Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Viry a antiviry ve světě počítačů

Jan Kliment

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačního inženýrství

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Kliment Jan

Podnikání a administrativa

Název práce

Viry a antiviry ve světě počítačů

Anglický název

Viruses and Antiviruses in the World of Computers

Cíle práce

Cílem práce je srovnání vybraných antivirových programů a následné vyhodnocení nejvhodnějšího antiviru pro studenty třetího ročníku studující obor Podnikání a administrativa na České zemědělské univerzitě v Praze.

Metodika

Bakalářské práce bude obsahovat charakteristiku a rozdělení škodlivého softwaru. Dále bude vybráno a popsáno několik antivirových programů, a poté vyhodnocen nejlepší z nich za pomoci vícekriteriální analýzy variant a předem zvolených kritérií a jejich vah. Velikost vah daných kritérií bude měřena za pomoci preferencí studentů třetích ročníků na České zemědělské univerzitě.

Harmonogram zpracování

Příprava a studium odborných zdrojů, definování cílů – 12/2012 – 06/2013
Návrh konceptu práce – 06/2013 – 08/2013
Dotazování se studentů, sběr dat – 07/2013 – 08/2013
Zhodnocení výsledků a vytvoření závěru dotazování – 08/2013 – 10/2013
Práce se získanými informacemi – 9/2013 – 12/2013
Tvorba finálního dokumentu práce 12/2013 – 03/2014
Odevzdání práce – 03/2014

Rozsah textové části
30 – 40 stran

Klíčová slova
vir, antivirový program, software, NOD32, Avast!, BitDefender, bezpečnost, červ, trojský kůň

Doporučené zdroje informací

HEINIGE, Karel. Viry a počítače: Průvodce světem počítačů. Praha: Computer Press, 2001. 80 s. ISBN 80-86593-02-9.

OOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Praha: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

ZELENKA, Josef a Pavel BAUDIŠ. Antivirová ochrana. Praha: PLUS, 1996. 183 s. ISBN 80-86297-74-4.

KRÁL, Mojmír. Bezpečnost domácího počítače - prakticky a názorně. 1. vydání. Praha: Grada, 2006. 336 s. ISBN 80-247-1408-6.

PALIKNEROVÁ, Daniela et al. Psychologie pro ekonomy a manažery. 3. vydání. Praha: Grada Publishing, a.s., 2012, 264 s. ISBN 978 80 247 3809 3.

ŠUBRT, Tomáš et al. Ekonomicko-matematické metody. Plzeň: Aleš Čeněk, 2011, 351 s. ISBN 978-80-7380-345-2.

Vedoucí práce
Pícka Marek, Ing., Ph.D.

Termín odevzdání
březen 2014

Elektronicky schváleno dne 19.2.2014
Ing. Martin Pelikán, Ph.D.
Vedoucí katedry

Elektronicky schváleno dne 28.2.2014
Ing. Martin Pelikán, Ph.D.
Děkan fakulty

V Praze dne 27.2.2014

Čestné prohlášení

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

V Praze dne 17. 3. 2014 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Marku Píckovi Ph.D. za cenné rady a konzultace při vytváření této bakalářské práce, dále bych chtěl poděkovat všem studentům, kteří se podíleli na vyplňování dotazníků potřebných ke zpracování této práce.

Viry a antiviry ve světě počítačů

Viruses and Antiviruses in the World of Computers

Souhrn:

Tato bakalářská práce se zabývá hodnocením vybraných antivirových programů a následného vyhodnocení nejlepšího z nich.

Práce se skládá ze dvou částí. První část práce se zabývá počítačovými viry a antiviry, kde je zahrnuto dělení virů podle různých hledisek, například dělení podle umístění v paměti počítače. Kromě problematiky počítačových virů a antivirů je zde stručně charakterizována dotazníková metoda. Na konci teoretické části práce je pojednáno o metodách vícekriteriální analýzy variant, použitých pro vyhodnocení nejlepšího antiviru.

Druhá část práce obsahuje samotnou vícekriteriální analýzu variant, a to metodu váženého součtu. Je vybíráno ze čtyř antivirových programů, a to AVG Antivirus 2014, Avast! Pro Antivirus 2014, Eset NOD32 Antivirus 7 a BitDefender Antivirus Plus. Váhy kritérií jsou zde určeny bodovací metodou na základě vyhodnocení dotazníků. Dotazníky vyplnili studenti třetích ročníků studující obor Podnikání a administrativa na České zemědělské univerzitě v Praze. Právě těmto studentům je určeno závěrečné doporučení antiviru, který v analýze dosáhl nejlepších výsledků.

Summary:

This bachelor thesis deals with evaluation of selected antivirus software and subsequent evaluation of the best of them.

The thesis consists of two parts. The first part deals with computer viruses and antivirus programs which includes distribution of viruses according to various terms, such as division by location in the computer's memory. In addition to the problems of computer viruses and antivirus programs is briefly described questionnaire method. At the end of the theoretical part of the thesis deals with methods of multi-criteria analysis of options used evaluate the best antivirus.

The second part of the thesis contains the multi-criteria analysis of options, the Weighted Sum Approach method. It is selected from the four anti-virus programs,

AVG Antivirus 2014, Avast! Pro Antivirus 2014, Eset NOD32 Antivirus 7 and BitDefender Antivirus Plus. Criteria weights are determined by a Scoring Method based on the evaluation of the questionnaires. Questionnaire filled in by students third year who study fields of Business and Administration at the Czech Agricultural University in Prague. To these students is determined the final recommendation antivirus that analysis achieved the best results.

Klíčová slova: vir, antivirový program, software, NOD32, Avast, BitDefender, červ, bezpečnost, trojský kůň

Keywords: virus, antivirus, software, NOD32, Avast, BitDefender, worm, safety, trojan horse

Obsah

1 Úvod

Na naší planetě existuje velice široké spektrum částic na pomezí mezi živými organismy a neživou přírodou, které mohou být klasifikovány jako viry. Napadají své hostitele a koexistují s nimi, dále se v jejich tělech množí a snaží se napadat i všechny potenciální hostitele kolem sebe. Hlavní úloha biologického viru je snaha přežít. Fakt, že napadenému hostiteli způsobí újmu, která může být zanedbatelná, ale může být pro hostitele dokonce i smrtelná, je už jen výsledek úmyslu viru přežít a množit se. Avšak bez existence hostitele by mnohé viry přežít nedokázaly.

Tak jako ve světě lidí, i ve světě počítačů existuje velice pestrá paleta různých druhů virů, které útočí pomocí odvětví výpočetní techniky. Původní záměr virů byla sebereplikace, avšak postupem času se tyto záměry poněkud pozměnily. Stále je podstatné množení sama sebe a napadení co nejvyššího počtu obětí (počítačů), ale přibyly také záměry poněkud vychytralejší, např. techniky, jak z napadených počítačů vymámit data a informace, které vedou k sebeobohacení na úkor napadeného, nebo destrukce systému počítače, atd. Při napadení virem může dojít až k totální destrukci napadeného objektu.

V biologickém světě se viry léčí především vakcínami, které vyhledají škodlivé kódy ukryté v jejich tělech, dále tyto kódy eliminují a nakonec, je-li to možné, hostitele vyléčí. Stejně je tomu i ve světě počítačovém, s rozdílem, že zde tyto “vakcíny” nazýváme tzv. „antiviry“ neboli antivirové programy. Zde už záleží jen na uživateli, jaký antivirový program si pro svou ochranu zvolí. Vybírá si podle určitých kritérií, např. ceny, preferencí, statistiky průměrné detekce virů, atd.

2 Cíl práce a metodika

2. 1 Cíl práce

Cílem této bakalářské práce je vyhodnocení nejvhodnějšího antivirového programu dle preferencí studentů za pomoci vícekriteriální analýzy variant.

Dalším cílem práce je podat studentům doporučení nejlepšího a nejvhodnějšího antivirového programu, jenž dosáhne nejlepších výsledků v analýze.

K dosažení těchto cílů bude vytvořen dotazník, který zjistí váhy kritérií na základě preferencí studentů třetího ročníku oboru Podnikání a administrativa České zemědělské univerzity v Praze. Za pomoci takto zjištěných vah kritérií budou hodnoceny zvolené antivirové programy.

2. 2 Metodika

Práce je rozdělena do dvou částí. V první části se práce zabývá teoretickým rozdělením škodlivého softwaru a dalšími útoky na počítače uživatelů. Z nastudované literatury jsou vypsány základní druhy škodlivých kódů a útoků na systémy počítačů. Dále je v této části práce uvedena a rozdělena forma ochrany proti těmto škodlivým kódům a útokům.

Druhá část práce se zabývá praktickým zpracováním dané problematiky. Jsou zde stručně charakterizovány předem zvolené antivirové programy. Vše za pomoci nastudované literatury a internetových stránek daných společností, které tyto programy prodávají a poskytují uživatelům.

Formou dotazníkového šetření bude zjištěno, jaké vlastnosti u antivirových programů preferují studenti třetího ročníku oboru Podnikání a administrativa České zemědělské univerzity v Praze. Na základě dotazníku budou bodovací metodou zvoleny váhy jednotlivých kritérií. Dále pomocí metody váženého součtu, začleňující se do vícekriteriální analýzy variant bude vybrán nejlepší a nejvhodnější antivirový program pro tyto studenty.

Dotazováni budou studenti z oboru Podnikání a administrativa, proto i výsledek vícekriteriální analýzy variant bude vztažen pouze na tyto studenty, aby nedošlo k potenciálnímu zkreslení výsledku z důvodu možných odlišných preferencí studentů na různých fakultách České zemědělské univerzity.

3 Teoretická východiska

3. 1 Historie

První zmínka o programu, který dokáže reprodukovat sama sebe, byla publikována již v roce 1949. Autorem byl John von Neumann, jenž v publikaci vysvětloval, jakou konstrukci může mít program, aby byl schopen sebereplikace.

Jedním z mnoha průkopníků v oblasti počítačových virů byl Dr. Frederik Cohen, jenž v roce 1983 sestrojil první samomnožící se program, který byl však neškodný a dokázal pouze sám sebe replikovat. Dr. Frederik Cohen poprvé použil pojem "počítačový vir". [3]

Další neškodný počítačový vir, jenž se šířil ve veřejné síti, se nazýval Elk Cloner. Sestrojil ho Richard Skrenta a tento vir se šířil pomocí disket. Úsměvná může být skutečnost, že nejhorší věc, kterou vir vykonával, bylo, že po 50. spuštění se zobrazovala báseň. [4]

V 80. letech 19. století se začala zvyšovat popularita počítačů, vznikali i první trojské koně v důsledku rozšíření výroby programů od soukromých osob.

V roce 1986 byl vytvořen vir Brain. Jeho autory byli bratři Basit a Amjad Farooq Alviovi. Vir napadal 360 KB diskety. Jeho úspěšnost v šíření spočívala ve společenské nepřipravenosti na virovou problematiku. Poté se tvorba škodlivého softwaru velice rozšířila. Známé starší viry, jež stojí za zmínění jsou např. vir Jerusalem, vir Morris, červ HI.COM, trojský kůň AIDS, polymorfní vir Chameleon. Na přelomu tisíciletí to byl makrovir Mellisa nebo vir ILOVEYOU. [2]

Postupem času se viry vyvíjely stejně rychle jako např. internet, byly stále propracovanější, zákeřnější a rychlejší. Všichni uživatelé počítačů museli být každodenně ve střehu.

3. 2 Dělení škodlivého softwaru

Škodlivý software se většinou jedním slovem nazývá malware. Tento výraz vznikl spojením dvou slov, a to: "malicious" a "software". "Malicious" se do českého jazyka překládá jako "zákeřný", tudíž název vystihuje spíše záměr autora, než specifikaci

vlastností samého programu. Pod názvem malware se skrývá souhrn pojmů jako počítačový vir, trojský kůň, počítačový červ, spyware[1], advare[2], apod. [5]

Malware se dělí na několik jednotlivých druhů. Nejprve bude uvedeno nejzákladnější dělení škodlivého softwaru, a to: počítačové viry, počítačové červi a trojské koně.

3. 2. 1 Počítačové viry

Pojem počítačový vir je vzhledem k jistým podobnostem odvozen od biologického viru, který napadají těla živočišných organismů. Vir je schopen sebereplikace (množení sama sebe), ovšem pouze za přítomnosti hostitele, k němuž je připojen. V počítačovém světě mohou být hostiteli například spustitelné soubory, systémové oblasti disku, nebo soubory, které lze vykonat za použití specifických aplikací (např. dokumenty Microsoft Word). Počítačový vir se dokáže šířit sám bez vědomí uživatele. Díky této analogii se někdy proces šíření viru nazývá infekce a napadený soubor se nazývá hostitel.

Co to počítačový vir je? Frederick B. Cohen definoval počítačový virus jako: *"Program, který může infikovat jiný počítačový program takovým způsobem, že do něj nakopíruje své tělo, čímž se infikovaný program stává prostředkem pro další aktivaci viru."* [1, s. 4]

Vytváření počítačových virů má mnohé důvody, které mohou mít destruktivní, ale i neškodné následky. Destruktivní viry mohou poškodit počítač zahlcením prostoru na disku nebo průchodnosti internetových serverů, mazáním, přepisováním nebo likvidováním dat uložených na pevném disku. Naproti tomu viry, u kterých nelze jednoznačně určit, z jakého důvodu byly vytvořeny, jelikož útočníkovi nepřinášejí užitek, jsou nejrozšířenější a jejich počet je nejpočetnější. Takové viry pouze obtěžují uživatele například žertovnými nebo propagačními nápisy, zpomalují počítač, vyžadují určité činnosti, apod.

Tak jako organický vir, tak i vir počítačový je programován tak, aby jeho velikost byla co nejmenší. Čím je vir menší, tím lépe unikne pozornosti běžného uživatele. Velikost běžného počítačového viru se pohybuje v rozmezí několika bytů až po desítky kilobajtů. [1]

[1] Program, využívající internetu k odesílání dat z počítače, bez vědomí uživatele
[2] Produkty, které zobrazují reklamní oznámení, např. bannery, pop-up okna, atd.

3. 2. 1. 1 Rozdělení dle umístění v paměti

Zde jsou viry rozděleny z hlediska, zda pro napadání systému počítače využívají paměť systému či nikoliv.

Rezidentní viry

Rezidentní vir je umístěn v paměti počítače ilegálně a bez vědomí uživatele. Využívá ji pro své šíření. Nejčastěji rozlišujeme dva typy rezidentních virů. Prvním z nich je souborový vir, jenž se stává rezidentním při prvním spuštění daného infikovaného souboru. Druhým typem je boot vir, jenž se stává rezidentním po prvním zavedení systému z napadeného boot sektoru.

Vir se do paměti počítače umisťuje takovým způsobem, že vyhledá či vytvoří volné místo v paměti systému. Takové volné místo v paměti se musí vyznačovat především dostatečnou velikostí a bezpečností. Jestliže se jedná o boot vir, není zde příliš na výběr, kam by se mohl uložit, jelikož instalace viru do paměti probíhá před okamžikem, než je zaveden operační systém. Boot vir zmíněný problém řeší nejčastěji tak, že uměle sníží velikost základní paměti a infikuje tu část, která je pro operační systém nepřístupná. Tato varianta infikace je však velice snadno zjistitelná, jestliže je uživatel schopen rozpoznat netypickou velikost základní paměti.

Významnou výhodou rezidentního viru je to, že si nemusí hledat program vhodný k napadení. Postačuje sledování činnosti uživatele a na programy, se kterými uživatel pracuje, útočit. [1]

Nerezidentní

Nerezidentní viry jsou opakem virů rezidentních. Tato skupina virů se nazývá také “viry přímé akce”. Nevyužívají paměť systému pro své šíření, naopak postačuje, jsou-li tyto viry spuštěny s hostitelským programem. Následně provedou pro uživatele nežádoucí činnost, nejčastěji sebereplikaci, a následně předají řízení zpět programu, jenž je hostí. Nerezidentní viry svou replikací napadají všechny vhodné soubory v adresáři. Mohou napadat soubory postupně nebo všechny současně.

Většina nerezidentních virů je především souborového typu. Jelikož je zde absence uložení sama sebe v paměti systému, nemohou tyto viry využívat všech moderních technik, které používají právě viry rezidentní, což představuje především to, že se nemohou natolik úspěšně před uživatelem skrývat a nejsou schopny analyzovat postup jejich vyhledání. [6]

3. 2. 1. 2 Typy počítačových virů

Zde jsou viry rozděleny podle toho, jakým způsobem napadají cílový počítač, tedy dělení podle napadených oblastí systému.

Boot viry

Jedná se o viry, které napadají systémové oblasti disku. Tuto oblast obsahuje každá disketa nebo pevný disk. Napadení tohoto sektoru virem, představuje zavedení a spuštění viru při každém startu počítače.

Boot viry jsou poměrně staré. Mnohdy mají svou velikost pouze do 512 bitů. Ukládají se do boot sektorů, což laicky řečeno znamená, jestliže je vir přítomen v boot sektoru na pevném disku, při startu počítače se jako první zavede vir a až poté BIOS[3] atd., zároveň každá disketa vložená do počítače (ať již pro čtení, nebo pro zapisování), je okamžitě virem také napadena.

Jestliže je vir přítomen v boot sektoru diskety, která byla vložena do počítače, a ten byl restartován, zároveň bychom měli na počítači nastavenou sekvenci BIOSu A: → C:, poté by byl opět zaveden jako první vir, poté BIOS a následně start systému počítače. Je zde popsáno „zavádění disket“, což v dnešní době není zcela obvyklé, z toho vyplývá, že je zde uvedena nedávná minulost, kde ještě nebyl určen postup zavedení OS[4] a počítač se snažil vždy zavádět systém nejprve z disketové mechaniky.

Jaké z toho plyne ponaučení? Mít na počítači nastavenou sekvenci BIOSu C: → A:. Tím by se mělo zamezit síření boot virů. [1, 6]

Souborové viry

Souborové viry využívají techniku, kde hlavním hostitelem jsou spustitelné soubory (EXE, COM, SCR, atd.), batové soubory (BAT), nebo ovladače (SYS).

Tyto viry nejčastěji napadají soubory, které může uživatel spustit sám (COM, EXE). Jsou ale i takové souborové viry, které napadají soubory DRV, DLL, ZIP, RAR nebo CAB. Souborové viry mohou být rozděleny podle metody infekce na přepisující, parazitické a doprovodné. [1]

V případě přepisujících virů jde ve většině případů o nerezidentní viry, pro které je typické přepisování obsahu (kódu) konečného souboru vlastním kódem. Tím se zničí

[3] Používá se především při startu počítače pro inicializaci a konfiguraci připojených hardwarových zažízení
[4] Operační systém

původní obsah souboru, a ten dále není schopen původní funkce a není možné ho opravit. Jestliže se uživatel rozhodne infikovaný soubor spustit, pouze se aktivuje vir a pravděpodobnost, že se rozšíří do dalších spustitelných souborů, je velmi vysoká. Pro odstranění tohoto viru musí být napadený soubor kompletně vymazán z pevného disku.[7]

Parazitické souborové viry přikládají vlastní programové kódy do kódů napadených programů. Viry mají tři možnosti.

První možností je připojení se na začátek kódu napadeného programu. Je to téměř totožná technika jako u připojujících virů s tím rozdílem, že napadený soubor zůstává nepoškozen.

Druhou možností je připojení se na konec kódu napadeného programu. Tuto možnost využívá většina souborových virů. Kód viru prodlouží celý kód infikovaného programu. Tento způsob infekce má pro vir tu výhodu, že soubor nadále vykonává svou činnost. Tzn., jestliže chce uživatel otevřít program, vir zde vytvoří “most” na konec kódu programu, kde je začátek kódu viru. Vir se realizuje a vytvoří druhý “most” na začátek kódu programu, který se bez povšimnutí uživatele spustí.

Třetí možností je snaha viru dostat se rozčleněně do jednotlivých míst v souboru, jenž program nevyužívá. Nedochází zde ke zničení programu, ani k prodloužení kódu programu. Pro antivirový program je velice náročné takový vir zjistit, zneškodnit a program (soubor) vrátit do původního stavu. [8]

Doprovodné viry mají omezenou působnost na OS DOC. Využívají vlastnost systému, že jestliže MS-DOS vysílá požadavek na zavedení programu, snaží se nejprve spustit soubor s příponou .com, a až poté soubor s příponou .exe. Vir vytváří své kopie s příponou .com k již existujícím souborům s příponou .exe, a to se stejným pojmenováním. Spuštění souboru začíná zavedením doprovodného viru s příponou .com, který vykoná útočnou činnost, a až poté se spustí původní program.

Likvidace těchto virů je velice snadná záležitost a ve většině případů nehrozí žádná ztráta dat. Stačí vir s příponou .com vymazat z počítače. Na druhou stranu je zde úskalí v tom, že vir nijak nemodifikuje kód souboru, tudíž je velice obtížné vyhledání viru antivirovým programem. [7]

Makroviry

Makroviry se síří pomocí datových souborů. Jedná se o viry skládající se z maker, které se tvoří pomocí programovacích jazyků, a ty mají vlastnost hýbat s daty aplikace a přitom i s makry, které jsou s těmito daty propojeny. Makroviry jsou makra, které mají možnost kopírovat sama sebe do jiného souboru (i několikanásobně).

Makroviry mohou provádět jakoukoli destruktivní činnost, mohou mazat či jinak poškozovat datové soubory. Mohou obsahovat i běžný vir, který infikuje ostatní soubory. Zastaralé antivirové programy je rozpoznávají a vyhledávají velice obtížně. Novější antivirové programy již zmíněný nedostatek nemají.

Vhodný antivirový program je nejlepší ochrana proti makrovirům. Kontrola přítomnosti makrovirů v dokumentu je možná občasnou kontrolou samotných maker daného dokumentu a eliminace všeho podezřelého.

Makroviry se mohou objevit tam, kde existuje makrojazyk a přítomnost automatického zavádění některých maker, např. během otevírání či zavírání souborů.

Makrovir je jako první schopen se šířit mezi různými typy počítačů (např. PC a MAC), protože makroviry mají schopnost šíření se na odlišných operačních systémech. [8]

3. 2. 1. 3 Další typy a vlastnosti počítačových virů

Adresářové viry

"Tyto viry modifikují vstupy adresářové tabulky tak, že virus je zaveden do paměti a spuštěn dříve než program, který uživatel chce spustit." [1, s. 54]

Adresářové neboli clusterové viry tvoří poměrně malou skupinu virů. Na disku se zpravidla vyskytuje pouze jeden exemplář. Pro eliminaci tohoto viru postačuje nalezení a překopírování do jiného adresáře a změna přípony tak, aby neobsahovala .com nebo .exe. Příkladem tohoto druhu viru může být například DIR II[5].

Kódované viry

Kódované viry měly původně jeden určitý záměr, a to kódováním znepřehlednit vlastní kód viru, jenž je velice důležitý při tvorbě antivirové databáze. Navíc, napadené programy bylo velice těžké uzdravit, jelikož kód viru byl uložen na samotném začátku

[5] Jedná se o rezidentní vir původem z Indie.

programu, zakódován pomocí určitého triviálního algoritmu, a teprve těsně před virem byla malá dekódovací smyčka.

Starší viry tohoto typu byly téměř konstantní, avšak novější generace v sobě již obsahovala proměnnou, která umožňovala, aby každý exemplář viru obsahoval jedinečný kód pouze se stejnou dekódovací smyčkou na začátku, což pro antivirové programy pochopitelně představovalo komplikace při vyhledávání těchto virů. [1]

Polymorfní viry

Tato skupina virů z části navazuje na předchozí skupinu kódovaných virů. Hlavní znak polymorfních virů je ten, že žádné ze dvou kopií virového těla nejsou zcela stejné (mají rozdílný kód).

"*Typickou činností je vkládání prázdných instrukcí, přehazování pořadí výkonu částí kódu nebo záměna sekvencí kódu jinými sekvencemi s ekvivalentní funkcí.*" [1, s. 11]

Tyto skutečnosti způsobují, že polymorfní viry nelze detekovat podle sekvencí, či podle klasických kontrolních součtů (CRC[6]).

Stealth viry

Viry používající pro svou ochranu před detekcí antivirovým programem tzv. stealth[7] techniky. Princip spočívá v kontrole některých služeb operačního systému, přes který je vir schopen ovlivňovat kontrolní operace. To v podstatě znamená, že je-li stealth vir aktivní, je nemožné jej zjistit, používá-li se standardních systémových služeb.

Stealth viry provádějí své maskování v reálném čase v závislosti na požadavcích kladených operačnímu systému. Viry jsou schopny dezinfikovat program, kdykoli je načítán do paměti, a poté program opět infikovat. To způsobuje, že i po použití antivirového programu není známa přítomnost viru v počítači.

Antivirové programy v dnešní době využívají tzv. anti-STEALTH techniky. Jde o to, že nepoužívají standardní systémové služby, které mohou být zavirované. Namísto toho antivirový program vyhledává původní obsah požadovaných služeb v paměti ROM. Jestliže je antivirový program úspěšný, dokáže stealth viry jednoduše zjistit a zneškodnit. [1, 8]

[6] Cílem CRC je detekování chyb v datech.
[7] Překládáno do českého jazyka jako neviditelný nebo obtížně zjistitelný. Snaha co nejvíce omezit možnost zjištění pomocí různých detekčních prostředků.

Metamorfní viry

"*Metamorfismus je polymorfismus těla.*" [10, s.16]

Metamorfní vir nemá decryptor[8], ani konstantní tělo viru. Přesto je schopen produkovat další generace, přičemž každý nově vyprodukovaný vir je odlišný od svého předchůdce. Tělo viru je uloženo v podobě kódu, kde jsou uložena i data. Vir nepoužívá žádné datové oblasti vyplněné konstantním řetězcem, a proto je velice nedetekovatelný běžnými způsoby, které používají antivirové programy. [10]

Multipartitní viry

Multipartitní viry kombinují více způsobů šíření. Např. boot vir v kombinaci se souborovým, souborový vir a makrovir, makrovir a skriptový vir, atd. Tyto viry mohou infikovat odlišné oblasti disku (nejčastěji zaváděcí sektor disku a spustitelný soubor).

Jakmile má vir počítač pod kontrolou, nemá zapotřebí útočit na něj dále, útočí již pouze na soubory směrem k síťovým diskům nebo výměnným médiím. Jako nejlepší příklad tohoto druhu viru může být vir OneHalf[9] nebo Starship[10]. [8]

Retro viry

Retro viry neboli odvetné viry se snaží obejít činnost, v lepším případě (pro viry) totálně znemožnit činnost antivirových programů. Toho se snaží dosáhnout mazáním nebo deaktivací antivirů, vhodnou úpravou virové databáze tak, aby antivirový program nebyl v budoucnu schopen vir odhalit, popřípadě vypínáním rezidentních ochran. [1]

Skriptové viry

S příchodem Windows Script Host se objevil problém. Skriptovací jazyk Visual Basic obsahuje možnosti, kde vytvoření viru, který se snadno šíří, je velice jednoduché. Elektronická pošta je pro šíření těchto virů nejlepší alternativa.

Skripty mohou být vloženy přímo do HTML kódů stránek. Jestliže je internetový prohlížeč nevhodně nastaven[11], je zde možnost samovolné aktivace viru. [6]

---

[8] Decript = dešifrovat
[9] Počítačový virus původem ze Slovenska z roku 1994, zvaný také jako Košický mor.
[10] Multipartitní virus původem z bývalého Sovětského svazu z roku 1991.
[11] Nevhodné nastavení je v některých případech zároveň standardním nastavením internetového prohlížeče (Internet Explorer)

Tunelující viry

Tunelující viry vyhledávají originální vektory přerušení a volají je přímo, čímž se vyhýbají aktivitě antivirů, které v počítači detekují pokusy o volání vektorů přerušení.

Běžné tunelující metody jsou například: skenování v paměti, trasování pomocí ladicího rozhraní, nebo na bázi emulace kódů, atd. [9]

3. 2. 2 Trojské koně

Program, jenž navenek navozuje dojem užitečnosti. Trojský kůň může být součástí užitečného programu, který si uživatel stáhne, nainstaluje, nebo pouze spustí ve svém počítači. Poté program buď vůbec nevykonává svou činnost a trojský kůň se dostane do počítače, nebo program funguje správně, může být i užitečný a uživateli prospěšný, ale v pozadí realizuje nepozorovaně nějaký druh destrukce (např. maže soubory, formátuje pevný disk, narušuje soukromí uživatele skrytou komunikací přes internet, apod.).

Trojský kůň je buď naprogramovaný jako původní aplikace, nebo je škodlivý kód přidán do již existujícího programu, nebo je trojský kůň samotným instalačním souborem samotného programu. Na rozdíl od virů není trojský kůň schopen sebereplikace a infekce souborů. V současnosti je nejrozšířenější forma trojského koně soubor typu EXE, který obsahuje pouze samotné “tělo” tohoto škodlivého kódu a zároveň není připojen k žádnému hostiteli. Z toho vyplývá, že pro likvidaci takového trojského koně se musí smazat dotyčný soubor. [1]

3. 2. 2. 1 Formy trojských koňů

Trojské koně mají různé vlastnosti, způsoby napadení cílového systému počítače, důsledky pro uživatele, atd. Zde je popsáno základní členění trojských koňů.

Pasword-stealing

Tento typ trojského koně je program, jenž sleduje a zaznamenává jednotlivé stisky kláves na počítači. Poté obvykle následuje odeslání těchto informací samotným tvůrcům trojského koně. Ti tak mohou získat velice citlivé informace, které by uživatel nikdy nezveřejnil, např. hesla k účtům. Zde nejsou v bezpečí ani ta nejdůmyslnější hesla, která si uživatelé vytváří podle pouček nebo příruček, které radí, jak vytvořit neprolomitelná hesla. Dále například detaily o kreditní kartě, logy z chatu a další citlivé informace. [6]

Destruktivní

Primární úkol tohoto trojského koně je mazání dat uložených na pevném disku nebo úplné zformátování disku. [6]

Backdoor

Jde o program, který umožňuje útočníkovi úplnou kontrolu nad počítačem uživatele. Jde tedy o vzdálenou správu počítače s přístupem k souborům, datům o síťových a internetových účtech, soukromé konverzaci, atd. Útočníci mohou nakládat s počítačem jakkoli chtějí, včetně zasílání, přijímání, zavádění a mazání souborů, restart počítače, zobrazování dat, apod. [6]

Dropper

Jedná se o program, nejčastěji s příponou .exe, který je určen k tomu, aby do cílového systému nainstaloval virus. Po spuštění trojského koně se do systému dostane další škodlivý software, jenž je většinou velice dobře zakódován v tomto dropperu způsobem, aby nebyl detekován antivirovým programem, ani žádnou jinou běžnou metodou obrany systému. [6]

Downloader

Trojský kůň určený ke stahování z internetu, z pevně definovaných adres (URL), buď další součásti sama sebe, což mu dodá větší kontrolu nad napadeným systémem, nebo další škodlivý software. Stažení jediného downloaderu může odstartovat totální destrukci systému tím, že bude stahovat další downloadery, které opět stáhnou další škodlivý software, až do okamžiku, kdy bude systém zahlcen nebo zničen. [6]

Proxy trojan

Díky tomuto trojskému koni se napadený počítač stane proxy serverem. To umožňuje útočníkovi využívat tento počítač například pro rozesílání nevyžádané pošty, jako anonymní telnet stanici[12], irc[13], atd. Tyto služby poté umožňují např. nákup na odcizenou platební katru a další protizákonné činnosti. Útočník je v naprosté anonymitě a vše se odehrává na počítači a síti oběti. [6]

[12] Umožňuje navázat nezabezpečené spojení mezi pracovní stanicí a hostitelských serverem.
[13] Internet Realy Chat byla jednou z prvních možností komunikace v reálném čase po internetu.

3. 2. 3 Počítačové červi

Program, jenž ke svému síření nepotřebuje hostitele, to je hlavní rozdíl oproti počítačovému viru. Počítačový červ nepotřebuje ke své existenci zásah uživatele. Výjimkou jsou červi, kteří se šíří pomocí e-mailové pošty. Červ se šíří pomocí síťových paketů, přičemž využívá komunikační propojení s dalšími počítači. Šíření červa je postaveno na zneužívání konkrétních bezpečnostních děr operačního systému.

Počítačoví červi s sebou přináší, kromě svého vlastního šíření, mnohé nepříjemnosti, např. zneprovoznění počítače, nebo jeho součástí, likvidace souborů či složek, šifrování uživatelských souborů, skenování počítače s úmyslem získání citlivých dat či tvorbu "backdoor", což většinou vždy bývá cesta k další infikaci počítače. Červ s sebou téměř vždy nese nestandardní chování systému. [1]

Za nejznámější incident Internetu způsobený počítačovým červem by mohl být uveden Lovsan/Blaster, jenž se na internetu objevil 11. 8. 2003. Červ Lovsan/Blaster pronikl téměř určitě ke všem uživatelům na světě, kteří byli připojeni k internetu a u nichž to bylo technicky možné. Průnik byl úspěšný tam, kde byl používán OS Windows 2000/XP bez pravidelné instalace bezpečnostních záplat. Lovsan/Blaster zneužíval bezpečnostní díru v DCOM RPC rozhraní. Útok se vyznačoval tím, že na uživatelských počítačích se objevovaly anomálie typu neočekávaných restartů Windows s minutovým odpočtem, popřípadě chyb ve spojitosti s procesem SVCHOST.EXE. [6]

3. 2. 3. 1 Typy počítačových červů

E-mailový červ

Ke svému šíření využívá e-mailový červ elektronickou poštu. Jakmile se červ dostane do počítače, začne se rozesílat právě pomocí elektronické pošty na další e-mailové adresy, které červ získává dvěma způsoby. Prvním je e-mailový adresář oběti a druhým je vyhledávání řetězců, které mají vyhovující tvar e-mailových adres, v obsahu uložených souborů.

Infikovaná zpráva, kterou zašle červ ve většině případů obsahuje škodlivý program jako přiložený soubor, nebo obsahuje odkaz na webové stránky, které mohou infikovat počítač příjemce. Záleží tedy na faktu, zda příjemce infikovanou přílohu nebo odkaz na webové stránky otevře, či nikoliv. [11]

Internetových červ

Ve své podstatě jde o skenování všech počítačů v síti za pomoci všech dostupných síťových prostředků daného počítače. Objeví–li červ zranitelnost jakéhokoli počítače v síti, vykoná na něj útok a je schopen se na počítač nainstalovat a spouštět zde svůj škodlivý kód. Internetový červ se může šířit bez vědomí či přičinění uživatele. [11]

IM a IRC červ

Podstata této hrozby spočívá v tom, že červ odešle odkaz na webovou stránku nebo svou kopii v souboru prostřednictvím Instant Messaging[14] komunikace. V případě IM červů jde o odkaz na webovou stránku schopnou infikovat cílový počítač, v případě IRC červů jde o zasílání svého programu jako spustitelného souboru. [11]

Červ využívající sdíleného prostoru

Tento druh červa nahraje svůj program jako spustitelný soubor většinou na sdílený prostor lokálního počítače nebo na vzdálený počítač, a infikovaný soubor dává k možnosti stažení. Infikovaný soubor je většinou pojmenován tak, aby nevzbuzoval žádné podezření. Uživatel musí infikovaný soubor stáhnout a spustit, tudíž by se mohlo zdát, že tento způsob šíření je velice neefektivní, ovšem opak je pravdou. [11]

Králíci

Králík je jedinečný typ počítačového červa, který v každém okamžiku existuje právě jednou, tzn., existuje pouze jedna kopie tohoto červa. Popisovaný druh červa, jak již napovídá název “králík”, poskakuje po počítačích propojených sítí. [8]

Chobotnice

Chobotnice je specifický druh počítačového červa skládající se z několika programů, které jsou rozmístěny na více počítačích v síti. Hlavní myšlenka spočívá v tom, že červ své jednotlivé části (hlava, ocas programu, atd.) nainstaluje do více počítačů v síti, a poté provádí nějakou funkci při vzájemné komunikaci těchto částí. Červ je hůře zjistitelný a tak může napáchat více škody. [8]

[14] Internetová služba, kde uživatel může sledovat, jací přátelé jsou připojeni, a dle potřeby s nimi chatovat, posílat soubory, nebo jinak komunikovat.

3. 4 Antivirové programy

V dnešní době je antivirová ochrana brána již jako samozřejmost. Při koupi počítače od nepřeberného množství výrobců je antivirový program již předem nainstalovaný a zaujímá postavení základního softwarového vybavení počítače.

Je to pochopitelné, jelikož ztráta dat způsobená útokem viru může mít ekonomické důsledky. V domácnostech uživatelům postačuje antivirový program, jenž je na počítači předem nainstalovaný, nebo si zdarma stáhnou či zakoupí nový antivirový software.

V případě firem je situace poněkud složitější. Zde nestačí antivirový program stáhnutý z internetu, ale situace vyžaduje vynaložení mnoho finančních prostředků a daleko více práce s udržením firemního systému. Ve firemní počítačové síti je nepřeberné množství citlivých informací a je zde mnohem větší potenciální finanční ztráta.

Dá se říci, že složitost a rafinovanost virů stoupá téměř každým dnem. Tudíž i antivirová ochrana se musí tomuto faktu přizpůsobovat. Nové viry a jejich modifikace (mutace) nutí výrobce antivirového softwaru reagovat na tuto situaci 24 hodin denně, 7 dní v týdnu.

Antivirový program vyhledává a provádí kontrolu dat na základě virové databáze, která musí být průběžně aktualizována. Tyto aktualizace se většinou stahují automaticky z internetu. Tvůrci virů se většinou zaměřují na systém Windows, do kterého se dnes značná část virů dostává přes elektronickou poštu.

Dnešním antivirovým programům již nestačí kontrolovat pouze to, co se kopíruje do počítače z disket, jak tomu mohlo být v minulosti, ale musí se potýkat s velice rozmanitými nástrahami a problémy. Dnes je pro antivirový program samozřejmostí kontrola dat na pozadí. Tuto činnost, jestliže je vše v pořádku[15], uživatel nezaregistruje.

3. 4. 1 Dělení antivirů

Antivirové programy se dají členit podle mnoha hledisek, například od nejjednodušších až po nejsložitější na jednoúčelové antiviry, on-demand antiviry a antivirové systémy.

[15] Počítač je dostatečně výkonný, antivirový scanner je dostatečně rychlý, není přítomen škodlivý software, atd.

3. 4. 1. 1 Jednoúčelové antiviry

Tyto antivirové programy jsou určeny k detekci nebo likvidaci jednoho určitého viru, popřípadě jeho mutací. Nelze je chápat jako plnohodnotnou ochranu počítače. Vytvářejí je především viroví specialisté a antivirové společnosti.

Jestliže uživatel jakýmkoli způsobem zjistí, že jeho počítač byl napaden určitým druhem viru, má možnost si většinou zdarma z internetu stáhnout jednoúčelový antivir, určený právě k likvidaci daného viru.

U jednoúčelových antivirů existují nástroje, které odstraní z počítače více druhů virů, které rozpoznají. To záleží na výrobci antiviru. [6]

Příklady jednoúčelových antivirů: Antivir LPUR (antivir proti viru LPUR – backdoor.Win32.SdBot.wv), Sophos Anti-Rootkit (detekce a odstranění nebezpečných roodkitů), ESET Conficker Removal Tool (nástroj na odstranění červa Conficker), Win32/Dipator – cleaner (odstraňuje vir Win32/Dupator a jeho následků), atd. [13]

3. 4. 1. 2 On-demand skenery

On-demand skenery neboli "skenery na požádání". Jedná se o druh antiviru, jenž neobsahuje rezidentní složku[16]. Z tohoto důvodu nemohou plnohodnotné antivirové programy nahradit, ale slouží jen ke skenování systému.

Ve většině případů se jedná o internetové online skenery poskytované zdarma. Tyto skenery plnohodnotně prohledají pevný disk uživatele a zjistí výskyt hrozeb. [6]

3. 4. 1. 3 Antivirové systémy

Jedná se o nejčastější formu antivirových programů, takových, se kterými se v dnešní době setkáváme. Jedná se o antivirové řešení, které má za úkol komplexně ochránit počítač před všemi hrozbami virového původu. Chrání počítač před červy, šířícími se pomocí elektronické pošty, škodlivými skripty, zabraňuje stažení infikovaných souborů, atd.

Součástí antivirového systému je aktualizace stahovaná z internetu. Osobní firewall[17] je v některých případech také součástí antivirového systému. [6]

[16] Rezidentní štít a další prvky, které obsahují plnohodnotné antivirové programy.
[17] Síťové zařízení, které definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Řídí a zabezpečuje síťový provoz mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení.

3. 5 Dotazníková metoda

Dotazníková metoda patří spolu s metodami pozorování, experimentem, rozhovorem a dalšími do metod psychologie, které se zabývají sběrem a analýzou dat.

Dotazníková metoda má tu výhodu, že oproti ostatním metodám není tolik časově náročná, avšak nevýhodou může být menší osobní kontakt s dotazovanými osobami, což vede ke ztrátě neverbálních informací.

3. 5. 1 Dotazník

Slouží k zjišťování informací v jakkoli velkém okruhu lidí, ať již jde o malou skupinu respondentů či celou populaci. Na základě dotazníků dále dochází k vyhodnocování zjištěných informací (preferencí, myšlenek, názorů).

Dotazníky se většinou dělí na dotazníky účelové[18] a standardizované dotazníky diagnostické[19].

Otázky v dotazníku se dělí na výzkumné a funkční. Na základě otázek výzkumných získáváme informace, které se týkají cílů výzkumu. Otázky funkční se týkají především identifikace (věk, pohlaví, atd.), motivace (dotazovanému se sdělují cíle výzkumu, navození zájmu) a kontroly (otázky zjišťují, jak spolehlivě dotazovaný odpovídá). [12]

"*Otázky dotazníku mohou být konstruovány buď jako tzv. otázky otevřené (respondent na ně odpovídá volně, svými vlastními slovy), nebo jako otázky uzavřené (jsou na ně různými formami předtištěné variant odpovědí a respondent zaškrtává tu z nich, která mu nejlépe vyhovuje).*" [12, s. 63]

3. 6 Vícekriteriální analýza variant

"*Teorie a model vícekriteriální analýzy variant se zabývá problémem, jak vybrat jednu nebo více variant z množiny přípustných variant a doporučit je k realizaci.*" [14, s.162]

Vícekriteriální analýza variant patří do skupiny metod zabývající se vícekriteriálním rozhodováním. S úlohami tohoto typu se velice často setkáváme v každodenním životě. Jde například o nákup automobilu, počítače, notebooku, výběr bankovního produktu atd. [14]

[18] Neboli příležitostné dotazníky, tvoří se k určité příležitosti pro daný (momentální) výzkum.
[19] Dotazníky aplikované standardně pro výzkumy a měření např. temperamentu, osobnostních charakteristik, atd.

Rozhodovatel, který úlohu řeší, musí být maximálně objektivní. K tomu slouží různé metody a postupy řešení těchto úloh. K maximalizaci objektivnosti někdy napomáhá oddělení osoby zadavatele[20] a analytika. Tento způsob řešení poskytuje své výhody (objektivnost) i nevýhody (možný výběr sice objektivní varianty[21], ale tato varianta nemusí být v praxi vždy ta nejlepší). [14]

V těchto modelech je určena konečná množina variant, které jsou hodnoceny podle zadaných kritérií. Cílem je analyzovat, která z těchto variant je hodnocena nejlépe, za pomoci všech uvedených kritérií (ideální či kompromisní varianta). [14]

3. 6. 1 Modely pro konstrukci vah

Stanovení vah[22] kritérií je počátečním a velmi podstatným krokem analýzy modelu vícekriteriální analýzy variant. Jestliže existuje slovní vyjádření hodnocení variant, můžeme následující metody použít i k jejich kvantifikaci.

Váhy kritérií mohou být stanoveny buď z ordinální (metoda pořadí, metoda Fullerova trojúhelníku), nebo kardinální informace (Bodovací metoda, Saatyho metoda).

Pro účely bakalářské práce je podstatná metoda bodovací. [14]

3. 6. 1. 1 Bodovací metoda

"Důležitost každé z variant podle tohoto kritéria vyjádříme určitým počtem bodů v rámci určité bodovací stupnice. Smí se používat i desetinná čísla a vice kritériím je možné přiřadit stejnou bodovou hodnotu." [14, s.173]

Tato metoda se používá, jestliže kritéria hodnotí více lidí, přičemž nejdůležitější kritérium získá nejvíce bodů, analogicky nejméně důležité kritérium získá nejméně bodů. Každý hodnotitel může mít na určité kritérium jiný pohled. Jestliže se používá například stupnice od 0 do 10 bodů, může jedno kritérium získat od dvou různých hodnotitelů např. 0 a 9 bodů, jelikož každý pohlíží na toto kritérium rozdílně (pro prvního hodnotitele je kritérium nevýznamné, pro druhého velice významné). [14]

[20] Osoba, která sbírá informace k dané problematice.
[21] Konkrétní rozhodovací možnosti, předmět vlastního rozhodování, je realizovatelná a není logickým nesmyslem.
[22] *„Váha kritéria je obecně hodnota z intervalu <0;1>, která vyjadřuje relativní důležitost tohoto kritéria v porovnání s kritérii ostatními. Součet vah všech kritérií je roven jedné."* [14, s. 165]

"*Hodnoty váhového vektoru se normalizují podle vztahu*

$$v_j = \frac{b_j}{\sum_{j=1}^{n} b_j}, j = 1, 2, \dots, n$$

kde b_j je součet všech bodů od jednotlivých expertů, které j-tému kritériu tito experti přidělili." [14, s. 174]

3. 6. 2 Ideální a bazální varianta

Ideální varianta dosahuje nejlepší možné hodnoty ve všech kritériích najednou. Může být hypotetická[23] ale i reálná[24].

Bazální variant představuje přesný opak varianty ideální, tudíž dosahuje nejhorších ohodnocení podle všech kritérií najednou. Také může být buď hypotetická[25], nebo reálná[26]. [14]

3. 6. 3 Metoda váženého součtu

Pro sestavení metody váženého součtu jsou zapotřebí kardinální informace, kriteriální matice[27] a vektor vah kritérií. Metoda váženého součtu je založena na výpočtu tzv. funkce užitku.

Funkční hodnoty metody náleží do intervalu od 0 do 1, přičemž čím více se funkční hodnota blíží k 1, tím je varianta výhodnější. Podrobnější postup metody, viz praktická část bakalářské práce. [14]

3. 6. 4 Funkce užitku

Možnost vyčíslení užitku, který byl získán při uskutečnění varianty, je předpokladem maximalizace užitku. Celkový užitek se určí tak, že se nejprve stanoví dílčí funkce užitku pro každé kritérium, poté se sloučí tyto dílčí užitky do výsledného, celkového užitku, podle kterého se určí optimální varianta. Funkce užitku převádí ohodnocení řešení do intervalu <0,1>. [14]

[23] Ideální varianta ve skutečnosti neexistuje.
[24] Ideální varianta existuje a představuje jedinou nedominovanou, jednoznačně optimální variantu.
[25] Bazální varianta ve skutečnosti neexistuje.
[26] Bazální varianta existuje a dosahuje nejhorších hodnot všech kritérií.
[27] Řádky kriteriální matice jsou tvořeny jednotlivými variantami, sloupce pak jednotlivými kritérii.

4 Vlastní práce

V praktické části se práce zabývá výběrem nejvhodnějšího antivirového programu pro studenty studující obor Podnikání a administrativa na České zemědělské univerzitě v Praze.

Pro větší vypovídající hodnotu analýzy byly z výběru vyřazeny bezplatné antivirové programy, které by mohli výsledky analýzy značně změnit.

Výběr se uskutečnil ze čtyř antivirových programů, a to: AVG Antivirus 2014, Avast! Pro Antivirus 2014, Eset NOD 32 Antivirus 7 a BitDefender Antivirus Plus.

4. 1 Vybrané antivirové programy

Na webových stránkách antivirových společností se uživatel může dočíst, že právě ten či onen antivirový program je nejlepší, nejrychlejší, poskytuje nejvyšší zabezpečení systému počítače, atd.

Programy od různých antivirových společností se liší většinou pouze technologiemi, s jejichž pomocí je dosahováno výsledných antivirových produktů. Antivirové programy nabízejí téměř shodné funkce, vylepšení a celkovou antivirovou ochranu. Liší se především inovacemi, které dříve či později budou obsahovat i ostatní, konkurenční antivirové programy.

Pro účely bakalářské práce jsou však nejdůležitější takové atributy antivirových programů, které nejčastěji ovlivňují potenciální zákazníky při koupi. Mezi hlavní rozlišovací rysy patří především cena produktů, systémové požadavky, které jsou kladeny na vybavení počítače, spolehlivost detekce škodlivého software, počet falešných poplachů[28], nebo vliv programů na výkon systému počítače.

Cena produktů byla zjištěna na webových stránkách antivirových společností. Byla zkoumána cena jednoročních a dvouročních licencí na antivirové produkty. Cena licence se týkala produktů zakoupených na jeden počítač. Do uvedené ceny bylo započítáno DPH.

Minimální systémové požadavky kladené na systém počítače byl zjištěn taktéž na webových stránkách výrobců. Zkoumáno bylo, kolik volného místa na pevném disku musí být k dispozici pro instalaci antivirového programu a minimální požadovaná velikost paměti RAM.

[28] Mylné hlášení antivirového programu, označující bezproblémový program za možnou hrozbu.

Spolehlivost detekce škodlivého softwaru a počet falešných poplachů antivirového programu byly zjištěny za pomoci nezávislých testů[29] neziskové organizace, zabývající se testováním antivirového softwaru.

Vliv antivirového programu na zatížení systému počítače byl taktéž zjištěn za pomoci testu stejné neziskové organizace. Test zkoumá chování systému počítače s různými antivirovými programy při běžné uživatelské činnosti (kopírování složek, stahování složek, instalace aplikací, otevírání PDF souborů, atd.). Každý antivirový program byl bodově ohodnocen, přičemž čím vyššího počtu bodů dosáhl, tím dopadl v testu lépe.

4. 1. 1 AVG Antivirus 2014

- Cena (licence pořízená na jeden počítač, 1 rok, cena včetně DPH) – 899 Kč
- Cena (licence pořízená na jeden počítač, 2 roky, cena včetně DPH) – 1299 Kč
- Minimální systémové požadavky na volné místo na pevném disku – 950 MB
- Minimální systémové požadavky na velikost paměti RAM – 512 MB

[15]

- Spolehlivost detekce škodlivého softwaru – 98,3 % [19]
- Počet falešných poplachů – 28 [21]
- Zatížení systému počítače – 181,1 bodů [20]

4. 1. 2 Avast! Pro Antivirus 2014

- Cena (licence pořízená na jeden počítač, 1 rok, cena včetně DPH) – 790 Kč
- Cena (licence pořízená na jeden počítač, 2 roky, cena včetně DPH) – 1190 Kč
- Minimální systémové požadavky na volné místo na pevném disku – 500 MB
- Minimální systémové požadavky na velikost paměti RAM – 128 MB

[16]

- Spolehlivost detekce škodlivého softwaru – 96,5 % [19]
- Počet falešných poplachů – 10 [21]
- Zatížení systému počítače – 188,8 bodů [20]

[29] Testy této nezávislé organizace se netýkají konkrétních virů, nýbrž antivirových společností jako celků.

4. 1. 3 Eset NOD32 Antivirus 7

- Cena (licence pořízená na jeden počítač, 1 rok, cena včetně DPH) – 1209 Kč
- Cena (licence pořízená na jeden počítač, 2 roky, cena včetně DPH) – 1814 Kč
- Minimální systémové požadavky na volné místo na pevném disku – 400 MB
- Minimální systémové požadavky na velikost paměti RAM – 128 MB

[17]

- Spolehlivost detekce škodlivého softwaru – 97,1 % [19]
- Počet falešných poplachů – 1 [21]
- Zatížení systému počítače – 183,6 bodů [20]

4. 1. 4 BitDefender Antivirus Plus

- Cena (licence pořízená na jeden počítač, 1 rok, cena včetně DPH) – 825 Kč
- Cena (licence pořízená na jeden počítač, 2 roky, cena včetně DPH) – 1376 Kč
- Minimální systémové požadavky na volné místo na pevném disku – 2000 MB
- Minimální systémové požadavky na velikost paměti RAM – 1000 MB

[18]

- Spolehlivost detekce škodlivého softwaru – 99,5 % [19]
- Počet falešných poplachů – 8 [21]
- Zatížení systému počítače189,0 bodů [20]

Cena tohoto antivirového programu byla na oficiálních webových stránkách 29,95 € za jednoroční licenci a 49,95 € za licenci trvající dva roky. Musel být proveden přepočet na 825 Kč za jednoroční licenci a 1376 Kč za licenci trvající dva roky, z důvodu sjednocení měny všech produktů. V den přepočtu byl platný kurz 27,53 Kč za EUR.

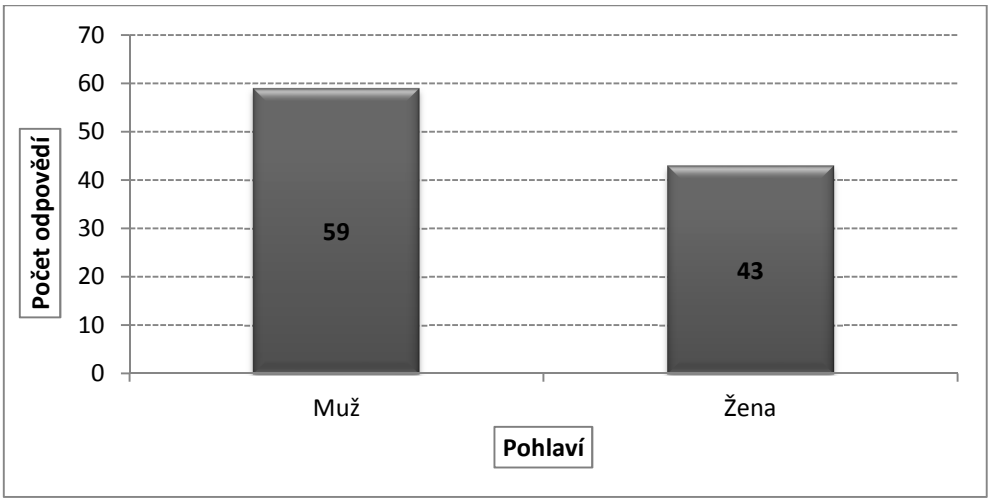
4. 2 Dotazník

Pro účely bakalářské práce byl vytvořen jednoduchý dotazník (viz. příloha 9.1), který byl zpracován v elektronické podobě. Dotazník vyplnilo 102 respondentů.

Dotazník se skládal z deseti otázek, kde prvních pět sloužilo ke zjištění věku respondenta, pohlaví, od jaké antivirové společnosti používá antivir, zda má zakoupenou licenci k produktu a případně kolik ročně za antivir zaplatí. Druhá polovina dotazníku

obsahovala otázky, u kterých měli respondenti k dispozici hodnotící škálu, na niž měli určit, jak by faktor, kterého se otázka týká, ovlivnil jejich rozhodování při koupi antivirového programu. Hodnotící škála se pohybovala v rozmezí 1 až 10 bodů, kde 1 bod znamenal absolutně nevýznamný faktor a 10 bodů absolutně významný faktor.

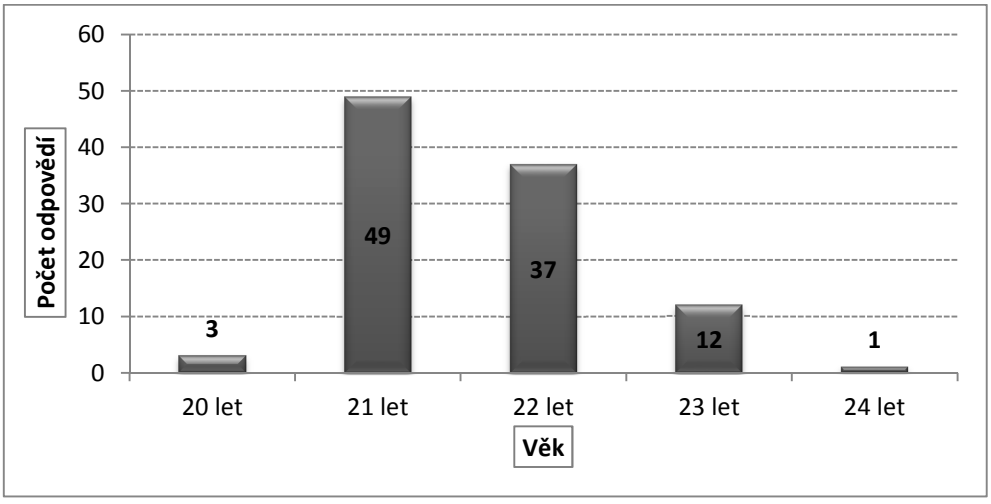
Graf: 1: Pohlaví respondentů



Zdroj: Vlastní zpracování

Dotazník vyplnilo 57,8 % mužů a 42,2 % žen.

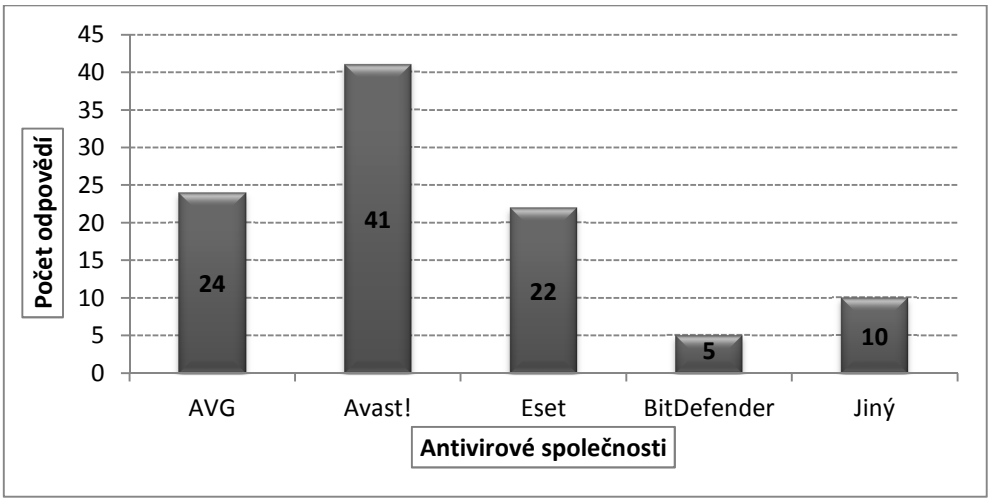
Graf: 2: Věk respondentů



Zdroj: Vlastní zpracování

Jelikož se jednalo o výzkum ve třetím ročníku, věkové rozhraní nemělo žádné výrazné odchylky. Věková škála se pohybovala v rozhraní 20 let až 24 let, přičemž 84,3 % respondentů bylo ve věku 21 a 22 let.

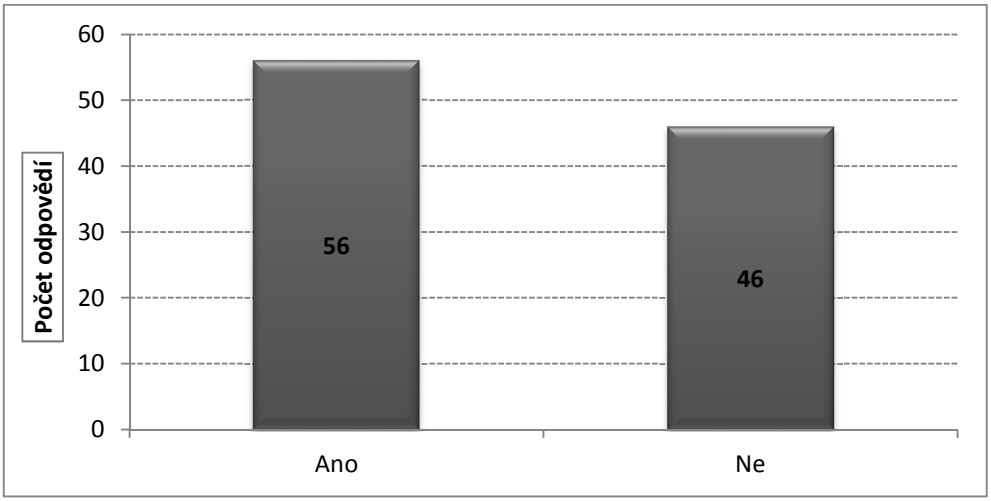
Graf: 3: V současnosti využívané antivirové společnosti



Zdroj: vlastní zpracování

Předběžný průzkum faktu, od jakého výrobce respondenti antivir využívají, obsahovala otázka č. 3. Nejvíce respondentů označilo antivirovou společnost Avast! (40,2 %). Druhá nejčastější varianta byl antivirový program od společnosti AVG (23,5 %). Téměř stejného výsledku dosáhla společnost Eset (21,6 %). Na posledním místě zůstaly produkty od společnosti BitDefender (4,9 %). Produkty od jiných společností využívá 9,8 % respondentů.

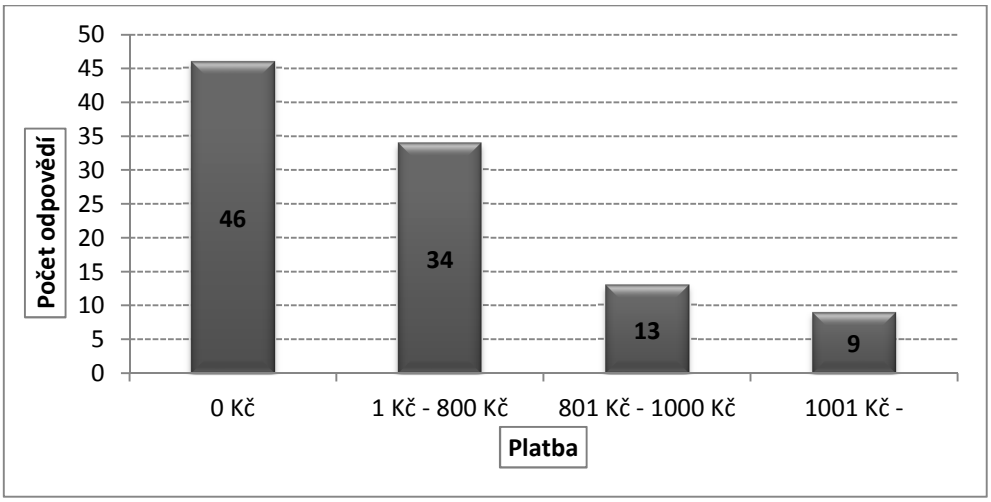
Graf: 4: Platí si uživatelé za antiviry?



Zdroj: Vlastní zpracování

Na otázku, zda si respondenti hradí licenci k antivirovému programu, překvapivě 54,9 % dotázaných odpovědělo kladně a zbylých 45,1 % záporně.

Graf: 5: Výdaje za antiviry



Zdroj: vlastní zpracování

Respondenti, kteří za svou licenci platí, jsou ochotni za antivirový program nejčastěji zaplatit částku pohybující se ve škále od 1 – 800 Kč.

Zbylých pět otázek je souhrnně řešeno v tabulce č. 1.

4. 3 Vícekriteriální analýza variant (metoda váženého součtu)

4. 3. 1 Určení vah kritérií

Z dotazníku byly zjištěny váhy kritérií bodovací metodou. Sečtením veškerých bodů, které jednotlivá kritéria získala od respondentů, vznikl váhový vektor. Poté byla provedena normalizace vah kritérií (viz. výše).

Musí být dodržena podmínka, že součet jednotlivých vah se rovná 1.

Tabulka 1: Zjištění vah kritérií

	Kritéria				
	Cena (Kč)	Minimální systémové požadavky (MB)	Detekce škodlivého softwaru (%)	Počet falešných poplachů	Zatížení systému (body)
Součet	725	643	886	639	672
Průměr	7,11	6,30	8,69	6,26	6,59
Váhy	**0,203**	**0,180**	**0,249**	**0,179**	**0,188**

Zdroj: vlastní zpracování

4. 3. 2 Přípravné výpočty

Jelikož se kritérium minimální systémové požadavky skládá ze dvou posuzovaných hledisek (velikost minimálního volného místa na pevném disku a minimální systémové požadavky na velikost paměti RAM), bylo provedeno sloučení (sečtení) těchto hledisek do jedné výsledné hodnoty, se kterou budou prováděny další výpočty.

Tabulka 2: Sloučení hledisek do výsledné hodnoty (Minimální systémové požadavky)

	Antivirové programy			
	AVG Antivirus 2014	Avast! Pro Antivirus 2014	Eset NOD32 Antivirus 7	BitDefender Antivirus Plus
Paměť RAM	512	128	128	1000
Místo na disku	950	500	400	2000
Celkem	**1462**	**628**	**528**	**3000**

Zdroj: vlastní zpracování dle [15, 16, 17, 18]

Hodnoty v tabulce č. 2 jsou uvedeny v megabajtech (MB).

Stejně tomu bylo u kritéria cena produktu. Celkové kritérium bylo hodnoceno pomocí dvou posuzovaných hledisek, cena licence produktu na období jeden a dva roky.

Tabulka 3: Sloučení hledisek do výsledné hodnoty (Cena)

	Antivirové programy			
	AVG Antivirus 2014	Avast! Pro Antivirus 2014	Eset NOD32 Antivirus 7	BitDefender Antivirus Plus
Cena na 1 rok	899	790	1209	825
Cena na 2 roky	1299	1190	1814	1376
Celkem	**2198**	**1980**	**3023**	**2201**

Zdroj: vlastní zpracování dle [15, 16, 17, 18]

Hodnoty v tabulce č. 3 jsou uvedeny v korunách (Kč). Do výsledné ceny je započítáno DPH.

4. 3. 3 Kriteriální matice

Kriteriální matice pro výpočet nejvhodnějšího antivirového programu je vytvořena na základě hodnot, které byly zjištěny o jednotlivých antivirových programech (viz. výše).

Nejvhodnější antivirový program se vybírá ze 4 možných variant (všechny antivirové programy) za pomoci pěti kritérií, které mohou být maximalizační, nebo minimalizační. V případě maximalizačního kritéria se vychází s předpokladu, že nejvyšší hodnoty představují nejlepší variantu. Opakem je kritérium minimalizační, kde nejlepší

variantu představují hodnoty nejnižší. Například kritérium cena, kde se hledá nejnižší cena (MIN), nebo kritérium detekce škodlivého softwaru, kde platí, že čím vyšší počet procent antivirový program získal, tím je výkonnější (MAX), analogicky u ostatních kritérií.

Tabulka 4: Kriteriální matice pro výběr vhodného antivirového programu

Antivirové programy	**Kritéria**				
	Cena (Kč)	Minimální systémové požadavky (MB)	Detekce škodlivého softwaru (%)	Počet falešných poplachů	Zatížení systému (body)
AVG Antivirus 2014	2198	1462	98,3	28	181,1
Avast! Pro Antivirus 2014	1980	628	96,5	10	188,8
Eset NOD32 Antivirus 7	3023	528	97,1	1	183,6
BitDefender Antivirus Plus	2201	3000	99,5	8	189
MIN/MAX[1)]	MIN	MIN	MAX	MIN	MAX

pozn. [1)] MIN – minimalizační kritérium, MAX – maximalizační kritérium

Zdroj: vlastní zpracování dle [15, 16, 17, 18, 19, 20, 21]

4. 3. 4 Stanovení ideální a bazální varianty

Pro výpočet metodou váženého součtu je zapotřebí určit ideální (H) a bazální (D) variantu. Význam těchto pojmů byl vysvětlen již v teoretické části bakalářské práce.

Tabulka 5: Stanovení ideální a bazální varianty

Ideální varianta	1980	528	99,5	1	189
Bazální varianta	3023	3000	96,5	28	181,1

Zdroj: vlastní zpracování dle tabulky č. 4

4. 3. 5 Standardizovaná kriteriální matice

Prvky standardizované kriteriální matice se získaly za pomoci vzorce

$$r_{ij} = \frac{y_{ij} - d_j}{h_j - d_j},$$

[14, s. 186]

kde r_{ij} je prvkem standardizované kriteriální matice, y_{ij} je prvkem kriteriální matice, h_j je ideální hodnota daného kritéria a d_j je bazální hodnota daného kritéria.

Tabulka 6: Standardizovaná kriteriální matice

Antivirové programy	Kritéria				
	Cena (Kč)	Minimální systémové požadavky (MB)	Detekce škodlivého softwaru (%)	Počet falešných poplachů	Zatížení systému (body)
AVG Antivirus 2014	0,791	0,622	0,600	0	0
Avast! Pro Antivirus 2014	1	0,960	0	0,667	0,975
Eset NOD32 Antivirus 7	0	1	0,200	1	0,316
BitDefender Antivirus Plus	0,788	0	1	0,741	1
Váhy	0,203	0,180	0,249	0,179	0,188

Zdroj: vlastní zpracování dle tabulky č. 4

4. 3. 6 Agregovaná funkce užitku

Užitek jednotlivých variant se vypočítá jako skalární součin normalizované matice a vah pro daná kritéria. Výpočet probíhá podle vzorce

$$u(a_i) = \sum_{j=1}^{n} v_j r_{ij}$$

[14, s. 186]

Tabulka 7: Výsledná tabulka agregovaného užitku jednotlivých antivirových programů

	Užitek	Pořadí
AVG antivirus 2014	0,422	4.
Avast! Pro Antivirus 2014	0,680	2.
Eset NOD32 Antivirus 7	0,469	3.
BitDefender Antivirus Plus	**0,730**	**1.**

Zdroj: vlastní zpracování dle tabulky č. 6

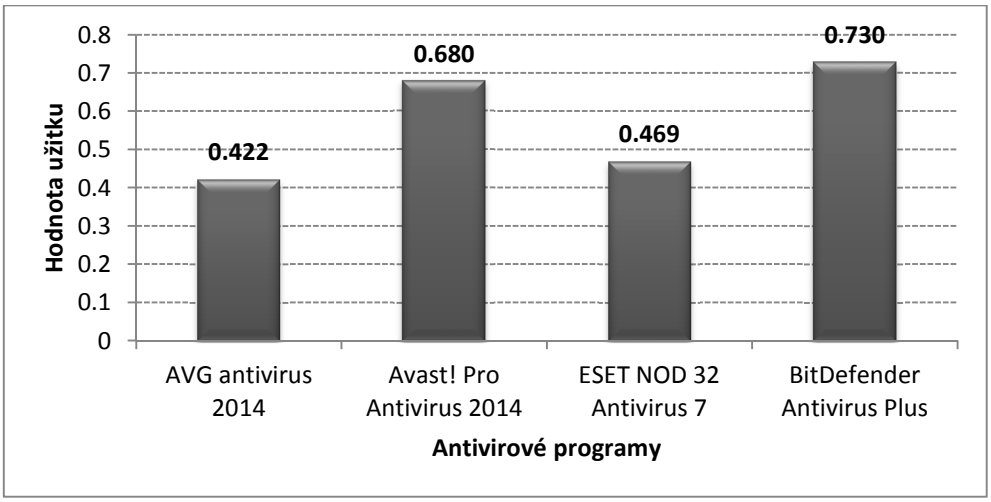
4. 4 Zhodnocení výsledků

V tabulce č. 7 bylo za pomoci metody váženého součtu zjištěno, že nejvyšší agregovaný užitek přináší, i přes své vysoké nároky na minimální systémové požadavky, antivirový program BitDefender Antivirus Plus, který dosáhl hodnoty užitku 0,730.

Na druhém místě se umístil antivirový program Avast! Pro Antivirus 2014. Program dosáhl hodnoty užitku 0,680.

Třetí příčku obsadil antivir Eset NOD32 Antivirus s hodnotou užitku 0,469. Poslední v testu skončil antivir AVG antivirus 2014, u kterého funkce užitku dosáhla hodnoty 0,422.

Graf: 6: Výsledky



Zdroj: vlastní zpracování

Graf č. 6 ukazuje, jak velkého agregovaného užitku antivirové programy dosáhly.

4. 5 Doporučení

Pomocí metody váženého součtu bylo zjištěno, že nejvyššího užitku dosáhl antivirový program BitDefender Antivirus Plus. Právě tento antivir je podle výsledků této analýzy pro studenty oboru Podnikání a administrativa na Provozně ekonomické fakultě České zemědělské univerzity v Praze nejvhodnější a nejužitečnější.

Na svém počítači používá tento antivir pouze 4,9 % dotázaných. Jelikož je to tak nízké číslo, měl by být tento antivirový program studentům doporučen, vzhledem k dosaženým výsledkům v provedené analýze.

5 Závěr

V dnešní době je kontakt se škodlivým softwarem na internetu velmi častý. Uživatelé by měli své počítače dostatečně chránit. Tato práce byla zaměřená na antivirové programy, což dnes již není dostatečná ochrana před všemi hrozbami, se kterými můžou uživatelé přijít do styku. Je potřeba, aby na počítači byly nainstalovány další ochranné prvky, například firewall. Běžnému uživateli se také vyplatí zálohovat data pro případ, že by ostatní ochranné prvky selhaly. S nadsázkou by se dalo říci, že nejúčinnější ochranou před internetovými útoky je používání rozumu.

Cílem práce bylo metodou váženého součtu vyhodnotit, který antivirový program je pro studenty třetího ročníku studující obor Podnikání a administrativa na České zemědělské univerzitě v Praze nejvhodnější. Do výběru nebyly zahrnuty antivirové programy, které jsou poskytovány zdarma z důvodu objektivnosti metody.

Z dotazníku, na který respondenti odpovídali, vyšlo najevo, že nejdůležitější vlastnost antivirového programu je pro ně detekce škodlivého softwaru, dále cena produktu, vliv programu na výkon systému počítače, minimální systémové požadavky a nejméně důležitý je pro respondenty počet falešných poplachů antiviru.

V práci byly porovnány čtyři antivirové programy. Za pomoci metody váženého součtu bylo zjištěno, že antivirový program, který přináší uživateli nejvyšší agregovaný užitek, je BitDefender Antivirus Plus. Tento antivir v analýze nepropadl téměř v žádném hodnoceném kritériu. Jediné kritérium, ve kterém byl BitDefender Antivirus Plus ze všech hodnocených variant nejhorší, bylo kritérium „minimální systémové požadavky“. Antivir BitDefender Antivirus Plus v analýze přesto zvítězil a může být studentům doporučen.

6 Seznam použitých zdrojů

[1] HEINIGE, Karel. *Viry a počítače*. Praha: Mobile Media, 2001, 80 s. ISBN 80-86593-02-9.

[2] Historie počítačových virů. *Geoinformatika* [online]. 2010 [cit. 2014-02-15]. Dostupné z: http://www.geo-info.ic.cz/zp_viry_hist.php

[3] Fred Cohen. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-02-15]. Dostupné z: http://en.wikipedia.org/wiki/Fred_Cohen

[4] Elk Cloner. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-02-15]. Dostupné z: http://en.wikipedia.org/wiki/Elk_Clone

[5] Malware. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-02-15]. Dostupné z: http://cs.wikipedia.org/wiki/Malware

[6] HÁK, Igor. *Moderní počítačové viry* [online]. Hradec Králové, 2005, 15.9.2005 [cit. 2014-02-15]. Dostupné z: http://www.fce.vutbr.cz/aiu/vojkuvka.m/u3v/vyuka/Kniha-o-virech.pdf. Bakalářská. Univerzita Hradec Králové. Vedoucí práce Doc. RNDr. Josef Zelenka, CSc.

[7] Souborové viry. *Ostravská univerzita v Ostravě* [online]. 2005 [cit. 2014-02-15]. Dostupné z: http://www1.osu.cz/home/matejka/soft/data/filev.htm

[8] ZELINKA, Ivan. *Výuka* [online]. 2013 [cit. 2014-02-15]. Dostupné z: http://arg.vsb.cz/Data/Vyuka/PVB2.pdf

[9] ZELINKA, Ivan. *Výuka* [online]. 2013 [cit. 2014-02-15]. Dostupné z: http://arg.vsb.cz/Data/Vyuka/PVB5.pdf

[10] ZELINKA, Ivan. *Výuka* [online]. 2013 [cit. 2014-02-15]. Dostupné z: http://arg.vsb.cz/Data/Vyuka/PVB6.pdf

[11] Počítačový červ. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-02-16]. Dostupné z: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv

[12] PAUKNEROVÁ, Daniela et al. *Psychologie pro ekonomy a manažery*. 3. vydání. Andrea Bláhová. Praha: Grada Publishing, a.s., 2012, 264 s. ISBN 978-80-247-3809-3.

[13] *Slunečnice* [online]. 1998 [cit. 2014-02-16]. Dostupné z: http://www.slunecnice.cz/sprava-a-zabezpeceni-pocitace/antiviry-a-antispyware/antiviry/jednoucelove/

[14] ŠUBRT, Tomáš et al. *Ekonomicko-matematické metody*. Plzeň: Aleš Čeněk, 2011, 351 s. ISBN 978-80-7380-345-2.

[15] *AVG: Ochrana před viry* [online]. ©2014 [cit. 2014-02-16]. Dostupné z: http://www.avg.com/cz-cs/buy-antivirus

[16] *Avast* [online]. ©1988 - 2014 [cit. 2014-02-16]. Dostupné z: http://www.avast.com/cs-cz/pro-antivirus

[17] *Eset* [online]. 1992 [cit. 2014-02-16]. Dostupné z: http://www.eset.com/cz/domacnosti/produkty/antivirus/?from=cz_sklik&utm_source=cz_sklik&utm_medium=ppc&utm_campaign=aj31&utm_content=nod5-antivir-dyn

[18] *BitDefender* [online]. © 1997 - 2014 [cit. 2014-02-16]. Dostupné z: http://www.bitdefender.com/solutions/antivirus.html

[19] File Detection Test of Malicious Software. *AV-Comparatives: Independent Tests of Anti-Virus Software* [online]. 2013 [cit. 2014-02-16]. Dostupné z: http://www.av-comparatives.org/wp-content/uploads/2013/09/avc_fdt_201309_en.pdf

[20] Performance Test (Suite Products). *AV-Comparatives: Independent Tests of Anti-Virus Software* [online]. 2013 [cit. 2014-02-16]. Dostupné z: http://www.av-comparatives.org/wp-content/uploads/2013/11/avc_per_201311_en.pdf

[21] False Alarm Test. *AV-Comparatives: Independent Tests of Anti-Virus Software* [online]. 2013 [cit. 2014-02-17]. Dostupné z: http://chart.av-comparatives.org/chart1.php

7 Seznam tabulek

8 Seznam grafů

9 Přílohy

9. 1 Dotazník (Antivirové programy)

1) Pohlaví?

a) Muž

b) Žena

2) Kolik Vám je let?

3) Od jaké antivirové společnosti používáte antivirový program?

a) AVG

b) Avast!

c) Eset

d) BitDefender

e) jiný

4) Platíte za licenci k antivirovému programu?

a) Ano

b) Ne

5) Kolik platíte za licenci ke svému antivirovému programu?

a) 0 Kč

b) 1 – 800 Kč

c) 801 Kč – 1000 Kč

d) více než 1001 Kč

6) Jak je pro Vás důležitá cena produktu?

Ohodnoťte na stupnici 1 – 10, kde 1 znamená „nedůležitý“ a 10 znamená „nejdůležitější“

7) Jak jsou pro Vás důležité systémové požadavky systému počítače?

Ohodnoťte na stupnici 1 – 10, kde 1 znamená „nedůležitý“ a 10 znamená „nejdůležitější“

8) Jak je pro Vás důležitá spolehlivost detekce škodlivého software u produktu?

Ohodnoťte na stupnici 1 – 10, kde 1 znamená „nedůležitý“ a 10 znamená „nejdůležitější“

9) Jak je pro Vás důležitá skenovací rychlost u produktu?

Ohodnoťte na stupnici 1 – 10, kde 1 znamená „nedůležitý“ a 10 znamená „nejdůležitější“

10) Jak je pro Vás důležité, jaký má antivirový program vliv na zatížení systému počítače?

Ohodnoťte na stupnici 1 – 10, kde 1 znamená „nedůležitý“ a 10 znamená „nejdůležitější“