Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Porovnání antivirových programů

Jiří Papica

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Papica

Provoz a ekonomika

Název práce

Porovnání antivirových programů

Název anglicky

Comparison of Antivirus Software

Cíle práce

Cílem práce je porovnání čtyř antivirových programů a následné vyhodnocení nejlepšího antiviru pro vybraný počítač.
Dílčími cíli práce je seznámení se s vlastnostmi antivirových programů, stanovení požadovaných vlastností antivirových programů a stanovení kritérií pro jejich hodnocení.

Metodika

Bakalářská práce bude vycházet z literární rešerše odborných zdrojů.

Dále budou stanoveny požadavky na antivirové programy a kritéria pro hodnocení splnění těchto požadavků.

Hodnoceny budou následující antivirové programy:

ESET NOD32 Antivirus

Avast! Antivirus

Norton Antivirus

Kaspersky Antivirus

Na základě výsledků měření bude vybrán vhodný antivirový program a budou stanoveny závěry práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

vir, antivirový program, software, bezpečnost, NOD32, Avast!, Norton, Kaspersky

---

Doporučené zdroje informací

DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. 1. vyd. Brno: CP Books, 2005. ISBN 80-251-0574-1

HÁK, Igor, ZELENKA, Josef. Ochrana dat: škodlivý software. Hradec Králové: Gaudeamus, 2005. ISBN 80-7041-594-0

HEINIGE, Karel. Viry a počítače. Praha: Mobile Media, 2001. ISBN 80-86593-02-9.

JALŮVKA, Josef. Moderní počítačové viry. 2. aktualizované vydání. Praha: Computer Press, 2000. ISBN 80-7226-402-8

JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KUCHAŘ, Martin, Mirek JAHODA a Petr BROŽA. Bible hardwaru. 1. vyd. Brno: Extra Publishing s.r.o., 2008. ISSN 1802-1220

SZOR, Peter. Počítačové viry: analýza útoku a obrana. 1.vyd. Brno: Zoner Press, 2006. ISBN 80-86815-04-08

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 8. 2. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 02. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Porovnání antivirových programů" 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 14. 3. 2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Martinu Havránkovi, Ph.D. za odborné vedení a rady při zpracovávání mé bakalářské práce.

Porovnání antivirových programů

Comparison of Antivirus Software

Souhrn:

Tato bakalářská práce se zabývá porovnáním vybraných antivirových programů a následného vybráním nejvhodnějšího z nich pro daný počítač.

Práce se skládá ze dvou částí. První část práce se zabývá počítačovými viry a malware, které jsou dále rozděleny podle různých typů a hledisek. Kromě problematiky počítačových virů jsou dále popsány antivirové prostředky a mechanismy, jako například firewall či heuristická analýza. Na konci teoretické části jsou stručně popsány základní hardwarové součásti počítače, na které se následně zaměří měření a testování kritérií.

Druhá část práce obsahuje stanovení vlastností antivirových programů, stanovení kritérií pro jejich hodnocení a samotné měření zvolených kritérií. Kritéria byly zvoleny následovně, a to Cena, doba konvertování videa v programu Sony Vegas Pro, doba konání GPU benchmark, doba konání CPU benchmark a efektivnost antivirových programů v reálném prostředí. Hodnoceny byly tyto antivirové programy: Eset Smart Security 9, Norton Security Deluxe, Avast! Internet Security a Kaspersky Anti-Virus. Naměřené hodnoty byly převedeny na body a následně zaneseny do paprskových grafů. Z tabulek a grafů na závěr vyšlo doporučení nejvhodnějšího antivirového programu pro daný počítač.

Summary:

This bachelor thesis focuses on comparison of selected anti-virus programs and subsequent choosing of the most suitable one for given computer.

The thesis consists of two major parts. The first part focuses on anti-viruses and malware, which are divided into various types. In addition to the anti-virus section there are topics which are covering things like anti-virus tools and mechanism, e.g. firewalls and heuristics. At the end of the theoretic part there are topics which are briefly touched upon, topics like hardware basics of every computer which are later on important for the actual testing parts.

The second major part of this thesis is about choosing the right attributes for ani-viruses, about choosing the right criteria for their future evaluation and finally the

measurement of said criteria. The criteria that were chosen are thus: price, time it takes for video to be rendered in Sony Vegas Pro, time it takes for GPU benchmark to finish, time it takes for CPU benchmark to finish and finally the last criteria that was picked is the effectiveness against real-life threats. Anti-virus programs that were being evaluated are Eset Smart Security 9, Norton Security Deluxe, Avast! Internet Security and lastly Kaspersky Anti-Virus. The recorded values were converted into a point-based system, which allowed for clear and evident illustrations via graphs and charts. From the final graphs and charts I was able to recommend the most suitable anti-virus for given computer.

Klíčová slova: vir, antivirový program, software, bezpečnost, NOD32, Avast!, Norton, Kaspersky

Keywords: virus, anti-virus program, software, safety, NOD32, Avast!, Norton, Kaspersky

Obsah

1 Úvod

V době plné různých internetových hrozeb se výrobci antivirových programů snaží co nejvíce prosadit a zviditelnit na trhu. Je jasné, že chování spotřebitele je ovlivnitelné dobrou pověstí antivirového programu a též jeho nároky na systémové zdroje počítače.

Téma mé bakalářské práce jsem si vybral, abych vyhodnotil a porovnal vybrané antivirové programy v době, kdy je současný trh přesycen různými produkty, které mají na první pohled obdobné funkce a liší se pouze názvem, popřípadě cenou. Každý uživatel má jiné priority. Někdo upřednostňuje cenu, jiný zase nároky na operační systém.

Je však nutné si uvědomit, že firmy zabývající se vývojem antivirových programů až následně reagují na vzniklé hrozby a tudíž není možné se na antivirové programy zcela spoléhat. Stejně jako je možné řídit auto bez bezpečnostních pásů, uživatel by neměl používat počítač bez antivirového programu i když to je samozřejmě též možné.

Tato práce a její závěry mohou pomoci méně zkušeným uživatelům výpočetní techniky se lépe orientovat v problematice antivirových programů a vybrat nejvhodnější antivir podle svých představ.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je porovnání čtyř antivirových programů a následné vyhodnocení nejlepšího antiviru pro vybraný počítač.

Dílčími cíli práce je seznámení se s vlastnostmi antivirových programů, stanovení požadovaných vlastností antivirových programů a stanovení kritérií pro jejich hodnocení.

Pro dosažení cíle bude použit vybraný počítač, na kterém proběhnou všechny testy a měření.

2.2 Metodika

Práce je rozdělena do dvou částí. V první části se práce zabývá seznámením s teoretickou stránkou problematiky virů a rozdělením na jednotlivé typy útoků. Dále jsou také popsány jednotlivé antivirové prostředky na obranu proti těmto virům. Na konci této části jsou stručně popsány základní hardwarové součásti počítače.

Druhá část této práce se zabývá praktickými měřeními jednotlivých vybraných kritérií. Jsou zde uvedeny hodnotící kritéria a měřící metody. Kritéria budou zvolena na základě tří hlavních požadavků: ceny, působení antivirového programu na systém zvoleného počítače a efektivnost v odhalování virů v reálném prostředí. Tato kritéria budou měřena sadou pěti testů.

Na základě naměřených hodnot budou jednotlivé výsledky obodovány a zobrazeny v grafech. Nakonec na základě součtu bodů bude vybrán nejlepší a nejvhodnější antivirový program pro zvolený počítač.

3 Rešerše

3.1 Škodlivý software

3.1.1 Počítačové viry

„U počítačů je virus vždy útvar umělý, záměrně vytvořený člověkem.“ [6, s.4]

Pod pojmem počítačový vir se rozumí druh infiltrace, která se snaží proniknout do počítače a vykonávat škodlivou činnost. Viry obvykle napadají už existující soubory na disku, například nejčastější spustitelné soubory a dokumenty. [10]

Pojem vir se často nesprávně používá pro označení dalších typů hrozeb a infiltrací. Tento dnes již zaběhnutý výraz se nahrazuje mnohem přesnějším termínem „malware“ (malicious software – škodlivý software). Průběh aktivace počítačového viru je tedy zhruba následující: po spuštění napadeného souboru nejprve dojde ke spuštění připojeného viru. Ten vyvolá akci, kterou má v sobě naprogramovanou. A teprve až se nakonec dostane uživatel k původní aplikaci. Vir může nakazit každý soubor, ke kterému má aktuálně přihlášený uživatel oprávnění pro zápis. [9]

„Viry na počítačích infikují soubory, nebo systémové prvky, nebo pozměňují odkazy na tyto objekty a poté, co převezmou kontrolu, se v dalších generacích opět množí.“ [7, s. 45]

Vlastní činnost aktivovaného viru může mít mnoho podob. Některé viry jsou obzvláště nebezpečné, protože dokáže mazat soubory z disku, jiné viry zase například uživatele „pouze“ obtěžují (zavírá a otvírá CD mechaniku, nebo maže ikony na ploše), než aby způsobovali více závažnější škody. [9]

3.1.2 Rozdělení virů dle umístění v paměti

Rezidentní viry

„Paměťově rezidentní virus setrvává ilegálně v paměti. Většinou při prvním spuštění infikovaného souboru (pokud se jedná o souborový virus), nebo při prvním zavedení systému z infikovaného boot sektoru (pokud se jedná o boot virus), se stane rezidentním v paměti a odtud potom provádí svoji škodlivou činnost.“ [12, s.45]

Vir se do paměti umisťuje rezidentně ve dvou krocích. Prvním je vyhledání nebo vytvoření vhodného místa, kam by se vir umístil. Takové místo musí být dostatečně velké a

současně bezpečné. U boot viru není výběr možností moc velký. Vir se totiž instaluje do paměti v okamžiku, kdy ještě není zaveden operační systém, a proto nemá k dispozici funkce pro manipulaci s pamětí, které DOS nabízí. Nejčastějším způsobem, kterým se boot viry s tímto problémem vypořádávají, je umělé snížení velikosti základní paměti, a využití uvolněného místa, které takto vznikne. Z hlediska tvůrců virů je nevýhodou této metody poměrně snadná možnost zjistit netypickou velikost základní paměti.

Další metodou, kterou používají zejména menší viry, je využití malých volných oblastí v datových oblastech v dobré víře, že do nich nebude nikdo jiný zapisovat. S využitím této techniky se lze občas setkat i v těle některých souborových virů. [6]

Nerezidentní viry

„Jinak nazývané „viry přímé reakce“ nevyužívají paměť pro své šíření. Stačí jim, když jsou aktivovány společně s hostitelským programem. Pak přebírají řízení jako první, provedou svoji činnost, nejčastěji replikaci a pak předají řízení zpět hostitelskému programu.“ [6, s. 15]

Viry přímé akce se načtou do paměti během zavádění hostitele a po předání řízení vyhledají objekty k napadení. To je ten důvod, proč je většina počítačových virů právě infektory přímé akce – takové viry je snadné vytvořit na mnoha platformách, v binárních i skriptovacích jazycích. Tyto viry obvykle používají k nalezení svých obětí sekvence FindFirst a FindNext a infikují po svém spuštění pouze několik souborů. Některé viry ovšem infikují všechny dostupné oběti. V jiných případech se ihned zkopírují na disketu nebo pevný disk a nečekají, až to provede uživatel. Tato operace je nicméně snadno postřehnutelná, protože práce s disketou je docela hlučná. [7]

3.1.3 Typy počítačových virů

3.1.3.1 Boot vir

Boot sektor je fyzicky první sektor (0. hlava, 0. stopa, 1. sektor) diskety či logické části pevného disku. Obsahuje zaváděcí kód sloužící k finálnímu zavedení operačního systému – načítá systémové soubory a předává jim řízení, které dále zajistí vlastní spuštění jádra DOSu, provedení systémových souborů a v neposlední řadě spuštění příkazového interpretu. [8]

„Na svůj přenos využívá boot sektor (případně i několik dalších sektorů) diskety zasunuté v mechanice A:, kde nahrazuje původní boot sektor (bez ohledu na to, zda šlo o bootovatelnou disketu nebo ne). Kód viru pro svoji aktivaci (nabootování ze zavirované diskety ponechané úmyslně nebo ze zapomnětlivosti v mechanice) obvykle přenese svoje tělo Boot sektoru logického disku C: nebo častěji Master Boot sektoru pevného disku (případně i několik dalších sektorů). Při nejbližším bootu z pevného disku se tedy virus spouští po BIOSu jako první (ještě před samotným operačním systémem) a záleží jen na typu viru, jak této skutečnosti využije.“ [6, s.8]

3.1.3.2 Souborové viry

„Druhou a svého času nejrozšířenější skupinou jsou viry souborové, jejiž hostitelem jsou soubory. Tyto viry bychom mohli dále třídit podle toho, jaké typy proveditelných[1] *souborů při infekci přímo či nepřímo napadají. Nejčastěji se jedná o soubory spustitelné binární (COM, EXE, atd.), může se též jednat o souborové viry infikující dávkové soubory (BAT) či ovladače (SYS). Mechanizmus činnosti souborových virů je však podobný ve všech případech.“* [5, s. 38]

Podle metody infekce/umístění viru vůči souborům můžeme souborové viry rozdělit na několik skupin – přepisující viry, parazitické viry a doprovodné viry. [5]

Po spuštění nakaženého souboru se vykoná nejdříve kód viru, který buď uskuteční přímou akci (infikování dalších souborů podle vhodné strategie), ale častěji se virus stane paměťově rezidentním a následně infikuje další spustitelné soubory (nejčastěji při jejich spuštění, ale i při kopírování, prohlížení, komprimaci a jiné manipulaci s nimi). V závislosti na splnění určité podmínky (čas, datum, počet spuštění) přitom může vir strategii svého šíření obměňovat, případně vykonávat i jinou (nesouvisející se samotnou replikací), např. destrukční akci. Po vykonání celého viru se zabezpečí aktivace samotného hostitelského programu. [6]

3.1.3.3 Makroviry

„Jde o viry, jejichž činnost je řízená makrojazykem příslušné aplikace, přičemž jsou v tomto smyslu vázané na konkrétní formát dokumentu – makrojazyk Word Basic a dřívější verze MS Word, respektive dnes nejčastěji Visual Basic for Applications ve spojení

[1] zajišťuje aktivaci viru při spuštění souboru

s novějšími verzemi MS Word, MS Excel, MS Access, MS Power Point, MS Project ale už i CorelDraw a dalšími aplikacemi.“ [6, s. 9]

„Makroviry jsou nejaktuálnějším trendem hrozeb podobných virům. Hlavním důvodem tohoto trendu je prostý fakt, že výměna dokumentů mezi uživateli je mnohem častější než výměna programů.“ [8, s. 41]

Systém je infikován wordovým makrovirem v okamžiku, kdy je editorem načten infikovaný soubor. Od tohoto okamžiku jsou infikovány všechny nově vytvořené textové dokumenty (soubory *.DOC). Prakticky to znamená, že v okamžiku otevření textového dokumentu spustí Word infikované makro prostřednictvím šablony, která může, na rozdíl od samotného dokumentu, makra obsahovat. Klíčem jsou tzv. AUTO-makra, která jsou spuštěna automaticky. Je-li pak ukládán na disk libovolný dokument, je uložen i s virovým makrem. [8]

Možnosti makrovou jsou omezené, Word např. není oprávněn provádět konfiguraci pevného disku či měnit obsah zaváděcího sektoru disku. Makrovirus nemůže v žádném případě provádět přímé systémové operace. Cílem makrovirů nejsou útoky proti daným aplikačním programům, ale proti jejich datovým souborům. [8]

3.1.4 Další vlastnosti a typy počítačových virů

Adresářový (linkovaci) vir

„Vir, který je na disku přítomný v jediném exempláři a který napadá jiné spustitelné soubory tak, že přepisuje v adresáři směrník na jejich začátek tak, aby ukazoval na začátek viru. Původní hodnotu směrníku se ale ukládá, takže pokud je vir paměťově rezidentní, je schopný zabezpečit po provedení vlastního kódu i spuštění původních souborů.“ [6, s. 10]

Adresářové viry (neboli také angl. Cluster viruses) je malá skupinka virů. Tyto viry modifikují vstupy adresářové tabulky tak, že virus je zaveden do paměti a spuštěn dříve než program, který uživatel chce spustit. Léčení je poměrně snadné, ale zdlouhavé. [6]

Kódovaný vir

Prvotním účelem kódování bylo znepřehlednit vlastní kód viru a ztížit tak jeho analýzu (která je nutná k vytvoření antivirového programu). Navíc je tímto způsobem zkomplikováno uzdravení napadeného programu, protože obsah začátku programu je také zakódován.

Novější viry začaly využívat kódování a proměnnou hodnotou k dosažení toho, aby každý exemplář viru byl z velké části odlišný; shodná zůstává pouze dekódovací smyčka na začátku programu. To sice značně zkomplikovalo vyhledávání některým antivirovým programům používajícím charakteristické sekvence, ale neustále je relativně snadné určit kódovací hodnoty a program dekódovat. Navíc lze stále použít vždy stejně vypadající dekódovací smyčku k identifikaci viru.

Nástupce této technologie představují polymorfní viry, které používají poměrně komplikovaných metod k tomu, aby i dekódovací smyčka mohla mít proměnlivou podobu. [6]

Polymorfní vir

„Polymorfní viry umějí měnit svůj decryptor[2] do vysokého počtu odlišných instancí, které mohou mít až milióny různých forem.“ [7, s. 237]

Vir, jehož jednotlivé exempláře mají rozdílný kód. Typickou činností je vkládání prázdných instrukcí, přehazování pořadí výkonu části kódu nebo změna sekvencí kódu jinými sekvencemi s ekvivalentní funkcí. V rámci úvodní části kódu viru spolu s technologií šifrování znemožňují zbývající části viru identifikaci viru jednoduchým hledáním pevné sekvence kódu. Vir je možné identifikovat jen specializovanými algoritmy, případně výkonnými heuristickými[3] metodami. [6]

Stealth vir (Neviditelný vir)

„Rezidentní virus, který se pokouší vyhnout detekci skrytím projevů své přítomnosti v infikovaných souborech. Aby toho dosáhl, zachycuje virus systémová volání, která prověřují obsah nebo atributy infikovaných souborů. Výsledky těchto volání musí být změněny tak, aby odpovídaly původnímu stavu souboru. Takto pracovat může pouze tehdy, je-li rezidentní v paměti.“ [6, s. 59]

Vir, který využívá příslušné služby operačního systému na zamaskování svojí aktivity. Například se může jednat o Boot viry, které při čtení Master Boot sektoru vracejí prohlížeči původní (nezavirovaný) obsah tohoto sektoru. Jiným příkladem jsou souborové viry, které maskují změnu délky zavirovaného souboru nebo se při otevření souboru za účelem hledání viru z hostitelského souboru vyčistí a po ukončení prohlížení souboru ho opětovně zavirují.

[2] úsek kódu viru, který zajišťuje převedení zakódované části viru do původní spustitelné podoby. Nejčastěji se vyskytuje na začátku viru. Může mít konstantní podobu v různých generacích téhož viru.
[3] obecná sémantická analýza kódu programu, která se používá k detekci neznámých virů.

Název těchto virů je odvozen od anglického slova stealth, což znamená lstivost, neviditelnost nebo činnost vykonávanou potajmu. [6]

Retro vir

Jinak také odvetný vir. Hlavním heslem těchto virů je, že nejlepší obrana je útok. A to taky dodržují. Snaží se obejít a ještě lépe znemožnit práci antivirovým programům. Proto je mažou, vypínají rezidentní ochrany apod. [6]

3.1.5 Trojské koně

„(angl. Trojan horse) jejich šíření a aktivace je závislá na využití spolupráce s viry nebo červy, nebo na lsti a oklamání uživatele.“ [5, s. 15]

Obecně se dá říci, že trojský kůň se maskuje za užitečný program, aby si zajistil své spuštění uživatelem. [10]

„Zřejmě nejjednodušším druhem škodlivého programu je trojský kůň. Takový program se snaží uživatele něčím zaujmout a vytvářet dojem „užitečnosti“ – aby uživatel neodolal a spustil jej na svém počítači.“ [7, s. 47]

„V současnosti mohou být trojské koně šířeny i ve spojení s počítačovými viry, nebo červy, mohou být nainstalovány při využívání aktivních skriptů na WWW stránkách a jejich šíření tak není vázáno pouze na zástěrku užitečných programů a utilit.“ [5, s. 18]

Trojský kůň je program, který navenek navozuje dojem užitečnosti. V dokumentaci programu slibovanou činnost však buď vůbec nevykonává, nebo ji vykonává, ale v pozadí realizuje nepozorovaně nějaký druh destrukce (maže soubory, formátuje pevný disk atp.). Trojský kůň je buď naprogramovaný jako původní aplikace, nebo je vytvořený z už existujícího programu jeho spojením s destrukčním kódem (který se vykonává před samotným programem), přičemž takový program se potom od původního kromě délky navenek ničím neodlišuje. [6]

V současné době jsou častými i trojské koně, které jsou vlastně instalačním souborem samotného programu, který se po své instalaci spouští při restartu operačního systému Windows a skrytě vykonává nějaký typ destrukce. [6]

3.1.5.1 Další typy trojských koní

Zadní vrátka (angl. Backdoor)

„Zadní vrátka jsou aplikace, sloužící pro vzdálenou správu PC a sama o sobě nemusí být škodlivá. Záleží pak na aktivitách osoby, která tuto vzdálenou správu vykonává, což bývá často spojeno i se způsobem, jak byla zadní vrátka na systém instalována.“ [5, s. 19]

Zadní vrátka jsou pro vzdálený přístup pro hackery nástrojem číslo jedna. Typický zástupce této skupiny po svém spuštění otevře síťový port (UDP/TCP) na daném počítači. Poté naslouchá a vyčkává na připojení útočníka, kterému umožní přístup do systému. Toto je nejčastější způsob fungování, který je často spojen s dalšími funkcemi z oblasti trojských koní. [7]

Trojské koně s funkcí hledání hesel (Password-stealing trojan)

„Jsou zaměřeny na hledání a odesílání hesel útočníkům. Poté se může útočník na daný systém kdykoliv připojit a pracovat na něm. Tyto programy jsou často kombinovány se zaznamenáváním stisku kláves na klávesnici (což je relativně snadný způsob získání hesla).“ [7, s. 48]

Skupina trojských koní, která obvykle sleduje jednotlivé stisky kláves (key-loggers) a tyto ukládá a následně i odesílá na dané emailové adresy. Majitelé těchto emailových adres (nejčastěji právě samotní autoři trojských koňů) tak mohou získat i velice důležitá hesla. [5]

3.1.6 Počítačoví červi

„*Červi – (též síťové červy; angl. Worms, network Worms) šířící se pomocí síťových služeb; lze nalézt ještě dvě podkategorie podle toho, zda vyzřívají pouze síťových služeb (užší pojetí červů), nebo zda využívají služeb aplikačních programů (především různé manažery e-mailové pošty), které realizují síťové služby (jsou někdy zahrnovány mezi počítačové viry).* [5, s. 14]

„Termín počítačový červ označuje síťové viry – tedy viry primárně se šířící sítěmi. Na vzdáleném počítači se obvykle spouštějí bez jakéhokoliv zásahu ze strany uživatele. Opačným případem jsou červi šířící se pomocí e-mailů, kteří pomoc uživatele potřebují.“ [7, s. 45]

„Červ (anglicky worm) je program, který neinfikuje spustitelné soubory jako je tomu v případě virů, ale infikuje systémy tím způsobem, že pomocí počítačové sítě rozšiřuje kopie sebe sama na připojené počítače.“ [8, s. 47]

Červi se nacházejí v souboru samostatně a nepotřebují žádného hostitele (až na vyjímky). Antivirové programy tak ve většině případů mažou všechny soubory, které si červ pro svůj chod v systému vytvořil. Nevracejí však do původního stavu registry Windows, popřípadě soubory, které červ zmodifikoval tak, aby si zajistil včasnou aktivaci po každém startu operačního systému Windows. Většina červů si zajistí automatické spuštění nejčastěji pomocí modifikace registrů nebo pomocí modifikace souboru WIN.INI, případně SYSTÉM.INI (ve složce s instalací Windows). [6]

Červům podobné jsou infiltrace neformálně zvané jako bakterie (bakterium) a králík (rabbit). Oba typy po spuštění kopírují sebe sama. Bakterie šíří své kopie jiným uživatelům a systémům za účelem rozšíření, králík šíří své kopie bez omezení s cílem, na rozdíl od bakterie, vyčerpat dostupné systémové zdroje (čas procesoru, diskový prostor atp.). Označení „králík“ je v tomto případě výstižné.

Rozvoj internetu přinesl novou podobu šíření červů, a to pomocí elektronické pošty. Definice červa dnešní doby zní: červ je program, který se šíří prostřednictvím e-mailové zprávy, ke které je připojen ve formě souboru. V zásadě totéž co platí pro makroviry. [8]

3.1.6.1 Další typy počítačových červů

Chobotnice

„Chobotnice je sofistikovaný druh počítačového červa, který je tvořen sadou více programů rozmístěných na více než jednom počítači v síti“. [7, s. 46]

Například, hlava a ocas takového programu jsou nainstalovány na různých počítačích a společně komunikujíce provádějí nějakou funkci. Chobotnice není příliš častá. [7]

Králíci

„Králík je zvláštní druh počítačového červa, který v každém okamžiku existuje v jedné kopii, která „poskakuje“ po sítěmi spojených hostitelských počítačích.“ [7, s. 46]

Někteří výzkumníci používají tento termín k popisu škodlivých aplikací, které se rekurzivně[4] spouští tak dlouho, dokud nezahltí paměť. V případě aplikací, které nejsou připraveny pracovat v prostředí s nízkými paměťovými zdroji, to může způsobit mnoho problémů. [7]

3.1.7 Hesla – základy

V počítači a na internetu prokazujeme svojí totožnost heslem. V dnešní době se obvykle jedná o kombinaci písmen, čísel a speciálních znaků. Zaheslováno může být prakticky cokoliv – od zapnutí počítače, přes spuštění operačního systému, po oprávnění instalovat a měnit programy v systému počítače.

Obecně rozumná minimální délka pro běžná hesla se uvádí hodnota osm až deset znaků. Heslo by se nemělo skládat z po sobě jdoucích čísel (1234) ale ani po sobě jdoucích stejných písmen (AAAA). Nemělo by mít souvislost s ničím z našeho života, co se dá snadno odhadnout, např. rok narození, jméno manželky, telefonní číslo, poznávací značkou a podobně.

Ideální heslo by mělo obsahovat kromě velkých a malých písmen také alespoň jednu číslici a speciální znak (závorka, hvězdička, plus, mínus apod.). Na druhou stranu není dobré, aby heslo obsahovalo Y a Z, kvůli různým rozložením české klávesnice. Stejné nepříjemnosti může způsobit také česká diakritika, pokud se jí tedy můžeme vyhnout, psát raději bez háčků a bez čárek.

Hesla pravidelně měnit. Toto pravidlo vychází s části z firemních pravidel o heslech. Důvodů pro změnu hesel je spousty. Některá hesla jsou přenášena pomocí internetu, kde je může při troše snahy někdo odposlechnout. Čím déle zůstávají nezměněna, tím větší šance, že se to někomu podaří. Jiná hesla přenášena online nejsou – typickým příkladem je heslo chránící přístupú do počítače nebo přístup k dokumentům ve Wordu. Aby je někdo mohl zjistit, musel by se nejprve dostat do fyzické blízkosti našeho počítače a strávit tam poměrně dlouhou dobu. Tato hesla tedy nemusíme měnit často, stačí hlídat fyzický přístup k počítači. [3]

[4] opakované vnořené volání stejné funkce

3.2 Antivirové programy

„Stále stoupající množství počítačových virů nás nutí brát antivirovou ochranu jako naprostou samozřejmost. V dnešní době je již poměrně vzácné najít zodpovědného uživatele, který by si hrozby neuvědomoval a ponechával počítač bez ochrany.“ [5, s. 108]

Dnešním domácím uživatelům stačí jednoduše stáhnout některý z dostupných antivirových programů. Řada antivirových programů je navíc šířena také bezplatně a lze si je tak za jistých podmínek stáhnout z internetu. Zajistit ovšem komplexní antivirovou ochranu firmy dá mnohem více práce a vyžaduje i nepoměrně více finančních prostředků.

Dalším faktorem ovlivňujícím náročnost je problematičnost nasazení antivirové ochrany. Nutností je odborná dovednost a zkušenost na takové úrovni, aby zajistila skutečně fungující antivirovou ochranu. Stoupající rafinovanost škodlivých kódů vede logicky i k růstu složitosti nasazované antivirové ochrany. Zatímco pro domácího uživatele tato složitost zůstává skryta uvnitř programů, pro administrátory sítí to často představuje těžce řešitelné problémy spojené s instalací a nastavením antivirové ochrany firemní sítě.

Se stále větší rozšířeností internetu a počítačových sítí obecně i stoupá pole působnosti škodlivých kódů. [2]

3.2.1 Základní antivirové prostředky a mechanismy

Softwarové prostředky

„*Programové prostředky jsou bezesporu základními, nejvíce používanými antivirovými produkty. V současné době je na domácím i zahraničním trhu značné množství antivirových programů a vyznat se v této informační změti není vůbec jednoduché. Každý produkt má své klady i zápory a tak určení, který je ten nejlepší je záležitost ryze individuální a do jisté míry i subjektivní.“* [8, s. 57]

Vyhledávač (skener)

Základní typ programu, který zjišťuje přítomnost virů (v paměti i na disku) pomocí virových identifikačních řetězců. Identifikační řetězec je jednoznačně definovaná posloupnost znaků (bajtů) reprezentující daný virus. Je-li nalezena daná posloupnost znaků v souboru, je tento soubor prohlášen za zavirovaný. Správné určení identifikačního řetězce je důležité pro zamezení falešných poplachů, kdy nevhodně navržené skenery mylně upozorňují na

přítomnost viru na počítači. Pro eliminaci tohoto problému používají inteligentní vyhledávací programy kombinaci identifikačního řetězce spolu s přesným umístěním tohoto řetězce v infikovaném souboru. Některé skenery používají pro důslednější identifikaci větší počet řetězců. Je velice těžké sladit skener tak, aby splňoval základní požadavky na velkou rychlost a spolehlivost. Kontrolována je především elektronická pošta, přenášené soubory a webové stránky. [8]

Heuristická metoda analýzy

Virové identifikační řetězce selhávají v případech polymorfních virů, kdy má tělo viru při každé replikaci jinou podobu. Heuristika je jednou ze základních možností, jak lze polymorfní viry identifikovat.

Principem heuristické analýzy je malý expertní systém, který sémanticky zkoumá úvodní instrukce programu a na základě databáze virových pravidel určuje, zda je program infikován či nikoliv. Heuristická metoda analýzy tedy nezkoumá přítomnost konkrétního viru, ale obecně viru jakéhokoliv. Cílem je zejména upozornit na podezřelý soubor, kdy je věcí uživatele zvážit možnost, zda se jedná o falešný poplach, či je-li program skutečně zavirován.

Samozřejmě, že ani tato metoda není všemocná, zejména v důsledcích způsobených častými obrannými mechanismy virů proti jejich analýze. Je-li program či virus vyzbrojen obranou proti krokování, dojde pochopitelně k selhání metody. Některé antivirové programy však disponují podporou softwarové emulace kódu, kdy instrukce nejsou skutečně prováděny a testování je proto naprosto bezpečné. Příkladem silně heuristicky zaměřeného antivirového programu je AVG. [8]

Léčitel (clean)

„Je-li úkolem skeneru virus najít, pak úkolem cleanu je nalezená virus odstranit.“ [8, s. 59]

Odstranění viru, zejména souborového, je věcí velice choulostivou. Obecně platí zásada, že nejlepší odvirování souboru je jeho obnovení ze záložní kopie. Některé viry totiž nejde odstranit z důvodu jejich přepisovacího charakteru, jiné viry nelze odstranit se zárukou z důvodu jejich programovacích chyb atp. Velkým problémem je mutace virů, kdy virus může být, díky značné podobnosti s jiným virem, mylně identifikován a jeho odstranění je pak logicky nekorektní.

Evolučním krokem ve vývoji odvinovacích programů je tzv. univerzální clean. Příkladem je program AVAST!, který si v jednom datovém souboru udržuje přehled o základních atributech souborů, jako jsou délka, datum a čas vytvoření, vlastní souborové atributy, kontrolní součet apod. Kromě těchto základních údajů jsou ukládány i originální hodnoty hlavičky EXE či sled úvodních instrukcí v případě programů *.COM. Tyto uložené originální údaje umožňují v případě infikace prodlužujícím virem jednoduše virus odseknout a vrátit tím infikovaný soubor na jeho původní velikost. Odvirováním je pak dokončeno obnovením hlavičky EXE resp. úvodních instrukcí v případě programu *.COM. [8]

Rezidentní štít

Možnost antivirové ochrany online. Rezidentní štít aktivním způsobem chrání počítač před virovou infiltrací v reálném čase. Nejčastěji jde o program typu skener, který provádí antivirovou kontrolu právě zpracovaných dat. Rezidentní štít tak může zakázat zkopírování zavirovaných souborů z diskety na pevný disk či zakázat spuštění infikovaného programu apod. Dokonalejší štíty nepracují na běžném skenovacím principu, který je časově velmi náročný, ale na principu databáze virových pravidel se zaměřením na vlastní viroví útoky. Kontrola volání krizových funkcí operačního systému je časově mnohonásobně úspornější nž databázové porovnání identifikačních řetězců. Další výhodou této metody je její univerzálnost i pro zachycení nových virů.

Za rezidentní variantu štítu lze považovat i rozličné online kontroly přicházející emailové pošty apod. [8]

Monitor diskových změn

Zaměřením monitoru je kontrola změn stavu na počítači, zejména spustitelných souborů. Nejedná se o standardní antivirový program, ale o program, který si pro své interní účely vytváří na disku databázi popisů základních atributů hlídaných souborů. Atributy jsou zejména délka souboru, datum a čas poslední aktualizace a hlavně kontrolní součet obsahu souboru. Kontrola atributu délky umožní detekci prodlužujících virů, kontrola kontrolního součtu pak detekci přepisujících virů. Duplicitní viry jsou registrovány vznikem nového duplicitního souboru COM na disku. Největší slabinou kontroly integrity dat je možnost jednorázově zaměřených virů, kdy po odmazání kontrolní databáze ztrácí kontrola svoji účinnost. [8]

3.3 Software

3.3.1 Firewall

„Firewally dovolují správcům sítě stanovit, kteří klienti v síti mohou přistupovat k síťovým prostředkům a které porty mohou být využívány zvnějšku pro přístup k síti.“ [4, s. 293]

Firewall je program, který chrání naše prostředky filtrováním síťových paketů. Zjednodušeně se dá říci, že firewall funguje jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Firewall pomáhá zabránit hackerům a škodlivému softwaru (např. viry) v získání přístupu k počítači prostřednictvím sítě nebo internetu. Brána firewall může taktéž zabránit tomu, aby počítač odesílal škodlivý software do jiných počítačů. [4]

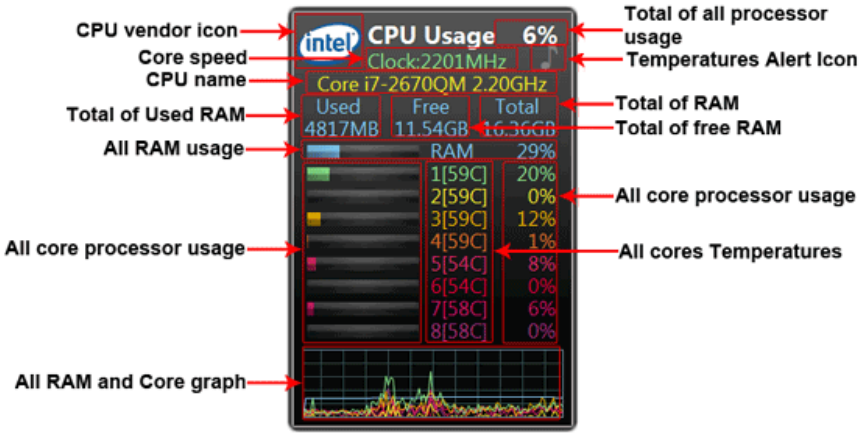
Firewally mohou běžet jako součást jiného softwaru. Kupříkladu naše kombinované zařízení přístupového bodu Wi-Fi a směrovače téměř jistě nabízí nějakou formu firewallu. Firewally mohou také na počítačích běžet jako samostatné programy. Na speciálních serverech vyhrazených pro tento účel mohou běžet také sofistikované firewally, i když taková situace obecně nastává až v kombinacích na podnikové úrovni. [12]

Operační systém Windows obsahuje software osobního firewallu v sobě zdarma.

3.3.2 Měřící programy

3.3.2.1 All CPU Meter

Je nejpopulárnější a nejpoužívanější gadget pro Windows. Tento malý prográmek umí zobrazovat využití procesoru (až 2 procesory, 16 jader a 32 vláken), využití RAM, CPU frekvenci a jméno procesoru (Intel nebo AMD). Taktéž umí zvukově notifikovat uživatele pro volitelné události (např. teplota CPU) nebo zobrazovat dodatečné informace ohledně procesoru, operačního systému, základní desky, BIOSu a počítačového systému. [13]

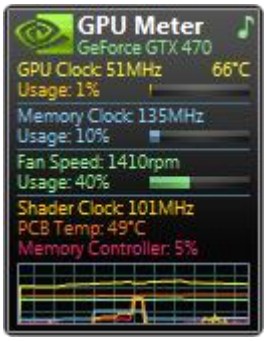


Obrázek 1: All CPU Meter [13]

3.3.2.2 GPU Meter

Zobrazuje informace o grafické kartě – název grafické karty (výrobce), GPU taktovací rychlost, teplotu grafického čipu, celkové vytížení grafiky (procentuální i vizuální zobrazení), paměťovou taktovací rychlost, celkové využití paměti (procentuální i vizuální), rychlost otáček větráčku (v RPM – revolutions per minute) a celkové využití větráčku (procentuální i vizuální zobrazení) a jiné.

Celkové GPU využití lze být zobrazeno v dvou různých grafech. V nastavení lze nastavit velikost tohoto gadgetu až na 400%, vybrat mezi zobrazování teploty v stupních Celsia či stupních Fahrenheit. Také lze nastavit barvu pozadí a barvu textu, nebo nastavit automatické aktualizace. [14]



Obrázek 2: All CPU Meter [14]

3.3.2.3 Drives Meter

Zobrazuje informace o discích v počítači. Lze zobrazovat až 8 HDD, SSD či flash disky. Tento programek umí měřit diskovou aktivitu, využité místo na disku, volné místo na disku, celkové místo na disku umí zobrazit pomocí lišty (vizuální zobrazení), čtecí/zapisovací rychlosti a jiné.

Další vlastnosti a informace lze zobrazit kliknutím na určitý disk, posléze vyskočí okno s těmito informacemi: model disku, sériové číslo, kapacitu, index, počet celkových cylindrů, počet sektorů, počet hlav a další.

Ve vlastnostech lze nastavit velikost tohoto měřícího zařízení až na 400%, změnit obnovovací rychlost, nastavit dané měřítko (bit/byte, kilobit/kilobyte nebo megabit/megabyte, zobrazit či schovat graf, nastavit barvu pozadí a barvu textu či nastavit automatické aktualizace. [15]

Obrázek 3: All CPU Meter [15]

3.4 Hardware

3.4.1 Základní deska

„Podle názvu není těžké odvodit, že právě tato komponenta zaručuje kooperaci všech ostatních součástí. Právě do základní desky totiž vložíte procesor, operační paměť, grafickou kartu nebo do ní připojíte jednotlivé pevně disky a optické mechaniky.“ [2, s. 5]

Dá se tedy zjednodušeně říci, že základní deska je komponenta, jejíž hlavní funkcí je propojit všechny součásti a poskytnout jim potřebné napájení. Jak plynul čas, výrobci si uvědomili, že je vhodné poskytovat zákazníkům více služeb, a tak se v současnosti na základní desku integrují součásti jako zvukové, síťové a grafické karty.

Nejdůležitější částí celé desky je osazený čip, který se nazývá čipset, nebo také čipová sada. Její typ určuje, jaký procesor a jakou operační paměť budeme moci do základní desky vložit. Tato řídící jednotka se zpravidla skládá z dvojice čipů pojmenovaných jako northbridge a southbridge (severní a jižní můstek), kdy každý plní lehce odlišnou funkci, ale celkově spolu samozřejmě stále komunikují a vyměňují si nezbytné řídící a signalizační zprávy. Dělení čipsetu na dvojici samostatných čipů bylo provedeno především z toho důvodu, že je takovéto řešení podstatně jednoduší na výrobu a produkce nestojí tolik financí.

Mezi hlavní výrobce čipových sad se v současnosti řadí především Intel a AMD. Tyto společnosti se postupně předhánějí v poskytování nejzajímavějších řešení a výrobci základních desek s úspěchem nabízejí koncovým zákazníkům nespočet různých variant svých produktů.

Pro připojení dalších součástí jsou na základní desce umístěny výstupy v podobě konektorů a slotů, kdy každý odpovídá některé z potřebných vlastností. Obecně tato vstupně-výstupní rozhraní dělíme na interní (přímo na základní desce a jsou určena pro připojení komponent uvnitř počítače) a na externí (na zadní straně počítače a jsou přímo dostupná) pro připojení periferních zařízení jako jsou monitor, myš, klávesnice, sluchátka apod. [2]

3.4.2 Procesor

„Procesor neboli CPU (Central Processing Unit) je hlavní součástí počítače, která plní funkci mozku, většiny počítačem prováděných operací.“ [2, s. 41]

Jeho pracovní náplní je postupně načítat jednotlivé instrukce z operační paměti a na jejich základě pak vykonávat cely program. Po základní desce, na které se nachází čipset, je jeho přítomnost druhou nejdůležitější. Základní deska je hlavním prvkem, který umožňuje jednotlivým komponentám mezi sebou komunikovat a provádět potřebnou kooperaci k zajištění správné funkce počítače. Procesor pak všechny tyto součásti řadí, určuje, co mají kdy vykonat a jak to mají provést. Právě kvůli tomu je celková rychlost procesoru velmi rozhodující při posuzování celkového výkonu počítače.

Na celkovém výkonu se samozřejmě podílí i nespočet dalších prvků, jejich funkce by ale bez pořádného procesoru nemohla být využita – procesor je tedy hlavním řídícím mozkem celé sestavy a bez jeho adekvátních parametrů není možné využít potenciál jiných výkonných komponent. [2]

3.4.3 Grafická karta

Grafická karta zajišťuje tvorbu obrazu, který potom vidíme na monitoru. Spolu s monitorem tvoří dohromady zobrazovací soustavu počítače. Bez grafické karty a monitoru bychom nemohli kontrolovat a řídit činnost počítače, zadávat údaje, přijímat výsledky apod. Proto je grafická karta nutnou součástí každého počítače.

Grafická karta má tvar běžné přídavné karty. Na desce je umístěn grafický procesor, paměťové čipy a další potřebné obvody. V současné době se pro grafické karty používají dva typy sběrnic. Jednak je to sběrnice PCI, která je díky svým vlastnostem určena pouze pro starší grafické karty. Většina moderních grafických karet se zasunuje do slotu AGP, který byl speciálně navržen pro grafické karty. V porovnání s PCI získáme vyšší výkon a menší zatížení počítače.

Na zadní straně grafického adaptéru najdeme konektor pro připojení monitoru. Některé typy karet obsahují ještě další konektory. Je-li např. karta vybavena výstupním TV konektorem, získáme možnost připojit počítač k televiznímu přijímači. Tato varianta je výhodná například při sledování filmů nebo při přehrávání DVD v počítačové mechanice.

Některé počítače mají grafickou kartu integrovánu na základní desce. To znamená, že v počítači nenajdeme samotnou (vyjímatelnou) grafickou kartu. Takovou desku poznáme podle toho, že konektor pro připojení monitoru se nachází přímo na desce nebo je k ní připojen pomocí plochého kabelu. Nevýhodou integrované grafické karty je to, že ji nelze vyměnit v případě poruchy ani v případě, že potřebujeme kartu výkonnější. U kvalitních desek lze však takovou kartu vyřadit z provozu.

Grafická karta dnes bývá zpravidla připojena přes sběrnici PCI Express, zatímco dříve nejčastěji přes dedikované AGP a ještě dříve přes opět univerzální PCI. [2]

3.4.4 Datová úložiště

Pevné disky

Z anglického názvu Hard Disk Drive neboli HDD byl odvozen český pojem pevný disk. Jedná se o zařízení, které slouží k dlouhodobému uložení velkého množství dat v počítačích. Technologie se za dobu své existence dostala na přední pozice mezi způsoby dlouhodobého uložení dat, a to především díky nízké ceně za danou kapacitu. Relativně

vysoká přenosová rychlost a trvanlivost uložených dat bez nutnosti stálého napájení činí z klasických pevných disků ideální nástroj k ukládání všech dat.

Jako jedna z mála technologií nezaznamenaly pevné disky za dobu své existence žádné výrazně změny. Jedná se stále o zcela totožný princip uložení dat, stejně jako jejich čtení i zápis. Jedinou výraznou změnou je podstatné navýšené kapacity spolu s maximální rychlostí přístupu k datům. Díky miniaturizaci bylo navíc možné výrazně snížit celkové rozměry při zachování stejných nebo dokonce vyšších kapacit. [2]

SSD disky

Solid State Drive (SSD) neboli „polovodičový disk“, je typ úložného zařízení, alternativa ke klasickým pevným (HDD) diskům. Je založena na soustavě energeticky nezávislých flash pamětí, které jsou osazeny na destičce tištěného spoje. K zajištění plné náhrady za mechanické harddisky jsou SSD vyráběny ve stejných velikostech a komunikují s PC přes stejná rozhraní (SATA i PATA).

Hlavním rozdílem mezi SSD a HDD je absence mechanických součástí u SSD. Solid state disky složení pouze z elektronických součástek nelze tak snadno mechanicky poškodit (nejsou náchylné na otřesy), nevydávají rušivé zvuky ani vibrace. Při práci potřebují méně elektrické energie a dosahují vysokých rychlostí díky velmi nízkým přístupovým dobám. Hlavní nevýhodou je prozatím jejich cena, který znemožňuje dosahovat tak vysoké kapacity, jako u HDD. [11]

3.4.5 Operační paměť

Operační paměť je v počítači prezentována tzv. RAM (Random Access Memory). Ve své podstatě se jedná o elektronické obvody ukládající data a umožňující k nim přistupovat v libovolném pořadí. Libovolné pořadí vlastně představuje situaci, kdy jakákoliv data z paměti mohou být okamžitě načtena bez ohledu na jejich fyzické umístění a na to, zda mají nějakou souvislost s jinými buňkami v paměti. Tento způsob přístupu je vlastně přesně opačný něž u pevných disků nebo optických médií, kde je potřeba, aby se čtecí hlava postavila přesně na potřebné místo – to má za následek značné zdržení. Tato prodleva je obecně výrazně delší než doba potřebná k samotnému čtení dat.

Stejně jako u procesoru je i operační paměť vlastně integrovaný obvod vytvořený z milionů tranzistorů a kondenzátorů. Ve valné většině případů je jako operační paměť

využíváno dynamického řešení, které využívá spojení tranzistoru a kondenzátoru k vytvoření paměťové buňky. Každá buňka reprezentuje vždy jeden bit z uložených dat, a to tak, že kondenzátor udržuje logickou informaci (1 nebo 0) a tranzistor umožňuje celému obvodu zjistit aktuální stav a případně jej změnit. [2]

4 Vlastní zpracování

Testovací prostředí

Testování bude prováděno na stolním počítači s operačním systémem Windows 10 Pro v 64bitové verzi, Intel Core i5-3470 CPU @ 3.20GHz s 16 GB DDR3 RAM, grafickou kartou NVIDIA GeForce GTX 760 s 2048 MB paměti, 1TB Western Digital HDD a 250GB Samsung SSD.

Testovací proces

Měření bude probíhat na stále stejném stroji, jehož technické specifikace jsou popsány výše. Před každým měřením bude resetován počítač a nechána systému krátká chvíle – většinou do 5 minut, na dokončení všech systémových procesů spojených se spuštěním operačního systému, které by mohly skreslit měření. Systémové procesy budou monitorovány s pomocí Windows Task Manageru, tak i s pomocí trojice widgetů CPU Meter, Drives Meter a GPU Meter.

Nejprve bude měřeno bez nainstalovaného antivirového programu. Následně postupně nainstaluji každý z vybraných antivirových programů a bude testováno zatížení CPU, GPU a disku během hloubkového scanovaní.

Testovací kritéria

První kritérium je cena licence na 1 rok, klasicky pro jedno zařízení a v základní verzi.

Druhé kritérium změří zatížení CPU, a to s pomocí programu Sony Vegas Pro 12.0, v kterém se bude dvouminutové video ve fromátu avi konvertovat do formátu mp4 HD 1080p. Měřen bude čas potřebný k plné konverzi videa.

Třetí kritérium je zaměřeno na grafickou kartu, a to s pomocí benchmarku Cinebench, který provede sérii měření a pak následovně vyhodnotí, jak si stím grafická karta poradila. Měřen zde bude čas potřebný k celkovému dokončení OpenGL (grafického) testu.

Čtvrté kritérium se týká převážně CPU, ale i v menší řadě zatížení disku a grafické karty. Zde bude opět měřen čas, který benchmark bude potřebovat k dokončení svého testu.

Druhé, třetí a čtvrté kritérium bude testováno obdobně a to s pomocí tzv. hloubkového scanování.

Hloubkové skenování systému pro hledání virů má negativní dopad na celkový výkon počítače, jelikož se antivirový program musí dělit ostatními aplikacemi o počítačový výkon. Když prováníme regulérní real-time scanování, většina novodobých antivirových programů je dobrá natolik, že si sami dokáží delegovat vlastní výkon, kterým zatěžují v pozadí počítač, a tím se jim daří méně či vůbec zatěžovat ostatní aplikace a běh systému. Oproti tomu provádění hloubkových scanů, často znatelně zatíží systém potřebami scanování natolik, že scanování má velký dopad na celkový výkon počítače a aplikací. Hloubkovým scanovaním je myšleno takové scanování, kdy antivirový program aktivně scanuje každý soubor na každé particii danného disku.

Páté a poslední kritérium je efektivnost antivirového programu v reálném prostředí. Zde budou data převzata z internetových stránek AV-Test.org.

Data budou převzata a ne měřena hlavně proto, že je velmi riskantní mít počítač plný nejnovějším malware a virů v době, kdy jsou všechny počítače prakticky připojeny na internet. Risk vypuštění malware na intranet či internet je příliš velký.

Testování efektivnosti léčení virů je dnes již už prováděno nezávislými organizacemi, např. AV-Test a AV-Comparatives. Pro potřeby mé práce jsem si vybral AV-Test.org. Během listopadu a prosince 2015 AV-Test nepřetržitě monitoroval mimo jiné, mnou zvolené čtyři antivirové programy, a to na jejich základní nastavení. Bylo jim dovoleno se průběžně Updatovat nebo dotazovat se jejich příslušné Cloud služby. Zaměřili se na reálné scénáře a na prověření produktů vůči skutečným hrozbám ve světě.

V tabulkách kritéria efektivnosti budou hodnoceny tři parametry – ochrana, výkon a použitelnost.

Ochrana

Ochrana proti malware infekcím (virusy, červy a trojani), ochrana proti 0-day[5] malware útokům, včetně webových a e-mailových hrozeb

[5] Zero day, zero day attack (zneužití či útok nultého dne) je v informatice označení útoku nebo hrozby, která se v počítači snaží využít zranitelnosti používaného software, která není ještě obecně známá, resp. pro ni neexistuje obrana.

Výkon

Výkon hodnotí průměrný vliv antivirového programu na každodenní využívání počítače. Dále také navštěvování webových stránek, stahování software , instalování a spouštění programů a kopírování data.

Použitelnost

Použitelnost, nebo také vytížení počítače hodnotí dopad antivirového programu na celý počítač. Jsou zaznamenávána falešná varování nebo blokování webových stránek, falešné detekce legitimních software jako malware během systémového scanování, falešná varování a blokování během instalování či používání legitimního software.

Stanovení požadovaných vlastností

Těchto pět kritérií bylo sestaveno podle základních vlastností, které by každý antivirový program měl splňovat. Cena je vždy důležitá, a tudíž je prvním kritériem. Následují tři měřená kritéria, která se zaměří na testování hardwaru daného počítače. Tyto testy byly navrženy tak, aby pokryly co největší škálu hardwaru – procesor, grafická karta a disková jednotka. Páté kritérium je navrženo a implementováno tak, aby doplnilo předešlé kritéria o data z reálného prostředí, proti reálným hrozbám a jejich potenciálním hledáním.

4.1 ESET Smart Security 9

Testování proběhlo na verzi ESET Smart Security 9. Tato verze antivirového (AV) programu má jako základ ESET NOD32 Antivirus, další funkce (Anti-Theft, personální firewall, rodičovská kontrola či Antispam) obsažené v této verzi jsou nadstavbové a nemají vliv na výsledky měření.

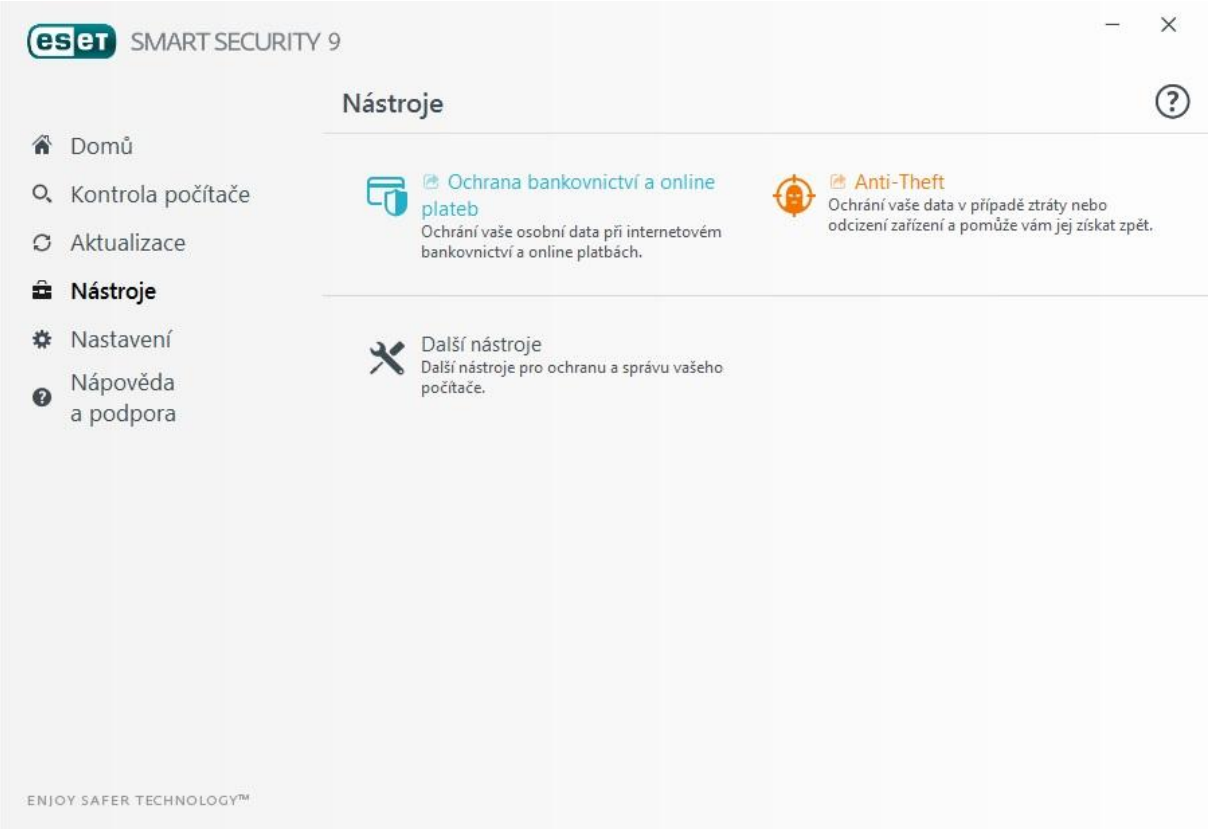
Hlavní menu vypadá takto:

Obrázek 4: Eset hlavní menu

Pod volbou Kontrola počítače se skrývá možnost si zvolit, jakou kontrolu uživatel chce spustit. Je na výběr Kontrola všech disků (celého PC), Volitelná kontrola – kde si lze navolit jaké disky či složky a jak podrobně scanovat a nakonec je tu možnost Kontroly výměnných médií – to jsou USB, DVD, CD a další.

Za povšimnutí z nabídky Nástroje bezpochyby stojí funkce Anti-Theft (česky anti-krádež) – viz Obr. 5. Po přihlášení do Anti-Theft programu ESET uživateli pomůže vystopovat ztracené zařízení. Dokáže pořizovat fotografie z webkamery nebo pomocí mapy zobrazit pozici, kde se ukradené zařízení právě nachází. Nakonec lze i poslat zprávu nálezci

zařízení i s potenciálním důkazem ve formě fotografie z webkamery. Funkcí Anti-Theft se ESET odlišuje od konkurence a pro uživatele notebooků může být jedním z kritérií pro volbu právě antivirového programu ESET Smart Security 9. Pro uživatele desktopů, tedy stolních počítačů, je však tato funkce nepodstatná.



Obrázek 5: Eset menu nástroje

Cena pro roční licenci ESET Smart Security 9 stojí 1490 Kč. [21]

Pro ESET jsou naměřené hodnoty v následující tabulce:

Tabulka 1: Eset výsledky měření

	Eset [min]	bez AV [min]
Sony Vegas	5:44	5:00
benchmark GPU	0:51	0:51
benchmark CPU	1:42	1:29

Tabulka 2: Eset výsledky efektivnosti

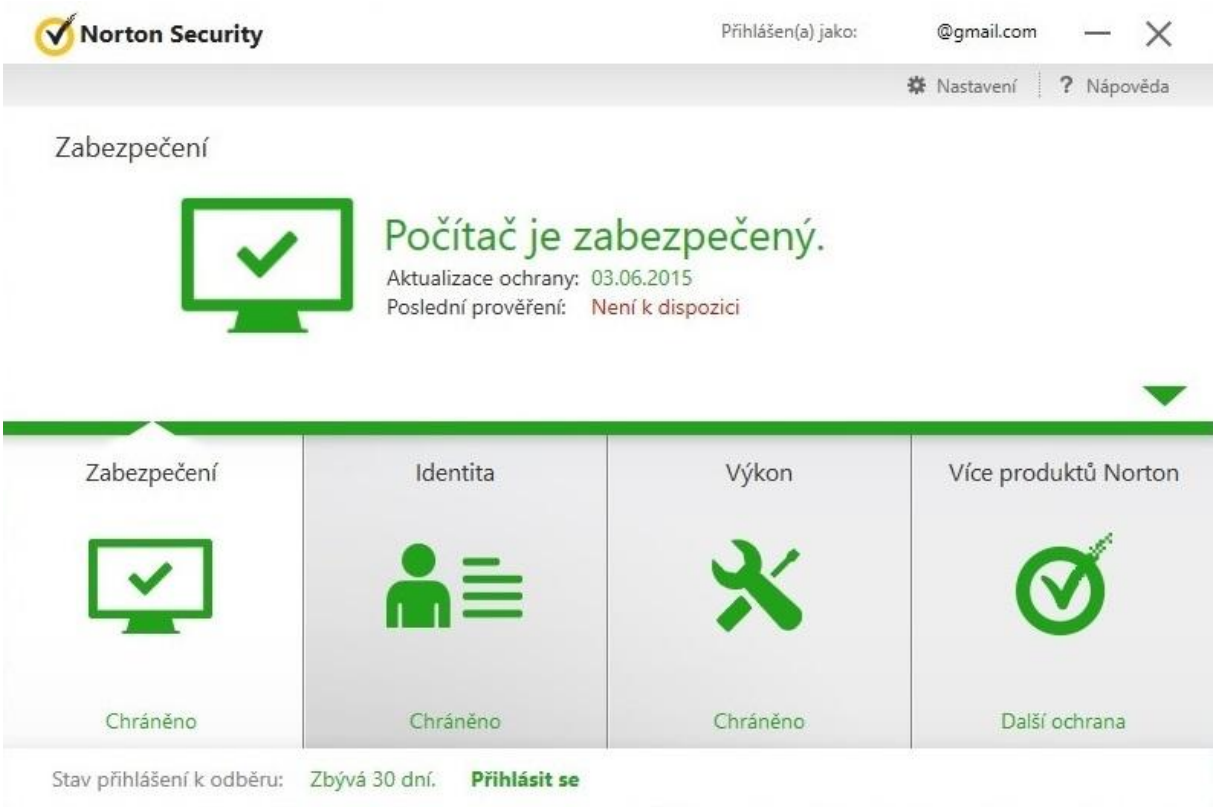
	Ochrana [body]	Výkon [body]	použitelnost/vytížení [body]
AV-Test	4,5/6	4/6	5,5/6

Zdroj: [18]

4.2 Norton Security Deluxe

Testovací verze Nortonu byla právě verze Norton Security Deluxe, protože o třídu nižší verze Norton Security Standard nebyla přístupná ve free trial verzi. Obě verze se od sebe liší pouze počtem licencí, verze Standard má pouze jednu licenci a verze Deluxe má licencí pět. V cenovém kritériu budu pracovat ale s verzí Standard.

Základní menu Nortonu vypadá takto:

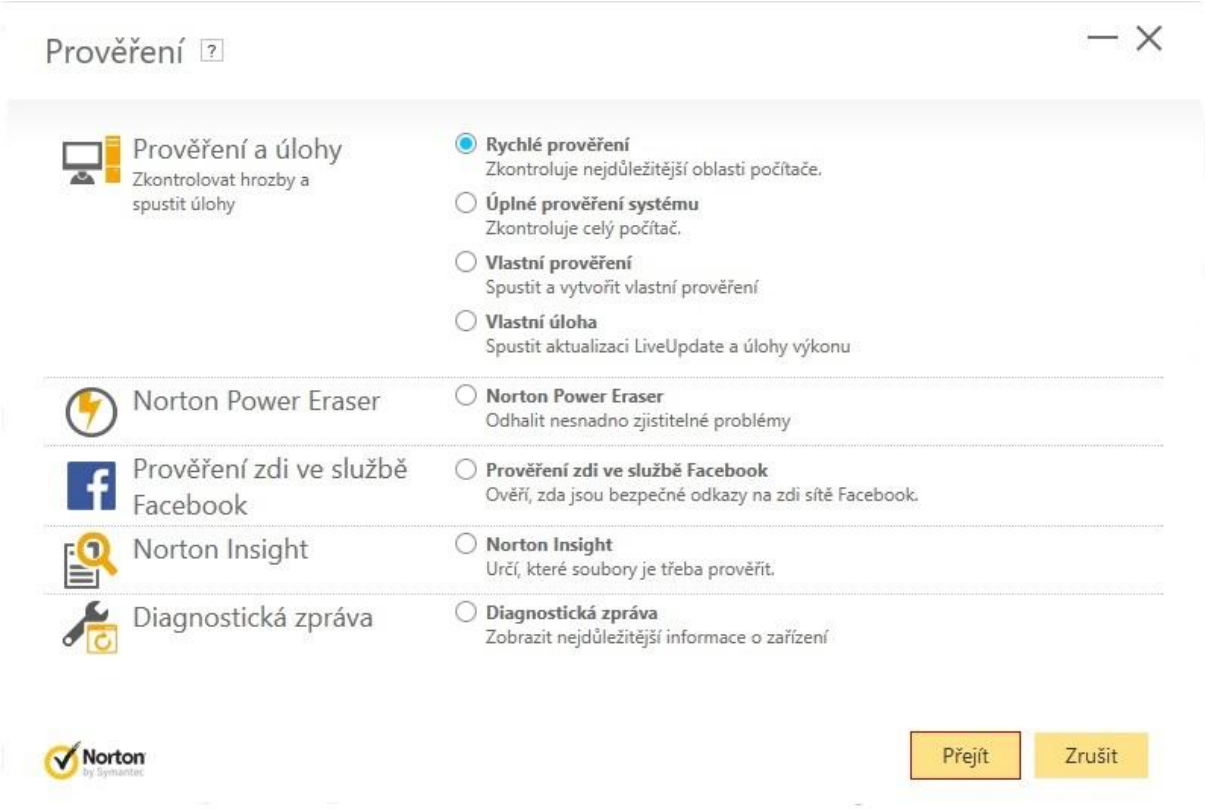


Obrázek 6: Norton menu

Ze základních tří nabídek Zabezpečení, Identita a Výkon se uživatel dostane do dalších nabídek. Za zmínku zde stojí z volby Výkon funkce Optimalizovat disk což je v podstatě malá defragmentace disku, dále funkce Vymazání souborů, která se postará o dočasné soubory systému Windows a dočasné soubory aplikace Internet Explorer. Zajímavá je i funkce Správce spuštění, která vypíše všechny programy, které se spouštějí při zapnutí počítače, vypíše jejich dopad (nízký, střední, vysoký) na využití prostředků, a nabídne možnost Zpozdit spuštění.

Z volby Identita lze nastavit mnoho různých vlastností Nortonu. Je zde např. fuknce Blokování nebezpečných stránek, Ochrana proti phishingu a Scam Insight (identifikace webových stránek, které požadují citlivé osobní údaje).

Z menu Zabezpečení se uživatel dostane mj. i ke klasické volbě scanování disku proti hrozbám. Za povšimnutí zde stojí funkce Prověření zdi ve službě Facebook, která ale po vyzkoušení napsala, že Facebook už neposkytuje potřebná data ke scanovaní zdi, a tudíž tato funkce nefunguje.



Obrázek 7: Norton možnosti prověření

Standardní verze Norton stojí 899 Kč. [22]

Naměřené hodnoty pro Norton jsou v následující tabulce:

Tabulka 3: Norton výsledky měření

	Norton [min]	bez AV [min]
Sony Vegas	5:37	5:00
benchmark GPU	0:51	0:51
benchmark CPU	1:48	1:29

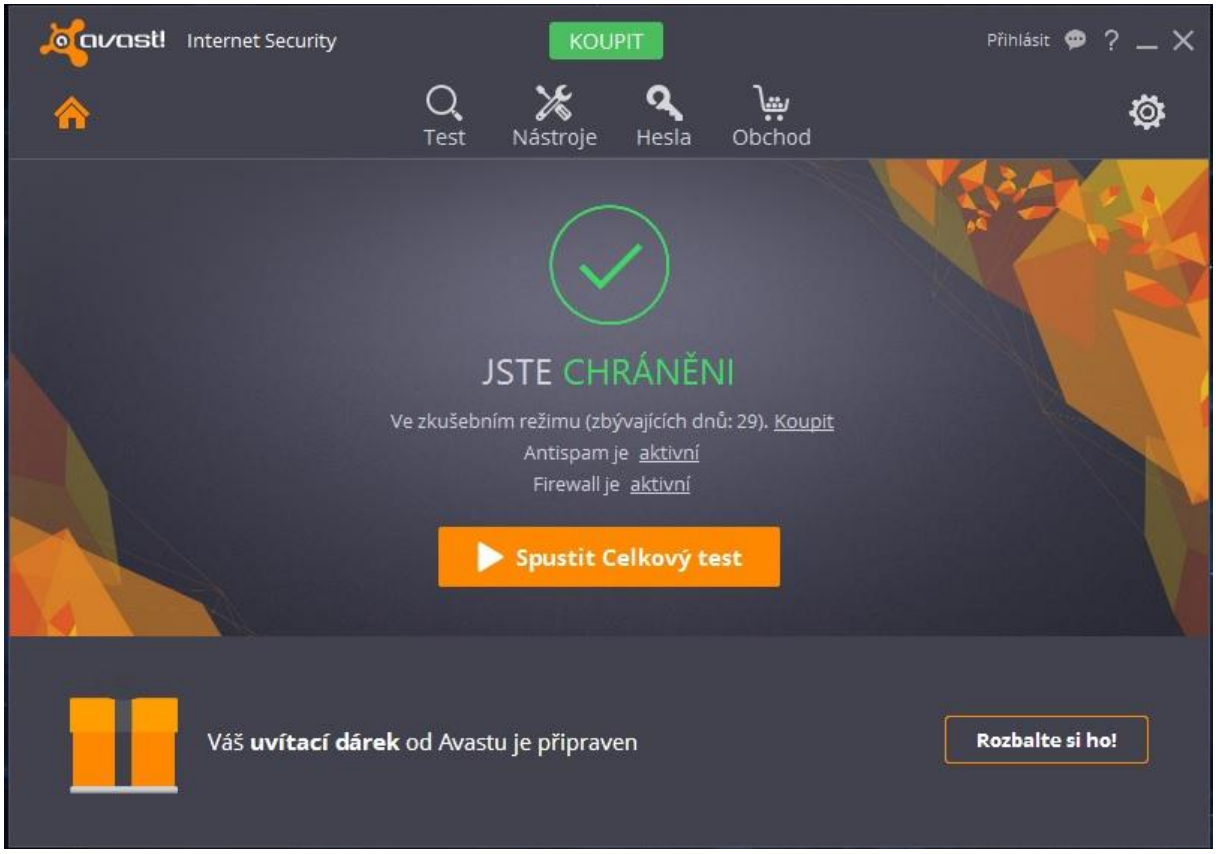
Tabulka 4: Norton výsledky efektivnosti

	Ochrana [body]	Výkon [body]	použitelnost/vytížení [body]
AV-Test	6/6	5/6	5,5/6

Zdroj: [20]

4.3 Avast! Internet Security

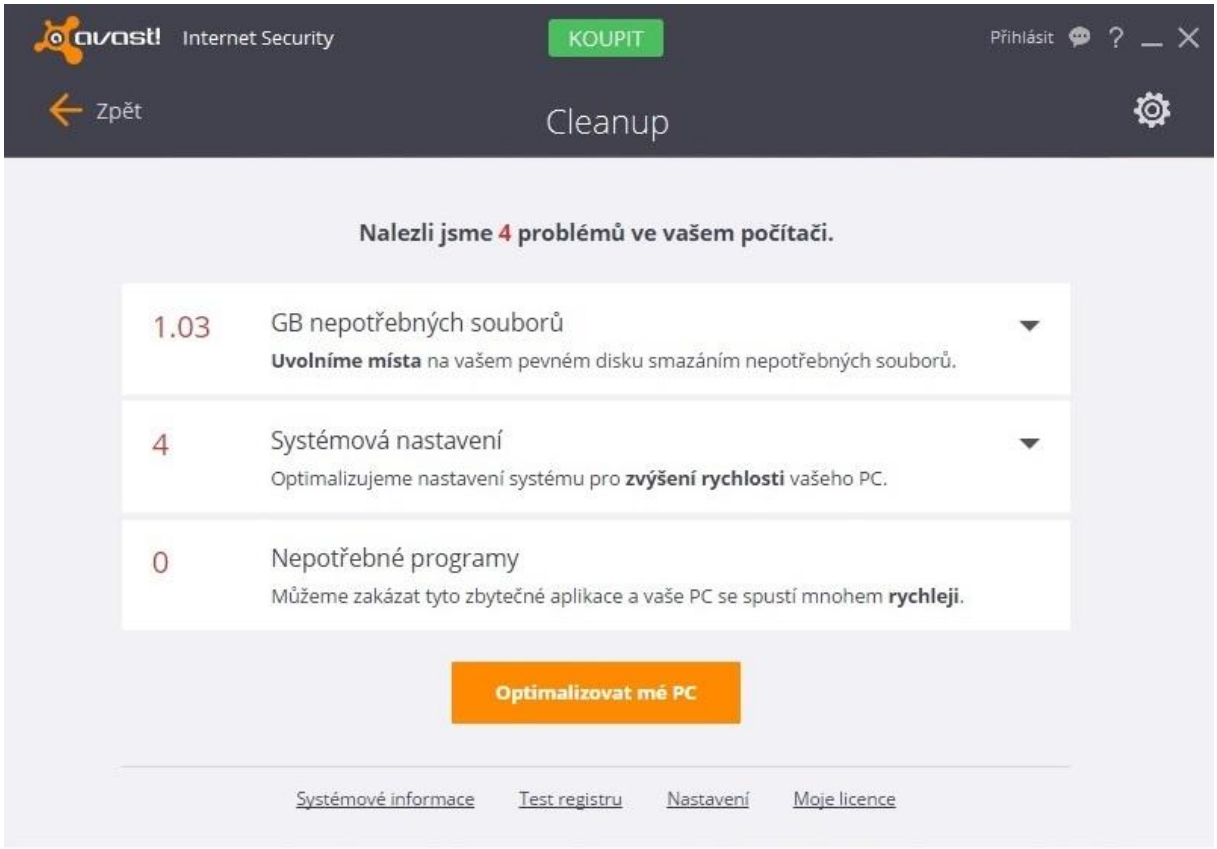
Testování proběhlo na verzi Internet Security, což je prostřední volba z celkových tří nabízených verzí. Hlavní nabídka vypadá takto:



Obrázek 8: Avast! základní menu

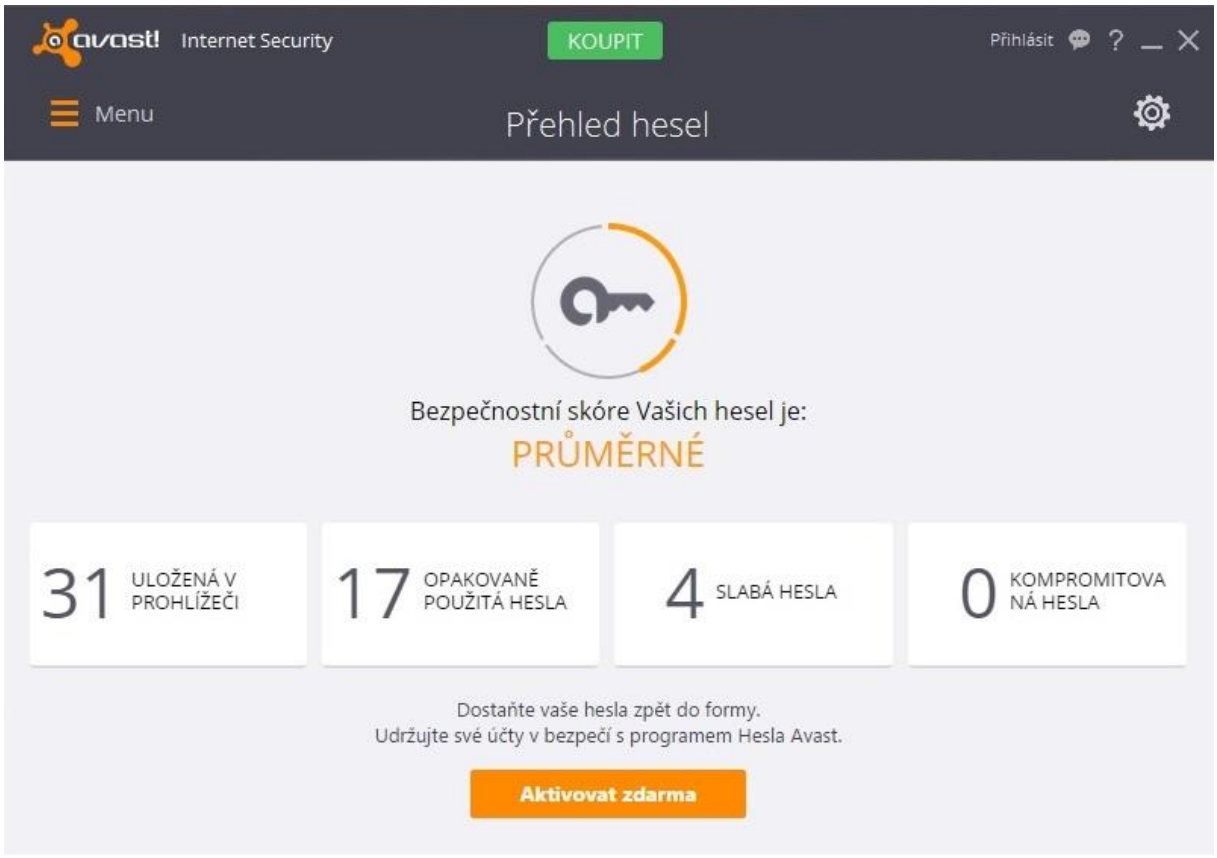
Z menu Test se uživatel dostane do šesti možností, co a jak hledat a testovat. Mimo obvyklých testovacích nabídek (Celkový test a Hledat viry), je zde i možnost volby Hledat zastaralý software, což by mělo pomoci urychlit chod počítače aktualizováním daných software (IrfanView, Flash Player ActiveX, Adobe Reader aj.). Zajímavá na první pohled je také funkce Hledat výkonnostní problémy, ale právě volba je trošku nečekaně zpoplatněná na 440 Kč za rok. Zde Avast! pouze vypíše počet „problémů“, které našel, a které jsou podle něj potřeba optimalizovat. V podrobnějším přehledu de sice problémy dále zkoumat, ale běžnému

uživateli nic neřeknou a je jen na něm, jestli Avastu bude věřit, a zda si optimalizační Add-on koupí.



Obrázek 9: Avast! možnosti optimalizace

Třetí hlavní záložka je správa Hesla. Zde zaujala práce Avastu z hesly uložených v počítači, resp. v internetovém prohlížeči Google Chrome. Funkcí Zkontrolovat moje hesla se uživatel dostane do přehledu svých uložených hesel. Avast! následně přehledně vypíše (Obr. 10), jaká je uživatelova úroveň bezpečnosti hesel, a jestli je nějaké heslo kompromitováno. Přes tlačítko Aktivovat zdarma, se uživatel dostane do prostředí, kde si lze nastavit jedno hlavní heslo, které bude použito ke každému účtu. Nevýhodou je, že toto heslo si musí uživatel důkladně zapamatovat, protože Avast! ho nedokáže obnovit.



Obrázek 10: Avast! přehled hesel

Avast! Internet Security stojí 690 Kč na rok. [Avast! obchod v antivirovém programu]

Pro Avast! jsou naměřené hodnoty v následující tabulce:

Tabulka 5: Avast! výsledky měření

	Avast! [min]	bez AV [min]
Sony Vegas	5:25	5:00
benchmark GPU	0:55	0:51
benchmark CPU	1:43	1:29

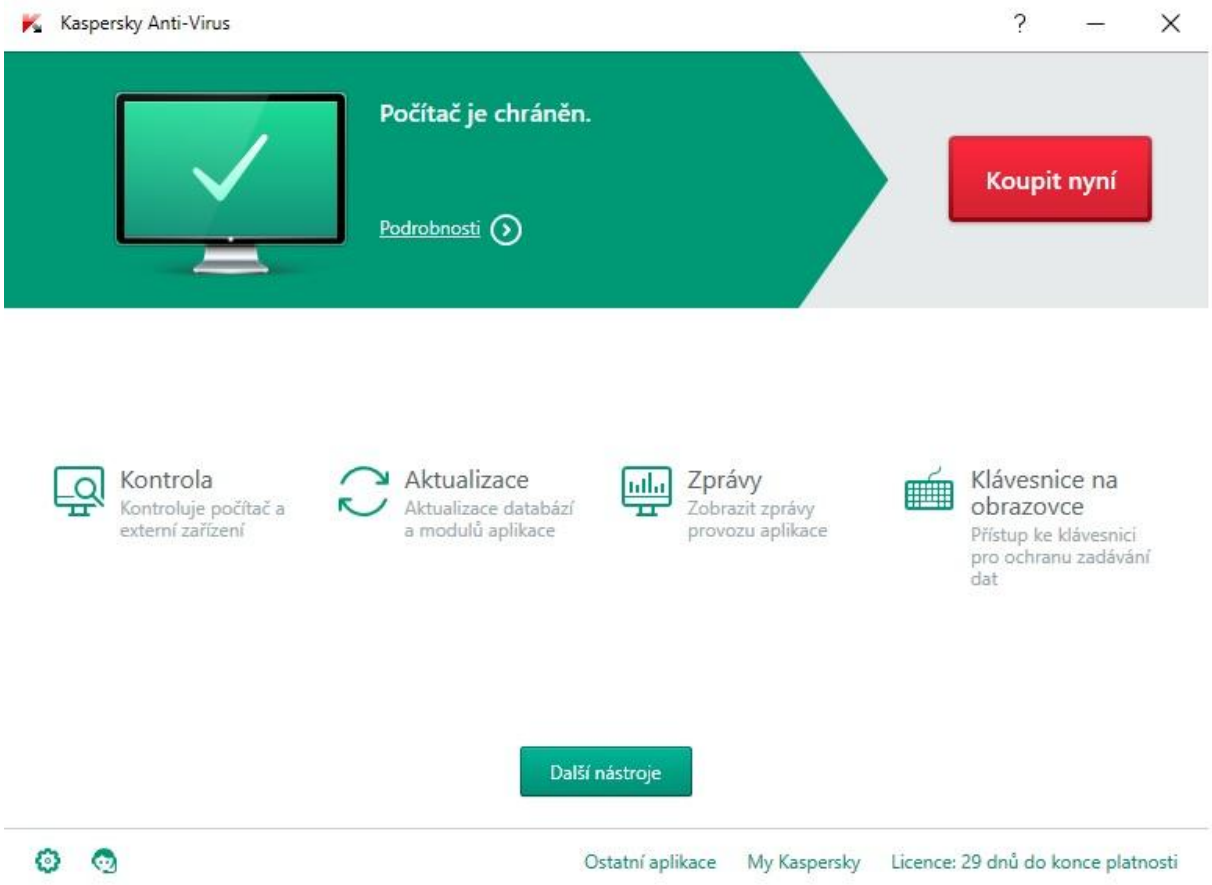
Tabulka 6: Avast! výsledky efektivnosti

	Ochrana [body]	Výkon [body]	použitelnost/vytížení [body]
AV-Test	6/6	5/6	6/6

Zdroj: [17]

4.4 Kaspersky Anti-Virus

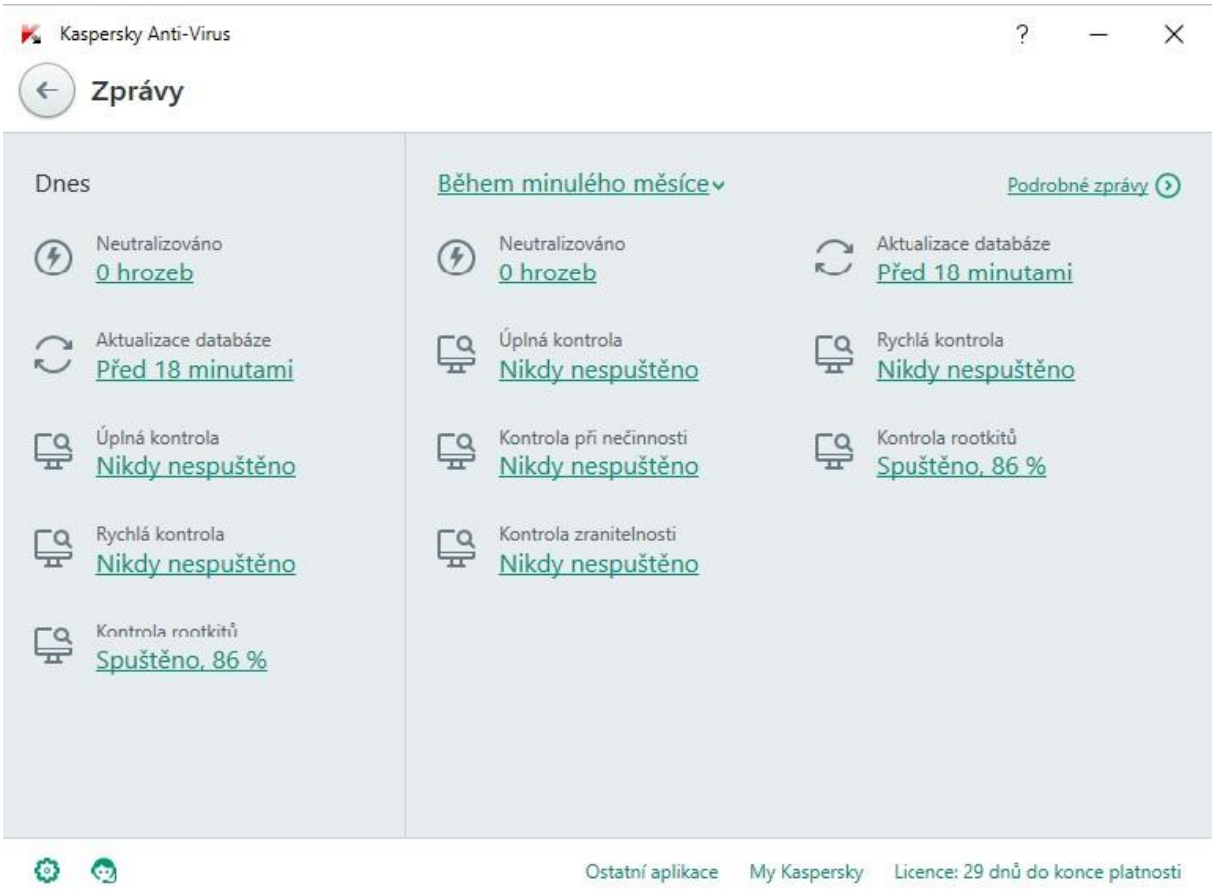
Testováno bylo na verzi Kaspersky Anti-Virus 2016 pro jeden počítač. Hlavní nabídka vypadá takto:



Obrázek 11: Kaspersky hlavní menu

Z možnosti Kontrola se uživatel dostane do klasického menu, kde si může zvolit různé typy kontroly, jak rychlého typu, přes kontroly externích disků, po dlouhé hloubkové kontroly celého PC.

Co Kaspersky má jiné oproti konkurenci je funkce Zprávy, která přehledně ukáže vše, co se dnes a za předešlý měsíc událo a kontrolovalo (Obr. 12).



Obrázek 12: Kaspersky Zprávy o kontrolách

Nad funkcí Klávesnice na obrazovce jsem se ale musel pozastavit. Windows klasicky umožňují přesně tuto funkci, stačí do hledání napsat keyboard, a Windows sám najde On-Screen Keyboard, která má sloužit přesně proti keyloggerům, tedy samozřejmě kromě psaní bez hardwarové klávesnice.

Pod tlačítkem Další nástroje se skrývá několik dalších pokročilejších nástrojů, jako např. Cloudová ochrana, karanténa, mazání soukromých údajů a Kaspersky Rescue Disk.

Osobně hodnotím Kaspersky Anti-Virus jako nejvíce intuitivní, má nejjednodušší základní menu kde je dle mého názoru přesně to, co běžný uživatel potřebuje ke správě antivirového programu.

Cena za roční licenci je 539 Kč. [23]

Pro Kaspersky jsou naměřené hodnoty v následující tabulce:

Tabulka 7: Kaspersky výsledky měření

	Kaspersky [min]	bez AV [min]
sony vegas	5:45	5:00
cinebench openGL	0:53	0:51
cinebench cpu	1:52	1:29

Tabulka 8: Kaspersky výsledky efektivnosti

	Ochrana [body]	Výkon [body]	použitelnost/vytížení [body]
AV-Test	6/6	6/6	6/6

Zdroj: [19]

4. 5 Vyhodnocení výsledků měření

Přehled cen (v Kč):

Tabulka 9: Cena za licenci

	Eset	Norton	Avast!	Kaspersky
cena za licenci	1490	899	690	539

Zdroj: [21] [22] [23] [Avast! obchod v antivirovém programu]

Přehled bodového ohodnocení. Body jsou chápány jako čím více, tím lépe.

Tabulka 10: Dosažené body v ceně za licenci

Body	Název antivirového programu
4	Kaspersky
3	Avast!
2	Norton
1	Eset

Tabulka 11: Výsledky měření

	Eset [min]	Norton [min]	Avast! [min]	Kaspersky [min]	bez AV [min]
Sony Vegas Pro	5:44	5:37	5:25	5:45	5:00
cinebench GPU	0:51	0:51	0:55	0:53	0:51
cinebench CPU	1:42	1:48	1:43	1:52	1:29

První ze série měřených testů je test renderovaní videa v programu Sony Vegas Pro. Tento test byl zaměřen na zatížení CPU (100 % u všech 4 jader), disk byl zatížen jen minimálně (kolem 10 %), jak postupně ukládá renderované video a grafický čip byl zatížen ještě míň (5 %).

Druhým měřením byl test přímo na grafický čip. Testováno bylo pomocí benchmarku Cinebench. Tento test byl nejvyrovnanější, a to dle mého názoru proto, že antiviry a celkově skenování disků (jak hluboké tak i rychlé) nepotřebují vůbec grafickou kartu jako systémový zdroj. Tento test zatížil CPU kolem 50 %, disky vůbec a GPU na 65 %.

Třetí a poslední měřený test byl zaměřený na CPU, a to konkrétně vykreslováním komplikovaného obrazce. Test byl znovu prováděn za pomocí benchmarku Cinebench. Tento test zatížil všechny jádra CPU na 100 %, disky vůbec a grafiku jen minimálně – kolem 1 %.

V následujících tabulkách budou časy jednotlivých měření přepočítány na bodové hodnocení. Nejrychlejšímu času budou přiděleny čtyři body, druhému nejrychlejšímu času tři body atp. V přepočítávání na body nebude bráno v úvahu, jak velké jsou rozdíly mezi jednotlivými naměřenými časy.

Tabulka 12: Dosažené body v renderování videa v Sony Vegas Pro

Body	Název antivirového programu
4	Avast!
3	Norton
2	Eset
1	Kaspersky

Tabulka 13: Dosažené body v GPU benchmark

Body	Název antivirového programu
4	Eset
4	Norton
3	Kaspersky
2	Avast!

Tabulka 14: Dosažené body v CPU benchmark

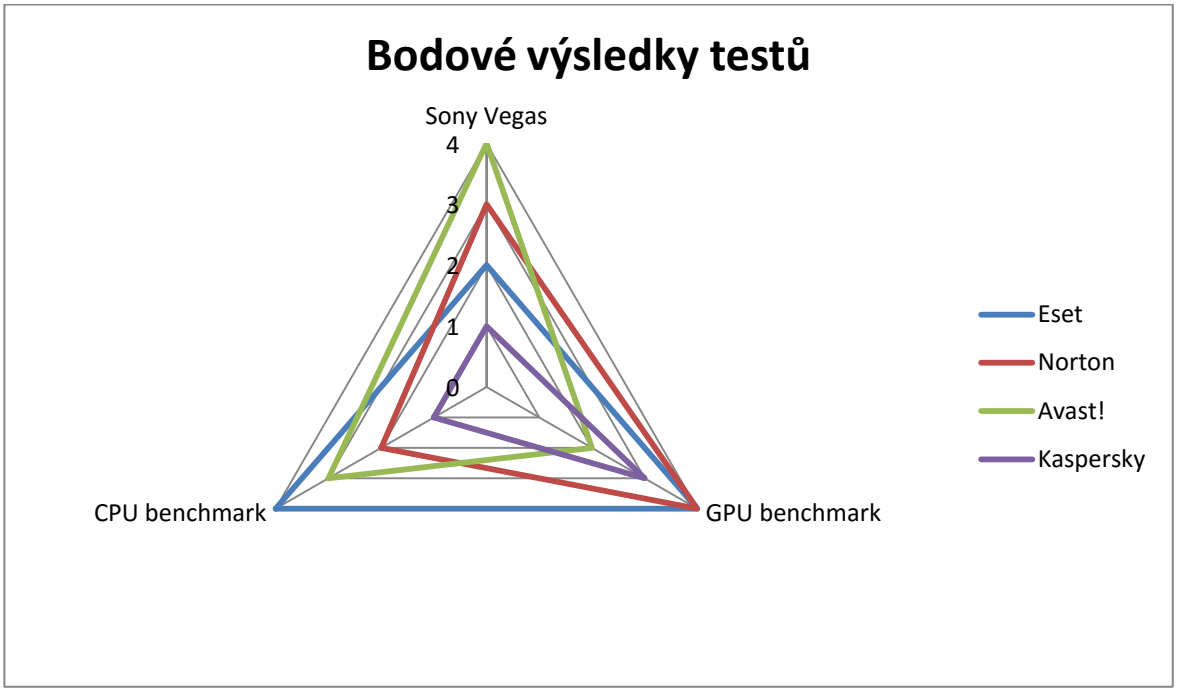
Body	Název antivirového programu
4	Eset
3	Avast!
2	Norton
1	Kaspersky

Zkombinováním Tabulek 12, 13 a 14 dosname Tabulku 15:

Tabulka 15: Bodové hodnocení pro měřené testy

	Sony Vegas	GPU benchmark	CPU benchmark	Celkem bodů
Eset	2	4	4	10
Norton	3	4	2	9
Avast!	4	2	3	9
Kaspersky	1	3	1	5

Graf 1: Bodové výsledky testů



Z Tabulky 15 a následného Grafu 1 je patrné, že v měření výkonnosti za hloubkového scanování na zvoleném počítači byl nejlepší Eset s deseti body, následován antivirem Norton a Avast!, kteří oba dosáhli devíti bodů. Poslední se umístil Kaspersky s pěti body.

Pátým kritériem bylo hodnocení efektivnosti antivirů v reálném prostředí. Data z Tabulek 2, 4, 6 a 8 jsou v následující Tabulce 16 a Grafu 2:

Tabulka 16: Výsledky hodnocení bodů za efektivnosti

	ochrana	výkon	použitelnost/vytížení	Body celkem
Eset	4,5	4	5,5	14
Norton	6	5	5,5	16,5
Avast!	6	5	6	17
Kaspersky	6	6	6	18

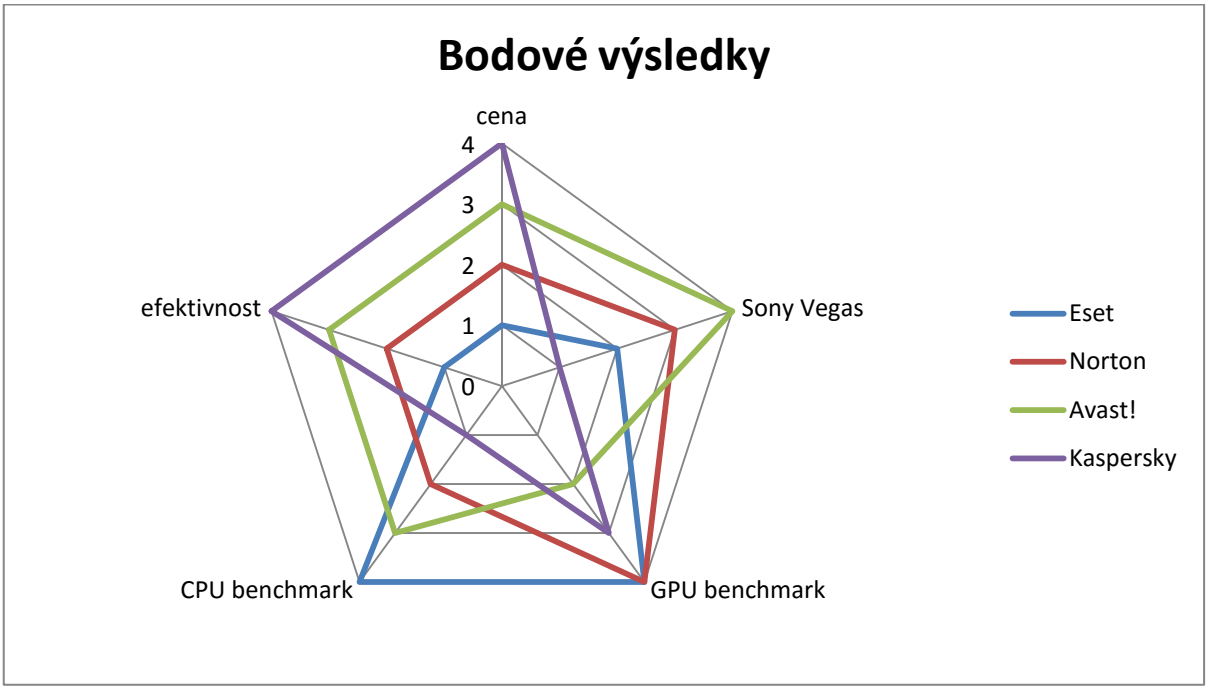
Graf 2: Výsledky bodů v efektivnosti

Z Tabulky 16 a Grafu 2 je patrné, že v pátém kritériu efektivnosti si nelépe vedl Kaspersky, následuje druhý Avast!, třetí je Norton a čtvrtý a poslední se umístil Eset. Pro potřeby této práce bylo převedeno pořadí na systém bodů, a to tak, že nejlépe umístěný antivirový program (Kaspersky), dostal čtyři body, druhému antivirovému programu (Avast!) byly uděleny tři body atp. Viz níže Tabulka 17., uvedená čísla jsou body za každý z pěti testovaných kritérií.

Tabulka 17: Výsledky kritérií

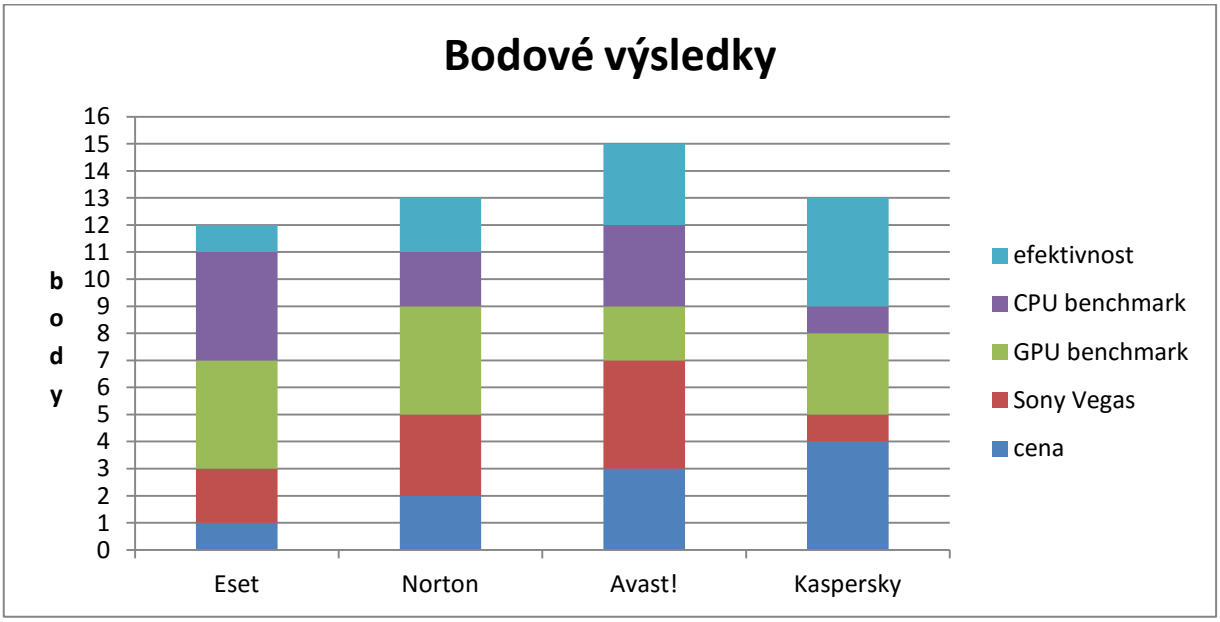
	Cena [body]	Sony Vegas [body]	GPU benchmark [body]	CPU benchmark [body]	Efektivnost [body]	Body Celkem [body]
Eset	1	2	4	4	1	12
Norton	2	3	4	2	2	13
Avast!	3	4	2	3	3	15
Kaspersky	4	1	3	1	4	13

Graf 3: Bodové výsledky



Výsledky se dají místo pavučinového grafu zobrazit také ve skládaném sloupcovém grafu – Graf 4:

Graf 4: Bodové výsledky



Na základně naměřených a převzatých hodnot vychází nejlépe Avast! s patnácti body, následovaným se stejným počtem třinácti bodu jsou Norton a Kaspersky a nejhůře dopadl Eset s dvanácti body.

5 Závěr

V dnešní době i ten základní antivirový program dělá více, než jen chrání náš počítač proti virům a malware, stará se také o mnoho moderních a komplexních hrozeb, na které běžně můžeme narazit při používání počítače. Přes antivirové a anti-malware detekce až po zesílení ochrany internetového bankovnictví jsou antivirové programy nepostradatelnou součástí základního vybavení každého počítače nezávisle na operačním systému. Antivirové programy procházejí neustálým vývojem a zdokonalováním jejich funkcí, přesto je nutno si uvědomit, že nejlepší ochranou před internetovými útoky je zdravý rozum.

Cílem práce bylo vybrat měřitelná kritéria a následně podle jejich výsledků najít nejvhodnější antivirový program pro zvolený počítač. Do výběru byly vybrány čtyři antivirové programy, co mají volně stažitelnou zkušební verzi a posléze taky koupitelnou plnou licenci na jeden rok.

Za testovací kritéria byla zvolena cena, doba konvertování videa v programu Sony Vegas Pro, doba konání GPU benchmark, doba konání CPU benchmark a efektivnost antivirových programů v reálném prostředí. Výsledky vybraných kritérií byly převedeny na body a zaneseny do paprskových grafů.

Za pomoci pavučinových grafů a tabulek bylo z výsledků měření zjištěno, že nejvhodnější antivirový program pro zvolený počítač je Avast! Internet Security. Jediné kritérium, ve kterém byl Avast! Internet Security ze všech hodnocených kritérií nejhorší, bylo kritérium „doba konání GPU benchmark“. Antivirový program Avast! Internet Security i přes tento nedostatek celkově zvítězil a může být doporučen jako nejvhodnější volba pro zvolený počítač.

6 Zdroje

[1] JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2

[2] KUCHAŘ, Martin, Mirek JAHODA a Petr BROŽA. *Bible hardwaru*. 1. vyd. Brno: Extra Publishing s.r.o., 2008. ISSN 1802-1220.

[3] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. 1. vyd. Brno: CP Books, 2005. ISBN 80-251-0574-1

[4] DAVIS, Harold. *Bezdrátové sítě Wi-Fi.* Praha: Grada, 2006. ISBN 80-247-1421-3

[5] HÁK, Igor, ZELENKA, Josef. *Ochrana dat: škodlivý software.* Hradec Králové: Gaudeamus, 2005. ISBN 80-7041-594-0

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

[7] SZOR, Peter. *Počítačové viry – analýza útoku a obrana.* Brno: Zoner Press, 2006. ISBN 80-86815-04-8

[8] JALŮVKA, Josef. *Moderní počítačové viry.* 2. aktualizované vydání. Praha: Computer Press, 2000. ISBN 80-7226-402-8

[9] *Eset Smart Security 9 Uživatelská příručka* [online]. [cit. 2016-03-13]. Dostupné z: http://download.eset.com/manuals/eset_ess_9_userguide_csy.pdf

[10] *Kaspersky User Guide* [online]. [cit. 2016-03-13]. Dostupné z: http://media.kaspersky.com/usa/documentation/kav2016_userguide_en.pdf?_ga=1.199363.502.1825894872.1449791528

[11] *Svět Hardware - Vše co jste chtěli vědět o SSD* [online]. [cit. 2016-03-13]. Dostupné z: http://www.svethardware.cz/vse-co-jste-chteli-vedet-o-ssd/26524

[12] *What is firewall* [online]. [cit. 2016-03-13]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/what-is-firewall#1TC=windows-7

[13] *All CPU Meter* [online]. [cit. 2016-03-13]. Dostupné z: http://addgadgets.com/all_cpu_meter/

[14] *GPU Meter* [online]. [cit. 2016-03-13]. Dostupné z: http://addgadgets.com/gpu_meter/

[15] *Drives Meter* [online]. [cit. 2016-03-13]. Dostupné z: http://addgadgets.com/drives_meter/

[16] *AV-Test: Avast!* [online]. [cit. 2016-03-13]. Dostupné z: https://www.av-test.org/en/pdfreport/10443

[17] *AV-Test: Eset* [online]. [cit. 2016-03-13]. Dostupné z: https://www.av-test.org/en/pdfreport/10467

[18] *AV-Test: Kaspersky* [online]. [cit. 2016-03-13]. Dostupné z: https://www.av-test.org/en/pdfreport/10483

[19] *AV-Test: Norton* [online]. [cit. 2016-03-13]. Dostupné z: https://www.av-test.org/en/pdfreport/10507

[20] *Eset: Cena za licenci* [online]. [cit. 2016-03-13]. Dostupné z: https://koupit.eset.com/default.aspx?pid=3

[21] *Norton: Cena za licenci* [online]. [cit. 2016-03-13]. Dostupné z: http://cz.norton.com/norton-security-for-one-device

[22] *Kaspersky: Cena za licenci* [online]. [cit. 2016-03-13]. Dostupné z: http://shop.kaspersky.cz/product/kaspersky-anti-virus-2016#tab=key-features

7 Seznam tabulek

8 Seznam grafů

9 Seznam obrázků