytit i nové viry, které nebyly odhaleny heuristickou analýzou. Tato metoda ale není moc pohodlná pro koncového uživatele, který se o ni musí správně a pravidelně starat, což je jeden z důvodů, proč pomalu mizí z antivirových programů [4, 9].

6.1.5 Rezidentní sledování

Antivirový program má možnost být rezidentní, tedy spustit se ihned po startu počítače a běžet na pozadí. Počítač je tedy neustále hlídán a antivirový program dokáže upozornit na podezřelé akce, které mohou probíhat [9].

6.2 Firmy zabývající se antivirovými programy

Je velmi mnoho společností, které se zabývají vývojem antivirových programů. Některé z nich zde budou představeny.

6.2.1 AVAST Software a.s.

Česká firma, nástupce firmy Alwil Software, založená Eduardem Kučerou a Pavlem Baudišem na začátku devadesátých let minulého století. Zpočátku nabízela antivirové programy především velkým firmám a bankám, ale společnost moc

neprosperovala. Průlom nastal v roce 2002, kdy poskytli novou verzi svého programu zcela zdarma. V současnosti je jejich hlavním produktem avast! 7 Internet Security [13, 14].

6.2.2 AVG Technologies

Další česká firma AVG byla založena roku 1991 a dnes je považována za jednu z největších na trhu bezpečnostního software. Již 110 miliónů uživatelů používá produkty od této firmy. Jejich produkty jsou AVG Anti-Virus 2012 a AVG Internet Security 2012 [15].

6.2.3 ESET

Slovenská firma sídlící v Bratislavě byla založena v roce 1992 a v současné době chrání více než 90 miliónů uživatelů. Podle žebříčku Deloitte Technology Fast 500 patří mezi jednu z nejrychleji rostoucích technologických společností v regionu Evropy, Afriky a Blízkého východu. ESET Smart Security 5 a ESET NOD32 Antivirus 5 jsou jejich vlajkovými loděmi v boji proti škodlivému kódu [17].

6.2.4 Kaspersky Lab

Kaspersky Lab, založená v roce 1997 a sídlící v Moskvě, patří mezi přední výrobce bezpečnostního software. Více než 300 miliónů uživatelů používá jejich software a dle nezávislých expertů má tato společnost nejrychlejší reakce proti novým hrozbám. Aktuální verze jejich programů jsou Kaspersky Anti-Virus 2012 a Kaspersky Internet Security 2012 [18].

6.2.5 McAfee

Společnost McAfee, sídlící v Kalifornii, patří mezi špičku mezi producenty antivirových produktů. Vysoká úspěšnost v boji proti virům je oceňována nejen odborníky, ale i veřejností. Njenovějším produktem firmy je McAfee AntiVirus 2012 [19].

6.2.6 Symantec

Světová jednička v poskytování zabezpečení nebo správ systému je společnost Symantec. Zároveň je to čtvrtá největší nezávislá společnost na světě v oblasti software. Velmi známými produkty jsou Norton Antivirus 2012 nebo Norton Internet Security 2012 [20].

6.2.7 TrustPort

Poměrně neznámá česká firma, která vznikla v rámci společnosti AEC v roce 1991. Zpočátku bylo hlavní zaměření na ochranu počítačů pro potřeby firmy, ale později si získala dobré renomé a od roku 2000 obdržela nespočet ocenění za kvality. Pro domácnosti vytváří produkt TrustPort Antivirus 2012 [21].

7 Výběr vhodného antivirového programu

7.1 Definování uživatele

Před zvolením ideálního antivirového programu je potřeba definovat uživatele, který bude tento druh software využívat.

V tomto případě bude naším uživatelem vlastník domácího počítače, který bude chtít co nejlépe ochránit svoje PC. U našeho uživatele se předpokládají pouhé základní znalosti práce s počítačem, jako je instalace a spouštění programů.

Porovnávané antiviry budou placené a výběr ideálního programu proběhne za pomocí několika kritérií, na jejichž základě se uživatel rozhodne.

7.2 Kritéria pro výběr antivirového programu

- **Schopnost detekce virů** – priorita 1
  Kritérium schopnosti detekce virů je asi nejdůležitějším kritériem pro výběr vhodného antivirového programu. Pro toto srovnání posloužil On-Demand Comparative test antivirových programů z internetových stránek http://www.av-comparatives.org/.

- **Vliv na výkon počítače** – priorita 2
  Jak působí antivirový program na výkon počítače je další důležité kritérium. Současné antiviry jsou rezidentní, běží na pozadí počítače a to mnohdy může způsobit jeho zpomalení. Srovnání poskytla internetová stránka http://www.av-comparatives.org/ v sekci Performance Test.

- **Cena licence na jeden rok** – priorita 3
  Běžný uživatel, který chce co nejlépe chránit svůj počítač, nebude brát ohled na cenu software, a tudíž tomuto kritériu přiřadíme střední prioritu.

- **Lokalizace do češtiny –** priorita 4
  Český jazyk je běžně podporován u většiny software a měl by být standardní výbavou i u antivirových programů.

- **Místo na disku** – priorita 5
  Prakticky nejméně důležitým kritériem při výběru antivirového programu jsou požadavky na volné místo na pevném disku počítače.

7.3 Testované antivirové programy

7.3.1 ESET NOD32 Antivirus 5

Tento slovenský antivirový program je možno stáhnout na oficiálních stránkách výrobce a na 30 dní zcela zdarma vyzkoušet. Pokud by se uživatel rozhodl pro zakoupení licence na jeden rok, zaplatil by 1199 Kč včetně DPH. Licence na dva roky stojí 1799 Kč s DPH a na tři roky 2518 Kč včetně DPH. Je také možnost koupit licenci na několik počítačů ve zvýhodněné ceně [22].

Program je plně podporován ve více než dvaceti jazycích a čeština je zde samozřejmostí.

Pro instalaci ESET NOD32 Antivirus 5 je potřeba 400 MB volného místa na pevném disku a pro registraci produktu je třeba připojení na internet, které je nutné ke stahování nejnovějších aktualizací. Standardně nastavené stahování aktualizací je každou hodinu, ale v případě potřeby je možno toto nastavení změnit pro potřeby uživatele.

Podporovanými procesory jsou Intel® 80386 a amd64. Program podporují i všechny nejnovější operační systémy Microsoft Windows (2000, XP, Vista, 7, HOME SERVER) [22].

Podle http://www.av-comparatives.org/ je schopnost detekce virů 97,3% a z testu zatížení počítače dostal tento antivir 189,8 bodů z 200, což je velmi nadprůměrný výsledek (čím víc bodů, tím lépe) [23, 24].

Oproti předchozí verzi je vylepšena ochrana všech médií (USB disků,

paměťových karet, CD/DVD) a také například inteligentní mód spotřeby pro notebooky, kde program pozná nízkou výdrž baterie a oddálí plánované činnosti [22].

7.3.2 Norton AntiVirus 2012

Norton AntiVirus 2012 má 30denní zkušební verzi, kterou si uživatel může zdarma stáhnout na adrese http://cz.norton.com/. Po 30denní zkušební lhůtě je možnost program odinstalovat nebo si zaplatit licenci. Za jeden rok ochrany programem Norton AntiVirus 2012 je třeba zaplatit 1189 Kč a za dva roky ochrany 1899 Kč, kde je DPH započítáno. Zvýhodněná cena za licenci pro několik počítačů je také dostupná [25].

Antivirový program podporuje český jazyk, operační systémy Microsoft Windows (XP, Vista, 7) a pro jeho instalaci je potřeba 300 MB volného místa na disku. Minimálními požadavky na hardware jsou 300 MHz pro systém Microsoft Windows XP a 1 GHz pro operační systémy Microsoft Windows Vista a 7 [25].

Dle nezávislého srovnání antivirových programů na stránce http://www.av-comparatives.org/ má Norton AntiVirus 2012 schopnost detekce virů 95,1%. Při testu zátěže počítače obstál na výbornou a z 200 bodů dostal 189,7 [23,24].

Program aktualizuje svojí databázi každých 5-15 minut bez toho, aby uživatele rušil. Bezplatná podpora 24 hodin denně a 7 dní v týdnu je samozřejmostí [25].

Funkce Insight kontroluje u souborů jejich původ a dobu cirkulace, a tak je schopna zastavit budoucí hrozby ještě dříve, než způsobí potíže [25].

7.3.3 Kaspersky Anti-Virus 2012

Kaspersky Anti-Virus 2012 má možnost, stejně jako většina současných antivirů, 30denní zkušební lhůty zdarma. Poté má uživatel možnost zakoupit licenci a pokračovat v používání antivirového programu. Licence na jeden rok stojí 876 Kč včetně DPH, na dva roky je cena licence 1464 Kč s DPH. Sleva při objednání licence na více počítačů je zde také [26].

Antivirový program běží pod operačním systémem Microsoft Windows XP, při výkonnosti procesoru vyšším než 800 MHz. Na operačních systémech Microsoft Windows

Vista a 7 bezproblémově funguje za předpokladu, že bude procesor výkonnější než 1 GHz. Instalace zabere přibližně 480 MB místa na disku a program lze spustit v několika jazycích včetně češtiny [26].

Z testů schopnosti detekce virů z http://www.av-comparatives.org/ vyšel Kaspersky Anti-Virus 2012 velmi solidně a měl úspěšnost 98,3% při hledání virů. Zátěžový test zvládl také dobře a získaných 188,9 bodů z 200 a umístil mezi nejlepšími [23, 24].

V nejnovější verzi je možnost podávání přehledu o bezpečnosti systému přímo v postraním panelu Windows. Kaspersky Anti-Virus 2012 má také unikátní technologii, která umožní instalaci programu na již zavirovaný počítač [26].

7.3.4 TrustPort Antivirus 2012

TrustPort Antivirus 2012 nabízí 30denní zkušební verzi a uživatel si ji zdarma může stáhnout na oficiálních stránkách produktu. Cena licence na jeden rok vyjde na 827 Kč včetně sazby DPH a dále je možno pořídit produkt ve zvýhodněných cenách pro licence na více počítačů [27].

Antivirový program je možné spustit na operačních systémech Microsoft Windows (2000, XP, Vista, 7) a procesorech Intel® Pentium IV nebo vyšších. Pro instalaci je potřeba minimálně 500 MB místa na disku a je možno nastavit více než deset světových jazyků včetně češtiny [27].

Test schopnosti detekce virů zvládl program excelentně a podle stránky http://www.av-comparatives.org/ dokáže odhalit 99,6% škodlivého kódu. Test zátěže pro počítač už tak dobrý nebyl a program získal 157,4 bodů z 200 [23, 24].

Program má možnost využít dva špičkové skenovací motory a díky tomu dosahuje jedné z nejvyšších úspěšností detekce, což se ale negativně odráží na zátěži počítače [27].

7.4 Výběr antivirového programu metodou váženého součtu

Metoda váženého součtu konstruuje celkové hodnocení pro každou variantu, tudíž je vhodná jak pro hledání nejvýhodnější nebo nejlepší varianty, tak i pro jejich uspořádání od nejlepší po nejhorší [10].

1. V našem případě si uživatel stanovil váhy jednotlivých kritérií. Váhy musí dávat dohromady součet 1 a platí, že čím větší priorita, tím vyšší váha.
2. Typ kritéria může být maximalizační nebo minimalizační. Je logické, že u ceny bude použito kritérium MIN (hledám nejnižší cenu) a u schopnosti detekce kritérium MAX (hledám program, který detekuje viry s co nejvyšší úspěšností).
3. Převedení kritéria minimalizačního na maximalizační proběhne tak, že z každého kritéria u MIN bude vybrána jeho nejvyšší hodnota a od ní odečtena hodnota u každé varianty. Dalo by se vyjádřit pomocí vztahu

   $$y_{ij} = \max_{i=1,\dots,m}(y_{ij}) - y_{ij} \ [10, \text{s. } 30]$$

   kde y_{ij} je prvkem kriteriální matice.
4. Stanoví se ideální a bazální varianta. Ideální varianta H s ohodnoceními $(h_1, \dots, h_n)$ je nejlepší možná hodnota a bazální varianta D s ohodnoceními $(d_1, \dots, d_n)$ je nejhorší možná hodnota.
5. Vytvoření standardizované kriteriální matice R proběhne pomocí vzorce

   $$r_{ij} = \frac{y_{ij} - d_j}{h_j - d_j} \ [10, \text{s. } 31]$$

   kde r_{ij} je prvkem standardizované kriteriální matice, y_{ij} je prvkem kriteriální matice, d_j je bazální hodnota daného kritéria a h_j je ideální hodnota daného kritéria.
6. Je třeba vypočítat agregovanou funkci užitku a to pomocí skalárního součinu všech prvků dané varianty a jejich příslušných vah. Vyjádřeno vzorcem

   $$u(a_i) = \sum_{j=1}^{n} v_j r_{ij} \ [10, s. 31]$$

   kde v_j je hodnotou příslušné váhy a r_{ij} je prvkem standardizované kriteriální matice.

7. Varianta s nejvyšší hodnotou užitku $u(a_j)$ bude nejlepší variantou pro výběr vhodného antivirového programu [10].

Tabulka č. 1: Kriteriální matice pro výběr vhodného antivirového programu

	Cena licence na 1 rok v Kč	Lokalizace do češtiny [1)]	Velikost na disku v MB	Schopnost detekce v %	Body za vliv na výkon PC
ESET NOD32 Antivirus 5	1199	1	400	97,3	189,8
Norton AntiVirus 2012	1189	1	300	95,1	189,7
Kaspersky Anti-Virus 2012	876	1	480	98,3	188,9
TrustPort Antivirus 2012	827	1	500	99,6	157,4
Váhy	0,1	0,03	0,02	0,5	0,35
Povaha	MIN	MAX	MIN	MAX	MAX

pozn. [1)] u lokalizace do češtiny je „Ano“ bráno jako hodnota 1 a „Ne“ jako hodnota 0

zdroj: autor dle [22, 23, 24, 25, 26, 27]

V tabulce č. 1 jsou uvedeny základní hodnoty jednotlivých kritérií. Váhy jsou stanoveny podle preferencí uživatele.

Tabulka č. 2: Kriteriální matice s převedenými kritérii z MIN na MAX

	Cena licence na 1 rok v Kč	Lokalizace do češtiny	Velikost na disku v MB	Schopnost detekce v %	Body za vliv na výkon PC
ESET NOD32 Antivirus 5	0	1	100	97,3	189,8
Norton AntiVirus 2012	10	1	200	95,1	189,7
Kaspersky Anti-Virus 2012	323	1	20	98,3	188,9
TrustPort Antivirus 2012	372	1	0	99,6	157,4
Váhy	0,1	0,03	0,02	0,5	0,35
Povaha	MAX	MAX	MAX	MAX	MAX
Ideální varianta	372	1	200	99,6	189,8
Bazální varianta	0	1	0	95,1	157,4

zdroj: autor

Tabulka č. 2 uvádí převedené hodnoty z minimalizačního kritéria na maximalizační. Je stanovena ideální a bazální varianta.

Tabulka č. 3: Standardizovaná kriteriální matice

	Cena licence na 1 rok v Kč	Lokalizace do češtiny	Velikost na disku v MB	Schopnost detekce v %	Body za vliv na výkon PC
ESET NOD32 Antivirus 5	0	0	0,5	0,488888	1
Norton AntiVirus 2012	0,02688172	0	1	0	0,99691358
Kaspersky Anti-Virus 2012	0,868279569	0	0,1	0,711111	0,97222222
TrustPort Antivirus 2012	1	0	0	1	0
Váhy	0,1	0,03	0,02	0,5	0,35
Povaha	MAX	MAX	MAX	MAX	MAX

zdroj: autor

Ve standardizované kriteriální matici (tabulka č. 3) jsou vypočteny hodnoty jednotlivých kritérií za pomoci ideálních a bazálních variant.

Tabulka č. 4: Výsledná tabulka

	Cena licence na 1 rok v Kč	Lokalizace do češtiny	Velikost na disku v MB	Schopnost detekce v %	Body za vliv na výkon PC	Výsledek (užitek)
ESET NOD32 Antivirus 5	0	0	0,5	0,488888	1	0,604444
Norton AntiVirus 2012	0,02688172	0	1	0	0,99691358	0,371608
Kaspersky Anti-Virus 2012	0,868279569	0	0,1	0,711111	0,97222222	**0,784661**
TrustPort Antivirus 2012	1	0	0	1	0	0,6
Váhy	0,1	0,03	0,02	0,5	0,35	

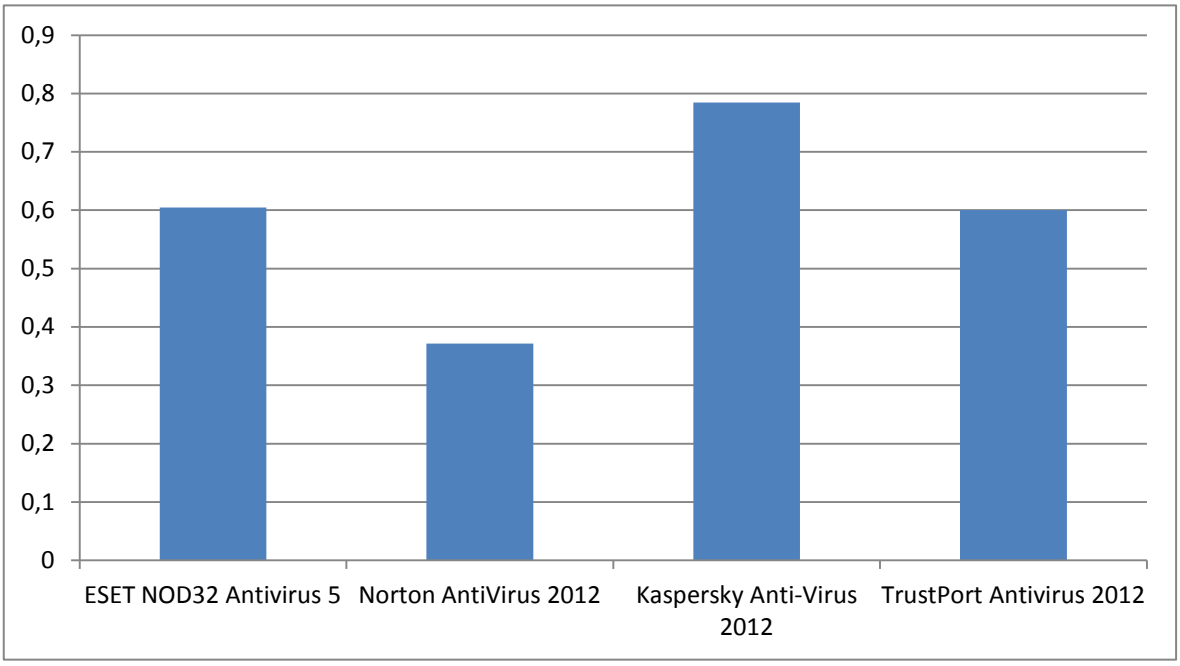
zdroj: autor

Ve výsledné tabulce č. 4 je pomocí výše uvedené metody váženého součtu zjištěno, že nejlepší možnou variantou antivirového programu je Kaspersky Anti-Virus 2012 s hodnotou užitku 0,784661.

7.5 Shrnutí

Za pomoci metody váženého součtu a stanovených vah bylo zjištěno, že nejoptimálnějším antivirovým programem je Kaspersky Anti-Virus 2012, který obržel nejvyšší známku ze všech hodnocených programů.

Graf č. 1: Výsledky



zdroj: autor

8 Závěr

V současné době je možné narazit na škodlivý software téměř kdekoliv. Proto je třeba počítač chránit. Existuje několik desítek firem, které se zabývají ochranou počítače a nabízí nepřeberné množství produktů. Jedním z nich jsou antivirové programy. Mít v počítači nainstalovaný antivirový program ale nestačí. Je třeba používat vhodný firewall, který je běžně součástí operačního systému, dále je třeba zálohovat důležitá data, aktualizovat antivirový program a hlavně také používat hlavu. Mnohdy se stane, že uživatel svojí neznalostí naletí na nějakou nástrahu na internetu a nakazí tak svůj počítač.

Výběr vhodného antivirového programu je ale dobrý začátek pro ochranu počítače. Tímto druhem softwaru by ale měl být bezpodmínečně chráněn každý počítač. Dnešní antivirové programy nabízí nespočet možností ochrany osobního počítače jak pro běžného uživatele, tak i pro firmy. Je možnost si je stáhnout z internetu, zdarma vyzkoušet na určitý počet dní a následně zakoupit licenci. To všechno lze pomocí internetu, a tudíž je to velice jednoduché pro každého běžného uživatele. Některé antivirové programy jsou dokonce dostupné zcela zdarma a často nabízí velice kvalitní ochranu, srovnatelnou s některými placenými programy.

V této bakalářské práci byly srovnávány čtyři placené antivirové programy na základě několika kritérií. Těmi byla cena, lokalizace do češtiny, schopnost detekce škodlivého kódu, zátěž pro počítač a velikost místa, které je potřeba na pevném disku. Největší váhy byly kladeny na schopnost detekce virů a také na kritérium, které ukazovalo, jak daný antivirový program zatěžuje počítač.

Pomocí metody váženého součtu bylo zjištěno, že na základě zvolených kritérií je optimální volbou pro ochranu počítače antivirový program Kaspersky AntiVirus 2012. Tento produkt firmy Kaspersky Lab je, stejně jako ostatní testované programy, plně podporován v českém jazyce a cena licence na jeden rok je 876 Kč včetně DPH. Dále má velmi vysokou schopnost detekce škodlivého kódu (98,3%), málo zatěžuje počítač (188,9 kladných bodů z 200) a pro svou instalaci potřebuje 480 MB na disku. Této srovnávací metody se také zúčastnily další antivirové programy a to ESET NOD32 Antivirus 5, Norton AntiVirus 2012 a TrustPort Antivirus 2012, ale tyto programy nedosáhly takových výsledků jako produkt firmy Kaspersky Lab.

9 Seznam literatury

1. HEINIGE, Karel. *Viry a počítače*. Brno: Mobil Media a.s., 2001. PCWorld Edition. ISBN 80-86593-02-9.
2. SZOR, Peter. *Počítačové viry*: *analýza útoku a obrana*. Brno: Zoner Press, 2006. ISBN 80-86815-04-8.
3. ČADA, Ondřej. *Ochrana proti počítačovým virům*. 2. dopl. vyd. Praha: PLUS, 1992. ISBN 80-85297-13-2.
4. HÁK, Igor a Josef ZELENKA. *Ochrana dat*: *škodlivý software*. Hradec Králové: GAUDEAMUS, 2005. ISBN 80-7041-594-0.
5. ZELENKA, Josef a Pavel BAUDIŠ. *Antivirová ochrana*. Praha: PLUS, 1996. ISBN 80-85297-74-4.
6. JALŮVKA, Josef. *Moderní počítačové viry*: *Podstata, prevence, ochrana*. 2. akt. vyd. Praha: Computer Press, 2000. ISBN 80-7226-402-8.
7. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
8. BITTO, Ondřej. *Jak zabezpečit domácí malou síť Windows XP*: *Účty, práva, firewally, antiviry a další nástroje*. Brno: Computer Press, 2006. ISBN 80-251-1098-2.
9. KRÁL, Mojmír. *Bezpečnost domácího počítače*: *prakticky a názorně*. Praha: Grada Publishing, a.s., 2006. ISBN 80-247-1408-6.
10. BROŽOVÁ, Helena, Milan HOUŠKA a Tomáš ŠUBRT. *Modely pro vícekriteriální rozhodování*. Praha: Česká zemědělská univerzita v Praze, 2009. ISBN 978-80-213-1019-3.
11. VŠETEČKA, Roman. Viry jsou staré několik desetiletí. Chcete znát jejich vývoj?. *IDnes* [online]. 4.11.2004 [cit. 2012-03-25]. Dostupné z: http://technet.idnes.cz/tec_technika.aspx?r=bezpecnost&c=A041103_5285981_bezpecnost.

12. KOLÁČEK, Michal a Roman VŠETEČKA. Počítačová havěť: vývoj a rozdělení malware. *Svět hardware*: *vše ze světa počítačů* [online]. 12.2.2009 [cit. 2012-03-25]. Dostupné z: http://www.svethardware.cz/art_doc-59D3ACB5ABE0B778C125755A007ABA09.html.
13. ŠVIDRNOCH, Roman. Lidé nám platí dobrovolně a rádi, říká duchovní otec antiviru avast!. *IDnes* [online]. 11.2.2009 [cit. 2012-03-25]. Dostupné z: http://ekonomika.idnes.cz/lide-nam-plati-dobrovolne-a-radi-rika-duchovni-otec-antiviru-avast-1co-/ekonomika.aspx?c=A100210_130718_ekonomika_ven.
14. ANTIVIROVÉ CENTRUM. PROČ ZROVNA AVAST!?. *Antivirové centrum* [online]. © 1998 - 2012 [cit. 2012-03-25]. Dostupné z: http://antivirovecentrum.cz/avast.aspx.
15. ANTIVIROVÉ CENTRUM. PROČ AVG?. *Antivirové centrum* [online]. © 1998 - 2012 [cit. 2012-03-25]. Dostupné z: http://www.antivirovecentrum.cz/avg.aspx.
16. AVG. Profil společnosti. *AVG* [online]. © 2012 [cit. 2012-03-25]. Dostupné z: http://www.avg.com/cz-cs/profil-spolecnosti.
17. ESET. Profil. *Eset* [online]. © 1992 - 2012 [cit. 2012-03-25]. Dostupné z: http://www.eset.cz/cz/o-nas/spolecnost/.
18. KASPERSKY. O nás. *Kaspersky Lab* [online]. © 1997 - 2009 [cit. 2012-03-25]. Dostupné z: http://www.kaspersky.cz/o-nas/.
19. ANTIVIROVÉ CENTRUM. PROČ ZROVNA PRODUKTY SPOLEČNOSTI MCAFEE?. *Antivirové centrum* [online]. © 1992 - 2012 [cit. 2012-03-25]. Dostupné z: http://www.antivirovecentrum.cz/mcafee.aspx.
20. SYMANTEC. Zaměstnání. *Symantec* [online]. © 1995 - 2012 [cit. 2012-03-25]. Dostupné z: http://www.symantec.com/cs/cz/about/careers/.
21. TRUSTPORT. Profil společnosti. *TrustPort* [online]. © 2012 [cit. 2012-03-25]. Dostupné z: http://www.trustport.com/cz/o-trustportu/profil-spolecnosti.
22. ESET. ESET NOD32 Antivirus 5. *Eset* [online]. © 1992 - 2012 [cit. 2012-03-25]. Dostupné z: http://www.eset.cz/cz/domacnosti/produkty/antivirus/.
23. AV COMPARATIVES. On-demand detection of malicious software. *AV Comparatives* [online]. 27.9.2011 [cit. 2012-03-25]. Dostupné z: http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf.

24. AV COMPARATIVES. Performance test. *AV Comparatives* [online]. 8.12.2011 [cit. 2012-03-25]. Dostupné z: http://www.av-comparatives.org/images/stories/test/performance/performance_nov_2011.pdf.
25. NORTON. Norton™ AntiVirus. *Norton* [online]. ©1995 - 2012 [cit. 2012-03-25]. Dostupné z: http://cz.norton.com/antivirus/.
26. KASPERSKY. Kaspersky Anti-Virus 2012. *Kaspersky Lab* [online]. © 1997 - 2009 [cit. 2012-03-25]. Dostupné z: http://www.kaspersky.cz/produkty/domaci-uzivatele/kaspersky-anti-virus/
27. TRUSTPORT. TrustPort Antivirus. *TrustPort* [online]. © 2012 [cit. 2012-03-25]. Dostupné z: http://www.trustport.com/cz/produkty/trustport-antivirus#vlastnosti.

10 Seznam tabulek a grafů