UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Zabezpečení Windows Server 2008 pomocí systému Kaspersky

Pavel Svoboda

Bakalářská práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Svoboda**
Osobní číslo:	**I10473**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Zabezpečení Windows Server 2008 pomocí systému Kaspersky**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Autor v bakalářské práci popíše možnosti a metody zabezpečení Windows Server 2008 pomocí systému Kaspersky. V práci budou popsány vlastnosti produktu, práce s tímto produktem a porovnání produktu s obdobnými produkty na trhu. Na praktických příkladech bude provedeno vyhodnocení bezpečnosti.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

ANDERSON, Christa a Kristin L GRIFFIN. Windows server 2008: terminel services : resource kit. Redmond: Microsoft Press, 2009, xxiii, 497 s. ISBN 978-0-7356-2585-3.
STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 8. 5. 2013 Pavel Svoboda

Poděkování

V první řadě bych chtěl poděkovat rodičům za veškerou podporu, kterou mi poskytli, za celou dobu studia. Můj průběh studia nebyl vůbec ideální a jednoduchý, ale i přes to mě neochvějně podporovali v dalším studiu. Velmi rád bych poděkoval také vedoucí práce ing. Soně Neradové za konzultace a pomoc při psaní této bakalářské práce. Zároveň bych chtěl poděkovat Mgr. Josefu Horálkovi za konzultace a novou perspektivu při psaní práce.

Abstrakt

Tato bakalářská práce se zabývá zabezpečením počítačů v malé podnikové síti. K zabezpečení je využit bezpečnostní systém od firmy Kaspersky pro malé firmy, který poskytuje kompletní zabezpečení jednotlivých počítačů a její vzdálenou správou. Hlavním cílem je popis systému a jeho nastavení pro správnou funkčnost. V další části práce je porovnání produktu s obdobnými produkty na trhu. V poslední části práce jsou provedeny pokusy o prolomení zabezpečení tohoto systému a shrnutí výsledků těchto útoků.

Klíčová slova

Zabezpečení, Kaspersky, LAN, antivir

Title

Securing Windows Server 2008 with Kaspersky system

Abstract

This bachelor's thesis addresses a problem of computer security in a small business. To secure the small business's computers, Kaspersky Small Office Security software is used. This software provides complete security of individual computers and remote control of the security system. Main target of this thesis is to describe this software and it's setup to reach the best functionality. The next part of this thesis is oriented on comparing of this software to similar products on market. In the last part of this thesis tests to break through the security are performed and results of these tests are assessed.

Keywords

Security, Kaspersky, LAN, antivirus

Obsah

Seznam zkratek

LAN	Local Area Network, lokalní síť
DDoS	Distributed Denial of Service, Distribuované odmítnutí služby
FTP	File Transfer Protocol
OS	Operational systém, Operační systém
URL	Uniform Resource Locator, Jednotný lokátor zdrojů
MBR	Master Boot Record
PID	Process Identification Number, identifikační číslo procesu

Seznam obrázků

1 Úvod

Spolu s příchodem prvních počítačů se začaly objevovat i první viry. Z počátku se jednalo o zcela neškodné programy, zaměřené zejména na neškodné vtipy na kolegy v práci či přátele. Šíření těchto programů nebylo v té době nijak snadné. Většinou bylo potřeba nahrát daný soubor na disketu, tu pak potají přenést do cílového počítače, daný program spustit a pak už se jenom bavit na účet oběti.

Stejně jako se vyvíjely technologie, vyvíjely se i tyto dříve neškodné programy. Postupem času se z těchto většinou úplně neškodných programů vyvinuly programy schopné ukrást veškerá data v počítači, vymazat všechna data nebo úplně znemožnit používání počítače. S příchodem prvních skutečných sítí se tyto programy stávaly stále větší a větší hrozbou, protože jejich distribuce přestávala být problém. Začaly se vytvářet skupiny expertů na počítačovou bezpečnost, které začaly tyto viry zkoumat, a snažily se přijít na techniky, jak se těchto programů zbavit či jak jejich fungování předcházet. Tyto skupiny počítačových expertů začaly vytvářet nástroje na odstraňování škodlivého softwaru. Postupem čase začali tito experti přicházet na to, že není možné vytvářet obranu proti jednotlivým virů a místo toho začali vytvářet nástroje, které by byly schopné zbavit se jakéhokoliv škodlivého programu. To bylo počátkem prvních antivirů a s nimi i společností zaměřených na jejich tvorbu.

Cílem této bakalářské práce je nastavit a otestovat antivir od společnosti Kaspersky Lab vytvořený za účelech ochrany počítačů malé firmy o velikosti 5-10 počítačů. Na začátku práce popíši škodlivý software, se kterým se v dnešní době můžeme setkat. V další části zmíním možné ochrany proti těmto hrozbám. Poté zmíním fakta o firmě Kaspersky Lab a o produktech, které nabízejí. V následující kapitole popíšu nastavení, které jsem v programu provedl pro správnou funkčnost. Na závěr provedu několik pokusů o prolomení tohoto softwaru.

2 Bezpečnostní hrozby

2.1 Viry

Virus je počítačový program, který replikuje sám sebe. Cílem viru může být poškození systému, na kterém se vir nachází, nebo nějaké jiné ovlivnění systému. Hlavním poznávacím znakem viru je, že ke svému šíření využívá spustitelné soubory, při jejichž spuštění se virus zkopíruje. Viry se mezi uživateli mohou šířit mnoha způsoby zejména přes síť (např. otevřením infikované emailové přílohy). Viry mohou být polymorfní (mění svojí strukturu při každém zkopírování) a nepolymorfní (nemění svoji strukturu).

2.1.1 Stealth vir

Sleduje systémové funkce pro čtení souborů nebo sektorů z paměťového média. Pokud se požadavek na čtení týká infikovaného souboru, vrací vir aplikaci data původního neinfikovaného souboru, čímž se snaží zamaskovat svou přítomnost. Antivirus odhalí tento typ viru tím, že zkontroluje, jestli byla adresa přerušení přepsána, anebo používá na čtení služby diskového řadiče.

2.1.2 Boot vir

Dnes se jedná o historický a raritní druh viru. Nachází se v MBR nebo boot sektoru pevného disku. Vir přepíše boot sektor vlastním záznamem a původní archivuje na jiné části disku. Tento typ viru se šířil zejména ve dřívější době pomocí disket v systému DOS. Se zánikem systému DOS skončil i tento typ viru.

2.1.3 Souborové viry

Tento typ viru je vždy spojen se spustitelným souborem. Cílem je, aby při spuštění souboru došlo k aktivaci viru, čímž se vir rozmnoží. Většina těchto virů má velmi podobnou činnost. Skoro vždy přepíší začátek souboru, kde umístí příkaz na skok k samotnému viru, nebo se rovnou sami umístí na začátek souboru. Nevýhoda takovéhoto viru je, že svým zásahem do souboru poškodí hostitelský program. Při spuštění programu tedy dojde k aktivaci viru samotného, ale program jako takový už nefunguje. Díky tomu dojde k upozornění uživatele na nesprávnou funkčnost a k odhalení viru.

2.1.4 Retroviry

Retroviry se snaží zabránit svému odhalení napadením antivirového softwaru. Občas jsou nazývány „anti-antiviry“. Retroviry bývají vytvořeny přímo na míru nějakému specifickému antiviru, jehož slabé místo tvůrce viru odhalil (např. smazání souborů, ve kterém si antivir schovává signatury jednotlivých virů).

2.1.5 Polymorfní viry

Polymorfní viry zašifrují své tělo pomocí speciální rutiny a tím se snaží skrýt svou prezenci před antivirem. Pokud se polymorfní antivirus chce rozšířit, musí nejdříve dešifrovat celý soubor podle šifrovací rutiny, čímž se dostane do původního stavu. Dešifrovací rutina se zmocní na dobu dešifrování řízení počítače a po proběhnutí předá řízení viru.

Najít polymorfní virus může být velmi složité, jelikož při každém napadení souboru vygeneruje virus úplně novou dešifrovací rutinu. Její signatura se po každém zavolání mění a není nikdy stejná. Ke změně dešifrovací rutiny se využívá tzv. mutátoru, který s použitím generátoru náhodných čísel a jednoduchých matematických operací přetvoří virus. K nalezení těchto virů, používají antiviry mechanizmy na vyhledávání šifrování.

2.1.6 Multipartitní viry

Napadají spustitelné soubory a boot sektory disku. Multipartitní viry se neomezují na specifickou část disku či na specifické soubory. Místo toho infikují systém několika způsoby najednou. Při spuštění infikovaného souboru dojde k napadení boot sektoru stroje. Při dalším spuštění stroje se virus zaktivuje a infikuje každý vhodný spuštěný program.

2.1.7 Fágy

Fágy nahradí obsah infikovaného souboru svým vlastním kódem. Tento typ viru se nesnaží o nenápadné připojení k souboru či ke skrytí v kódu souboru. Místo toho kompletně přepíše obsah souboru svým vlastním kódem. Virus pak takto vzniklému souboru nastaví stejné vlastnosti, jako měl původní soubor (datum, čas vzniku, atributy, velikost) a tím se snaží zamaskovat.

Veškeré informace o virech jsem čerpal z [1], [2].

2.2 Červy

Zatím co počítačové viry se rozmnožují v systému a přenáší se kontaktem, červy se mohou šířit sami a to dokonce i bez infekčního mechanismu. Červy se dokáží šířit pomocí připojení (místní síť, Internet) nebo i jako přílohy elektronických zpráv (červoviry). Další typy červovirů se šíří za pomoci zjištění slabého místa v softwaru a nevyžadují žádnou interakci od uživatele. Tyto programy prohledávají síť a snaží se zneužít počítače, které obsahují slabá místa v softwaru. Není tedy zapotřebí žádného emailu či jeho přílohy.

Červy vytvoří velké množství svých kopií v paměti počítače a tím vytlačí ostatní programy. Paměť počítače je spotřebovávána až do doby, kdy zahltí celý operační systém a ten se pod náporem zhroutí. Takto infikovaný systém zároveň infikuje ostatní uživatele v síti.

2.3 Trojský kůň

Trojský kůň je speciální typ škodlivého softwaru, který umožňuje útočníkovi monitorovat či ovládat činnost systému na vzdáleném systému. Trojští koně se skrývají většinou uvnitř užitečných programů (počítačové hry, stažené soubory), ale na rozdíl od virů a červů se nesnaží sami sebe replikovat a šířit se dále. Místo toho umožňují útočníkům ovládat a monitorovat napadené systémy za účelem získání citlivých informací (např. heslo do internetového bankovnictví).

2.3.1 Keylogger

Speciální typ trojského koně, který zaznamenává veškeré stisknuté klávesy od spuštění systému a výsledek ukládá do souboru nebo rovnou zasílá útočníkovi.

2.3.2 DDoS

Trojský kůň se dá využít i k provedení takzvaného DDoS útoku. Tento typ trojského koně v napadeném systému aktivuje FTP službu na portu 21 a dovolí útočníkovi přenášet soubory. Při útoku pak několik (desítek, stovek a víc) napadených počítačů na povel útočníka zaútočí naráz na cílový server, který tento nával požadavků nezvládne a přestane poskytovat služby.

2.4 Rootkit

Rootkity jsou ve skupině počítačových hrozeb poměrně mladou záležitostí. Hlavním cílem rootkitu je zakrýt neautorizovanou činnost útočníka či škodlivého softwaru v systému. K dosažení tohoto cíle využívá dvou přístupů – modifikaci systémových struktur nebo modifikaci cest. Modifikace cest funguje na bázi přesměrování API funkcí operačního softwaru (rootkit je umístěn mezi uživatelskou aplikaci a DLL knihovnu, kterou tato aplikace využívá). Modifikace systémových struktur funguje na bázi maskování změn v registrech či systémových procesech OS.

„Rootkit nepředstavuje přímé nebezpečí, je to pouze nástroj, který může být zneužit. Škodlivé kódy se dokáží pomocí rootkitu velmi dobře skrýt: rootkit maskuje jejich přítomnost skrýváním adresářů, v nichž jsou instalovány, API volání, položek registru Windows, procesů a systémových služeb tak, aby přítomnost škodlivého softwaru nebyla běžnými systémovými nástroji (např. Windows Task Manager) a bezpečnostními aplikacemi odhalitelná.

Pokud chce někdo rootkit zneužívat, musí instalovat do počítače nejprve ten a následně i nějakou aplikaci (virus, trojského koně, zadní vrátka, bot apod.). Instalace rootkitu je jen prvním, ale nesmírně důležitým krokem ke kompromitaci počítače.“ [3]

2.5 Spyware [4]

Jak už název napovídá, jedná se o software, který sleduje činnost uživatele na infikovaném stroji. Mnohdy se instaluje bez vědomí uživatele, např. při instalaci shareware softwaru či při instalování bezplatného softwaru jako „doplňková“ služba. Úkolem spyware může být sledování webových stránek, které si uživatel prohlíží, jaké klávesy (a tím pádem i jaká hesla) uživatel zadává na klávesnici při prohlížení určitých webových stránek. Sledovat může ale i informace o tom, jaký software má uživatel nainstalovaný na svém systému či jaké dokumenty se vyskytují na pevném disku. Tyto informace pak spyware zasílá pomocí internetu útočníkovi, který data může využít pro cílenou reklamu či pro uskutečnění nějaké nekalé činnosti. Spyware jako takový nepoškozuje počítač přímo, ale škodí samotnému uživateli, jelikož parazituje na jeho soukromí.

Zbavit se spywaru, bez softwaru přímo k tomu určenému, je obtížné. Většina spywaru bývá rezistentní proti odinstalování a snaží se zanechat důkladně ukryté položky v registrech,

které je obtížné dohledat a zbavit se jich. Jiný způsob, kterým se dá zbavit spywaru, je filtrovat komunikaci na portu 80. Většina typů spywaru se přes tento port instaluje bez vědomí firewallu.

2.6 Adware [4]

Adware, neboli propagační software, není přímo škodlivý či nebezpečný software. Dostává se do systému za uživatelova vědomí a podobnými způsoby jako spyware. Adware způsobuje vyskakování oken s reklamou. Tyto reklamy mají uživatele vybídnout ke koupi zboží nebo ho po kliknutí na ně přesměrují na internetové stránky, kde se dané zboží dá koupit. Při kliknutí na reklamu ale většinou dochází k instalování dalšího adwaru nebo spywaru. Jedná se tedy spíše o software, který nám znepříjemňuje naší práci na počítači, než aby byl škodlivý.

2.7 Phishing

Phishing je podvodný způsob, jak z uživatele dostat přístupová hesla a citlivé informace. Nejčastěji se s phishingem setkáváme formou podvodných emailů. V takovýchto emailech po nás důvěryhodný zdroj (banka, internetový obchod, administrátor webové hry) požaduje důvěryhodné informace ve formě přístupového hesla či čísla kreditní karty. Většinou není možné tyto podvodné emaily na první pohled odhalit jako podvod. Vzhledově jsou totožné s emaily, které vám od důvěryhodného zdroje přicházejí, a emailová adresa odesílatele vypadá důvěryhodně. V emailu se často vyskytuje i odkaz na webovou stránku s formulářem, který po nás žádá ona přístupová data. Tato stránka se dá velmi lehce rozpoznat, jelikož její URL adresa je odlišná od adresy důvěryhodného zdroje.

Obranou proti phishingu je zejména obeznámení veřejnosti s nebezpečím, které poskytování důvěrných informací představuje. [4]

2.8 Spam

Za spam je obecně považována jakákoliv nevyžádaná pošta. Z pohledu českého právního řádu je ale spam definován jako nevyžádané obchodní sdělení. Historie spamu a definice obchodního hlediska je z právního hlediska velmi zajímavá a názorně ukazuje, jak se právní systém snaží potýkat s problémy, které moderní technologie přinášejí. Spam je v dnešní době ve své podstatě nelegální a je právně postihnutelný. Pokuta pro fyzickou osobu činí až 100.000,- Kč a pro právnickou osobu až 10 mil. Kč.

K 1. 8. 2006 bylo možné obchodní sdělení zasílat pouze za využití tzv. principu opt-in, což znamenalo, že je možné zasílat obchodní sdělení pouze, pokud k tomu uživatel dal souhlas. Od 1. 8. je ovšem možné využívat měkčího principu opt-out. To znamená, že odesílatel nám může zasílat obchodní sdělení do té doby, dokud výslovně neřekneme, že o něj nemáme nadále zájem (většinou ve formě odkazu na konci emailu, který slouží k odebrání z databáze odběratelů obchodních sdělení).

K 1. 1. 2012 bylo samotné obchodní sdělení z právního hlediska definováno takto: „všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle“. [10] Tato forma definice povolovala zasílání obchodních sdělení, ve kterých byl pouze odkaz na adresu internetových stránek prodejce, bez jakéhokoliv možného právního postihu.

Od 1. 1. 2012 ovšem platí nový zákon č. 468/2011 Sb, ve kterém je definice obchodního sdělení upravena takto: „všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem 3 nebo vykonává regulovanou činnost“. Tato právní úprava je mnohem přísnější a postihuje i předtím nepostihnutelnou elektronickou poštu, ve které se nacházel pouze odkaz na stránky prodejce. [5]

2.9 Banner

Jedná se o grafickou formu internetové reklamy, mnohdy ve formě reklamního proužku. Nejčastěji bývají bannery statické obrázky, které informují o zajímavé nabídce prodejce. Dnes se stále častěji objevují spíše v animované formě (často za pomoci technologie flash).

3 Možnosti ochrany počítače

V dnešní době, kdy nám, při přístupu na Internet, hrozí útoky ze všech stran, je potřeba si svůj systém dostatečně zabezpečit proti všem možným útokům. Největším rizikem pro počítač, či jiné zařízení schopné připojit se k Internetu, je jeho uživatel. Proto je dobré, aby každý uživatel měl alespoň minimální znalosti o bezpečném užívání Internetu. Žádný bezpečnostní software, který si do našeho systému nainstalujeme, není absolutně perfektní a neproniknutelný. Vždy se najde někdo, kdo je schopný naše zabezpečení překonat (firmy jako Google či Microsoft pořádají každoročně soutěže zaměřené právě na prolamování ochrany v jejich produktech).

Není v lidských silách, aby člověk sám ochránil svůj počítač. Proto je potřeba aby si na svůj počítač nainstaloval software, který mu s problémem zabezpečení pomůže. Tyto programy se podle svého účelu dají rozdělit do několika skupin podle jejich primární funkce. Mezi základní bezpečností software patří: firewall, antivir a antispyware.

3.1 Firewall [6]

Základní ochranou, kterou by měl mít každý počítač, který se připojuje do jakékoliv sítě, je firewall. Firewall je obecně systém, který zamezuje neautorizovaný přístup do privátní sítě. Firewall může být síťový prvek, nacházející se na rozhraní dvou sítí, přes který prochází veškerá síťová komunikace, nebo jím může být software, nainstalovaný na zařízení (popř. se jedná o kombinaci obou variant). Firewall zkoumá veškerou komunikaci, která přichází či odchází ze sítě, a zkoumá, zda splňuje specifická bezpečnostní kritéria. Nejjednodušší firewally zkoumají komunikaci pouze na základě zdrojové a cílové IP adresy a čísla portu.

Základní typy firewallů:

- *Paketový firewall*: Firewall se podívá na každý příchozí či odchozí paket, zkontroluje jeho hlavičku (IP adresy a porty) a podle uživatelem definovaných pravidel rozhodne, zda daný paket pustí dál, či jej zahodí. Tato metoda filtrování je poměrně účinná, zvláště pokud jsou pravidla pro filtrování správně nastavená. Naopak je tato metoda absolutně neúčinná, pokud útočník zaútočí metodou IP spoofing (při tomto typu útoku podvrhuje útočník adresu svých paketů za důvěryhodnou adresu). Toto filtrování funguje na 3. vrstvě ISO/OSI modelu.

- *Aplikační brána*: Specifickým aplikacím (např. FTP, e-mail, atd.) je nastaven bezpečnostní mechanismus ve formě proxy serveru (brány). V tomto případě jsou od sebe obě sítě kompletně oddělené a komunikace probíhá přes proxy server. Komunikace jde od klienta nejdříve na proxy server a teprve až poté ke zdroji. Naopak zdroj zasílá komunikaci na proxy server, který po kontrole zašle zprávu klientovi. V tomto případě nemá zdroj tušení, že nekomunikuje přímo s klientem, ale s proxy serverem. Ke kontrole dochází na 7. vrstvě ISO/OSI modelu a díky tomu

poskytuje kvalitní zabezpečení. Nevýhodou tohoto principu je velká výpočetní náročnost a může proto dojít ke zpomalení komunikace.

- *Stavový firewall:* Při zahájení relace si uloží informace o této relaci do tabulky aktuálně navázaných spojení. Adresy příchozích paketů jsou poté porovnávány s touto tabulkou a na základě shody jsou vpuštěny či zahozeny. Informace nacházející se v tabulce spojení by měly být jednoznačné a podrobné, aby nemohlo dojít k podvržení informací útočníkem. Veškerá komunikace je sledována pro příznaky ukončení spojení. Pokud takový paket dorazí, spojení je vymazáno z tabulky a pakety už nadále nejsou propouštěny k cíli. Firewall funguje na 4. vrstvě, popř. i nižší vrstvě, ISO/OSI modelu. Celkově je bezpečnější než paketový filtr a není tak výpočetně náročný jako proxy server.

- *Hardwarově akcelerovaný firewall:* Většinou se jedná o externí zařízení (např. PCI karta), které obsahuje programovatelný hardware. K samotnému filtrování komunikace dochází na kartě a nedochází tak k zatížení procesoru hostitelského stroje.

3.2 Antivir [7]

Se škodlivým softwarem se setkáváme dnes a denně, a proto je nutné se proti těmto hrozbám chránit co nejlepším způsobem. Abychom náš systém proti těmto hrozbám ochránili, je potřeba nainstalovat speciální software, který je pro tento účel navržen, tzv. antivirus. Antivirus je program, který chrání náš systém a aktivně vyhledává a maže škodlivý software. Sehnat vhodný antivirus pro náš systém není složité. Na Internetu se vyskytuje jak v placené tak i v neplacené verzi. Operační systémy Windows dokonce už mají určitou formu antiviru v sobě zabudovanou. Aby byl antivirus účinný, proti neustále se měnícím a nově vznikajícím hrozbám, je potřeba, aby po dobu spuštění systému, běžel antivirus neustále na pozadí. Dalším nutným požadavkem na správnou funkčnost antiviru je mít aktualizovanou databázi škodlivého softwaru, kterou si antivirus uchovává.

Principy, kterými antivirus vyhledává škodlivý software:

- *Slovníkový přístup:* Antivirus prohledává jednotlivé soubory a porovnává jejich obsah se svou databází známých virů. Při nalezení kódu v programu, který se shoduje se známým virem ve virové databázi, může antivir tento soubor smazat, umístit do karantény anebo pokusit se o opravení souboru, vymazáním části škodlivého kódu ze souboru. K efektivnímu využití tohoto přístupu je nutné, mít neustále aktualizovanou virovou databázi.

- *Monitorování podezřelého chování:* Antivirus se nesnaží o identifikaci známých virů a místo toho monitoruje chování spuštěných programů. Pokud se program pokusí zapsat část kódu do spustitelného souboru, je toto chování zaznamenáno jako podezřelé. Uživatel je informován o podezřelém chování programu a požádán o zvolení dalšího postupu při práci s programem. Tato metoda detekce je schopna

nalézt i doposud neidentifikovaný škodlivý software. Problémem této metody je, že v dnešní době zasahuje i spousta triviálních programů do spustitelných souborů. Výsledkem je velkém množství falešných pozitiv a s neustálým vyptáváním uživatele na další postu, ztrácí uživatel zájem o tento druh kontroly. Místo zkontrolování nové potenciální hrozby tak uživatel automaticky potvrdí, že se nejedná o škodlivý software. Moderní antiviry proto od této techniky stále více a více odstupují a dále ji nevyužívají.

- *Emulování spustitelných souborů:* Některé antiviry se emulují počátek běhu spustitelného souboru ještě před tím, než je samotný program spuštěn. Pokud se kód programu sám od sebe mění, anebo se jinak chová jako virus, pak dochází antivirus k názoru, že se jedná o škodlivý software. Tento typ detekce vyvolává velké množství falešně pozitivních zpráv.

- *Sandbox:* Dochází k emulaci operačního systému, ve kterém se spustí program. Po doběhnutí programu, je emulovaný systém zanalyzován na změny, které by mohly značit přítomnost viru. Tato metoda je výpočetně velmi náročná a proto se používá pouze na přímé vyžádání uživatele.

3.3 AntiSpyware

Podobně, jako se antiviry zaměřují na odstranění virů (resp. dříve se zaměřovaly na viry, dnes většinou poskytují téměř kompletní ochranu), se antispywarový software zaměřuje na odstranění spywaru a adwaru. Spyware a adware byly popsány dříve v kapitole 2.5 a 2.6. Rozdílem mezi antivirem a antispywarem je pouze typ škodlivého softwaru, po kterém tyto programy pátrají. Dnes dochází ke spojování těchto ochran dohromady a je zcela běžné, že námi nainstalovaný antivir obsahuje i antispyware a naopak.

Antispyware, podobně jako antivir, běží na pozadí a vyhledává běžící programy, které se shodují s jeho databází a jsou vyhodnoceny jako hrozby anebo vyhledává na disku soubory, které obsahují kusy škodlivého kódu.

3.4 Antispam [8]

Antispam je softwarový nástroj, který filtruje veškerou příchozí elektronickou poštu. Díky tomuto nástroji se nemusíme probírat několika desítkami nevyžádané pošty denně. Nejde tedy proto tak o nástroj, který je určený k ochraně systému, jako spíše o nástroj, který nám ulehčuje naši práci.

Nejčastější technikou rozlišení vyžádané a nevyžádané pošty je použíti spam filtrů. Tyto filtry fungují zejména a na bázi dvou technik: seznam slov a černá/bílá listina. Seznam slov obsahuje slova, která jsou běžně spojována se spamem (např. půjčka, viagra). Pokud se tyto slova objeví v příchozím emailu, je takový email přesměrován do adresáře se spamem. Černá listina funguje na bázi ukládání IP adres známých odesílatelů spamu. Veškerá komunikace z těchto IP adres je tedy rovnou přesměrována do adresáře se spamem. Naopak bílá listina

obsahuje uživatelem nastavené IP adresy, ze kterých si přeje přijímat elektronickou poštu. Takováto elektronická pošta již není kontrolována na přítomnost spamu.

Další typ filtru, který se často používá, je obsahový filtr. Zástupcem těchto filtrů je například Bayesův filtr. Tento filtr funguje na bázi prozkoumání obsahu každé příchozí a odchozí komunikace z emailové adresy a postupným učením se slovních frází a vzorů spojených s vyžádanou a nevyžádanou poštou. Podle takto naučených vzorů poté třídí spam v příchozích zprávách.

Tyto techniky se většinou používají najednou, aby bylo dosaženo co možná nejlepšího výsledku. Bohužel žádná z těchto technik není úplně dokonalá a může za spam označit i zprávu, která spamem není. Takovéto zprávy bývají velmi často přehlédnuty ve spamovém adresáři a k uživateli se nikdy nedostanou.

3.5 Antibanner

Antibanner je většinou zásuvný model ve webovém prohlížeči, který brání vyskakování oken s reklamou. Jejich funkčnost bývá dost nejistá. Existují skripty, kterými se dá tento zásuvný model obejít.

3.6 Heuristická analýza

Heuristická analýza je technologie pro vyhledávání virů, které se nenacházejí v databázi antiviru. Umožňuje detekci objektů, u kterých existuje možnost infikování neznámým či pozměněným virem. Heuristická analýza je schopná odhalit až 92% nových hrozeb. Na druhou stranu, heuristické metody pouze odhadují nebezpečné soubory a mají tak velké množství falešně pozitivních nálezů.

Analýza objektu začne prohledáváním kódu za účelem nalezení podezřelých vlastností (příkaz) typických pro škodlivý software. Při nálezu takovéhoto podezřelého příkazu si analyzátor zvedne číslo všech těchto nálezů v souboru. Pokud, na konci analyzování objektu, překročí toto číslo předem definovanou hranici, je takovýto objekt označen jako podezřelý.

Heuristická analýza může probíhat i dynamicky. V tomto případě zkopíruje analyzátor část kódu aplikace do virtuálního prostředí, ještě před spuštěním aplikace, a pozoruje její chování a snaží se odhalit podezřelé chování, jako je snaha o replikaci či snaha o utajení části kódu.

3.7 Komplexní ochrana

Mnoho programů se v dnešní době už nedá klasifikovat jako antivir, firewall či antispyware. Jde většinou o software, který nabízí všechny zmíněné funkce. Není se čemu divit, že se tvůrci těchto softwarů rozhodli jít touto cestou. Kdo by dne s chtěl na svém počítači mít 3 a více programů, když mohou mít nainstalován pouze jeden, který má stejnou funkčnost. Dá se tedy říct, že pokud si dnes nainstaluje uživatel na svůj počítač antivir, nejedná se čistě o antivir, ale zpravidla i o firewall, antispyware či antispammer.

4 Kaspersky [8]

4.1 Kaspersky Lab

Eugene Kaspersky, zakladatel firmy Kaspersky Lab, se začal zabývat studiem počítačových virů na konci 80. let 20. století. V roce 1987 absolvoval z Moskevského Institutu Šifrování, Telekomunikací a Informatiky. Roku 1991 začal Eugene Kaspersky vytvářet antivirové programy pro Ukrajinskou firmu dovážející počítače a krátce poté začal za 100 dolarů měsíčně pracovat pro Kami, jednu z prvních hardwarových a softwarových firem v Rusku. Roku 1994 Oddělení informatiky na Univerzitě v Hamburgu vyhlásilo nástroje Kaspersky nejlepším antivirovým skenerem na světě. Poptávka po tomto softwaru začala růst a v roce 1997 se Eugene Kaspersky rozhodl z firmy Kami odejít.

Roku 1997 založil Eugene Kaspersky spolu se svou ženou Natalií firmu Kaspersky Lab. Dnes je tato firma 4. největší antivirovou firmou na světě. Většími firmami zabývajícími se antiviry jsou pouze americké firmy Norton a McAfee a japonská firma Trend Micro.

Kaspersky Lab má sídlo v Moskvě v Rusku. Společnost má oblastní pracoviště ve 30 zemích po celém světě a dnes je jednou z nejrychleji rostoucích firem v oboru IT.

4.2 Nabízené produkty

Firma má v portfoliu rozsáhlý sortiment softwaru pro ochranu osobních počítačů a firem. Počítače ale nejsou jediným cílem nabízené ochrany a proto nabízí firma i ochranu pro mobilní telefony využívající OS Android a BlackBerry, tablety využívající OS Android a počítače od firmy Apple. Veškerý software je zakoupen s licencí platnou na jeden rok.

4.2.1 Software pro koncové uživatele

Kaspersky Internet Security 2013 – vlajková loď firmy pro zabezpečení osobního počítače. Software chrání před viry a jiným škodlivým softwarem, dokáže rozpoznat nové hrozby, které dosud nemá v databázi, monitoruje vaši aktivitu na internetu a kontroluje, jestli stránky na kterých se pohybujete, jsou bezpečné. Další vrstvou ochrany je zabezpečení při online bankovních transakcích, ve formě kontroly důvěryhodnosti webových stránek a zamezení odchytávání zadávaných kláves na těchto stránkách. V neposlední řadě filtruje spam, který se nachází mezi emaily, a zamezuje vyskakování reklam při pohybu na internetu.

Kaspersky Pure 3.0 – nabízí nejrozsáhlejší ochranu počítače. Obsahuje všechny formy ochrany, které nabízí Kaspersky Internet Security 2013, a zároveň rozšiřuje ochranu o možnost zabezpečení a zašifrování cenných dat, zálohování dat do celkové velikosti 2GB na Internetu. Dalšími výhodami je možnost kompletního přemazání obsahu z disku a nástroje na vyčištění nepotřebných souborů. Kaspersky Pure 3.0 dokáže vzdáleně spravovat zabezpečení na jiných zařízeních, využívajících ochranu od společnosti Kaspersky Lab.

Kaspersky Anti-Virus 2013 – obsahuje pouze základní verzi ochrany osobního počítače. Dokáže ochránit počítač proti virům a jinému škodlivému softwaru. Zároveň při pohybu na internetu kontroluje, jestli jsou stránky bezpečné.

Kaspersky Security for Mac – nabízí stejnou ochranu jako Kaspersky Anti-Virus s tím rozdílem, že je určen pro počítače od firmy Apple.

Kaspersky Tablet Security – software na ochranu tabletů s operačním systémem Android. Ochraňuje tablet před veškerým škodlivým softwarem a nebezpečím na Internetu. Obsahuje zároveň ochranu proti odcizení a to ve formě vzdáleného zamknutí tabletu, vymazání jeho obsahu, vytvoření fotografie držitele tabletu a určení pozice, na které se zařízení nachází pomocí souřadnic GPS, sítě GSM či pomocí připojení k internetu a služby Google Maps.

Kaspersky Mobile Security – tento program je vytvořen pro mobily využívající operační systém Android či BlackBerry. V případě odcizení je možné vzdáleně mobilní telefon zamknout, vymazat jeho obsah a nalézt jeho polohu. Navíc pokud dojde k výměně SIM karty, software mobil ihned zamkne a zašle uživateli email s novým číslem. Další funkcí je ochrana soukromí. Uživatel mobilního telefonu si může nastavit kontakt jako soukromý. Díky tomu, pokud nebude telefon v režimu soukromí, nebudou po tomto kontaktu v mobilním telefonu žádné stopy.

Kaspersky ONE – tento software je možno instalovat na osobní počítač, počítače Mac a tablety či mobily používající OS Android. Nabízí standartní ochranu proti škodlivému softwaru, při pohybu na Internetu a proti odcizení (v případě mobilního telefonu a tabletu).

4.2.2 Software pro malou kancelář

Pro malou firmu o rozloze 5-10 počítačů spolu s jedním souborovým serverem je možné zakoupit produkt Kaspersky Small Office Security (viz. níže).

4.2.3 Software pro podnik

Ochrana pro podnik se dá rozdělit podle typu zařízení, které má software zabezpečit. Jedná-li se o koncové zařízení, pak má firma možnost vybrat si produkt z řady Kaspersky Endpoint Security for Business. Na výběr jsou tři úrovně, které se liší množstvím nabízených služeb, a to Core, Select a Advanced (vzestupně podle počtu služeb).

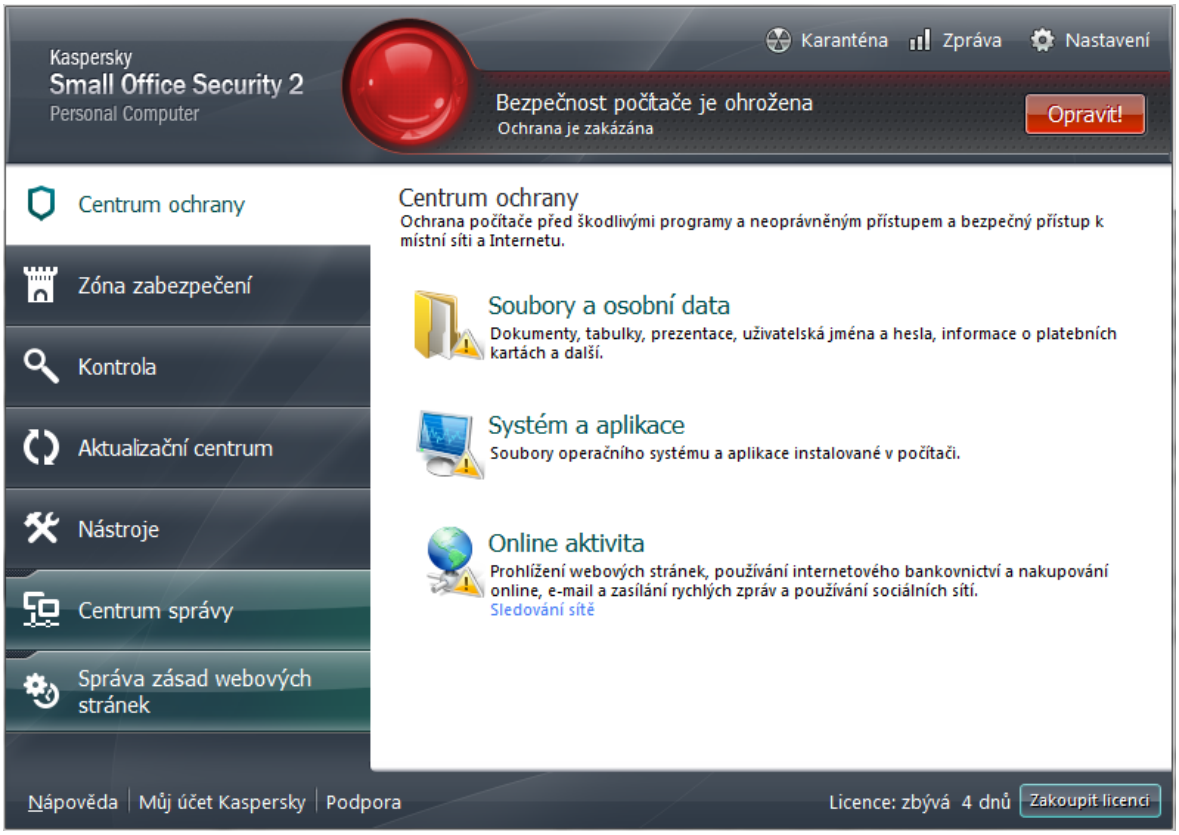
Dalšími produkty pro firmy je software zaměřený na specifický server či zařízení. S těmito produkty se dá zabezpečit SharePoint server (Kaspersky Security for Collaboration), souborový server (Kaspersky Security for File Server), poštovní server (Kaspersky Security for Mail Server). Přístup k Internetu přes brány je možné zabezpečit se softwarem Kaspersky Security for Internet Gateway, který podporuje nejčastější brány, běžící na platformách Windows a Linux. Mobilní zařízení se dají ochránit za pomocí softwaru Kaspersky Security for Mobile, který poskytuje ochranu smartphonů a tabletů se širokým spektrem platforem: iOS, Android, BlackBerry, Windows Mobile, Windows Phone, Symbian.

Kaspersky Systems Management je dalším produktem určeným pro větší firmy. S jeho pomocí je možné spravovat a monitorovat činnost všech bezpečnostních systémů, na všech zařízeních ve firemní síti, z jednoho místa.

Kaspersky Total Security for Business nabízí kompletní ochranu firmy ve formě všech předchozích produktů v jednom.

5 Kaspersky Small Office Security

Produkt Kaspersky Small Office Security je hlavní náplní praktické části bakalářské práce. Jedná se o systém, který je speciálně určený pro malé firmy, o rozloze maximálně 10 počítačů a jednoho souborového serveru. Systém poskytuje prakticky kompletní ochranu systému, složenou z ochrany souborů a osobních dat, zabezpečení systému a online zabezpečení. Každá z těchto částí ochrany se skládá z individuálních služeb, které jsou navzájem provázané. Každá služba se stará o jinou část systému a je možné ji vypnout, pokud je to žádoucí.



Obrázek 1 - Základní okno systému

5.1 Centrum ochrany

Základní funkcí systému je ochrana počítače před škodlivým softwarem, neoprávněným přístupem a bezpečným pohybem na Internetu. O tuto funkci se stará část Centrum ochrany, které se stará o ochranu na třech frontách: ochrana souborů a osobních dat, zabezpečení systému a bezpečný pohyb na internetu.

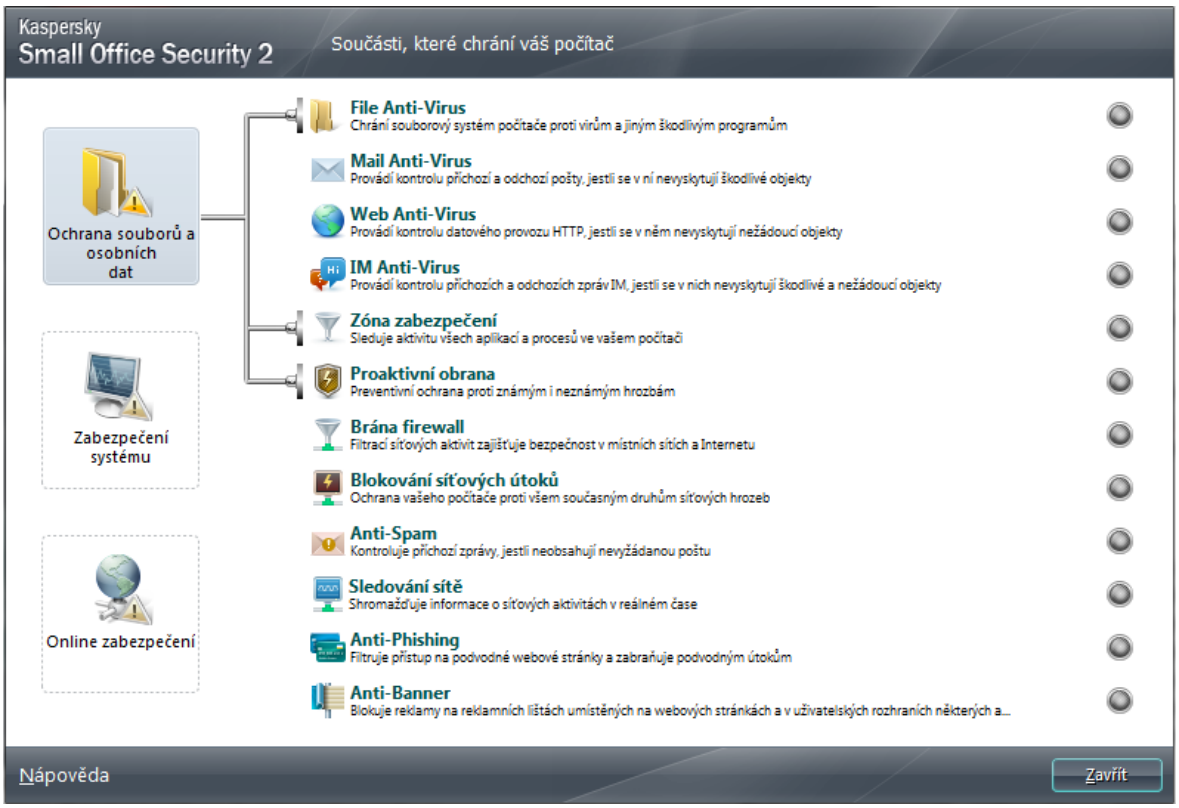
5.1.1 Ochrana souborů a osobních dat

Ochrana souborů a osobních dat se stará o bezpečnost dokumentů, tabulek, prezentací, uživatelských jmen, informací o platebních kartách, atd. Na této části ochrany se podílejí zejména tři služby: File Anti-Virus, Zóna zabezpečení a Proaktivní obrana.

File Anti-Virus – kontroluje všechny otevřené, uložené a aktivní soubory na přítomnost škodlivého softwaru. Soubory kontroluje na základě pravidelně aktualizované databáze a Heuristické analýzy (popsána v podkapitole 3.6).

Zóna zabezpečení – klasifikuje všechny aplikace a přiřazuje je do skupin zabezpečení. Aplikace v jednotlivých skupinách jsou dále omezovány podle pravidel platících pro danou skupinu. Celkem jsou 4 skupiny zabezpečení: důvěryhodné, nízké omezení, vysoké omezení a nedůvěryhodné. Každé z těchto skupin lze upravit pravidla. Pomocí těchto pravidel se dají upravovat práva aplikací pro práci v systému. Pokud má aplikace digitální podpis nebo se vyskytuje v databázi důvěryhodných aplikací služby Kaspersky Security, je možné přesunout aplikace rovnou do skupiny důvěryhodných aplikací. V opačném případě je nutné zjistit, jak velké riziko aplikace pro systém představuje.

Proaktivní obrana – chrání počítač před nejnovějšími hrozbami a to i těmi, které se zatím ještě nevyskytují v databázi programu. Je možné nastavit, které činnosti v systému bude proaktivní obrana v systému sledovat a vyhodnocovat jejich škodlivost.



Obrázek 2 - Přehled služeb ochrany

5.1.2 Systém a aplikace

Tato část ochrany se zabývá zejména ochranou souborů operačního systému a aplikací, instalovaných v počítači. Na ochraně se podílejí tyto služby: File Anti-Virus, Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Zóna zabezpečení, Brána firewall, Blokování síťových útoků.

File Anti-Virus – viz výše.

Mail Anti-Virus – kontroluje příchozí a odchozí zprávy na přítomnost nebezpečných objektů. Podporuje protokoly POP3, SMTP, IMAP, MAPI, NNTP. Je možné nastavit kontrolu pouze příchozí nebo příchozí i odchozí pošty. K identifikaci hrozeb se využívá Heuristická analýza.

Web Anti-Virus – chrání příchozí webové přenosy a zabraňuje spouštění nebezpečných skriptů v počítači. Při procházení webových stránek kontroluje, jestli se URL stránky, na které se právě uživatel nachází, nevyskytuje v databázi podezřelých adres či v databázi podvodných adres. Je možné nastavit citlivost Heuristické analýzy pro vyhledávání. U důvěryhodných adres je možné kontrolu vypnout. Ve spolupráci s Internet Explorerem je možné zakázat spouštění nebezpečných skriptů.

IM Anti-Virus – chrání přenosy z aplikací pro zasílání rychlých zpráv. Podporovanými aplikacemi jsou: ICQ, MSN, AIM, Yahoo!, Jabber, Google Talk, Mail.Ru Agent a IRC. Je možné nastavit kontrolu příchozích a odchozích zpráv a kontrolu URL adres nacházejících se ve zprávách.

Zóna zabezpečení – viz výše.

Brána firewall – filtruje veškerou síťovou aktivitu podle zadaných pravidel. V rozšířeném nastavení je možné upravovat pravidla firewallu jak pro odchozí tak pro příchozí komunikaci. Sítě se dělí do tří skupin: Důvěryhodné sítě, Místní sítě a Veřejné sítě. Při každém připojení do nové sítě, která nebyla dosud v programu uložena, se nás program dotáže, do jaké skupiny chceme právě připojenou síť zařadit. Pro jednotlivé skupiny sítí je pak možné upravit pravidla pro komunikaci v těchto sítích. Záznamy o všech sítích jsou uloženy v tabulce a je možné je nadále upravovat (název, skupinu oprávnění, podsítě, upozornění).

Blokování síťových útoků – zjišťuje síťovou aktivitu a útoky, které by mohly být nebezpečné. Zde je možné změnit pouze časový interval, po který bude daný počítač v seznamu blokovaných.

5.1.3 Online aktivita

Jak už název napovídá, tato část systému se stará o bezpečné prohlížení webových stránek, používání internetového bankovnictví a online nakupování, zasílání rychlých zpráv a používání sociálních sítí. Služby podílející se na této části bezpečnosti: Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Proaktivní zóna, Brána firewall, Blokování síťových útoků, Anti-Spam, Sledování sítě, Anti-Phishing a Anti-Banner.

Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Proaktivní zóna, Brána firewall, Blokování síťových útoků – viz výše.

Anti-Spam – kontroluje příchozí zprávy na obsah nevyžádané pošty. Veškerou příchozí poštu je možné filtrovat na základě adresy odesílatele, adresy příjemce a frází vyskytujících se v emailu. Programy Microsoft Office Outlook, Microsoft Windows Mail, Thunderbird a The Bat! mohou využívat tuto službu prostředím zásuvného modulu.

Sledování sítě – prostřednictvím firewallu shromažďuje informace o síťových aktivitách v reálném čase.

Anti-Phishing – kontroluje pokusy o otevření podvodných webových stránek a zabraňuje v přístupu na tyto stránky. V databázi si program udržuje informace o všech dosud známých podvodných webových stránkách. Tuto službu je možno využívat ve spojení se službami Web Anti-Virus, IM Anti-Virus a Anti-Spam.

Anti-Banner – na webových stránkách ve webovém prohlížeči a v některých aplikacích blokuje reklamu.

5.2 Zóna zabezpečení

Zóna zabezpečení zaznamenává chování aplikací v systému a přiřazuje jednotlivým aplikacím pravidla pro práci v systému podle toho, do jaké skupiny zabezpečení patří. Je možné zde označit aplikace, které mají běžet v simulovaném (sandbox) módu.

5.3 Kontrola

Spuštění a naplánování klasické kontroly systému. Máme možnost provést úplnou kontrolu systému, rychlou kontrolu systému nebo kontrolu pouze vybraných částí systému.

5.4 Aktualizační centrum

Aktualizační centrum se stará o pravidelnou aktualizaci databází a programových modulů softwaru. Zároveň obsahuje přehled počtu škodlivého softwaru, nevyžádané pošty, síťových útoků, atd. Máme možnost ručně spustit aktualizaci softwaru či návrat k předchozí verzi databáze, pro případ stažení špatné aktualizace.

5.5 Nástroje

Kromě základních nástrojů pro ochranu systému nabízí Kaspersky Small Office Security i řadu pokročilých nástrojů.

5.5.1 Zálohování a obnovení

V dnešní době, kdy většina důležitých a osobních informací existuje pouze v elektronické formě, je potřeba si zajistit, že o tato elektronická data nepřijdeme. Za tímto účelem nabízí Kaspersky možnost zálohování dat.

Před vytvořením zálohy dat je nejdříve potřeba vybrat si úložiště kam budeme zálohovaná data ukládat. Na výběr je ze 4 typů úložišť: vyměnitelná jednotka (např. externí disk), místní jednotka, síťová jednotka či FTP server. Každý typ úložiště je nejdříve potřeba nastavit a přidat do skupiny úložišť. Následně můžeme vytvořit zálohu dat. Nejdříve je potřeba vybrat si data, která si přejeme zálohovat. Poté vybereme, do kterého úložiště si přejeme zálohu vytvořit a jestli chceme, aby se záloha dat prováděla periodicky po určené době. V poslední řadě pouze určíme název zálohy a spustíme zálohování dat.

5.5.2 Správce hesel

Správce hesel umožňuje vytvoření bezpečných hesel a jejich uložení v bezpečném úložišti. Prvním krokem je nastavení hlavního hesla pro přístup do aplikace Password Manager a nastavení jeho základního nastavení (např. interval doby nečinnosti, po které se Password Manager zamkne).

Správce hesel je v podstatě databází přístupových hesel do aplikací, webových stránek, internetového bankovnictví, atd. Kromě hesel umožňuje i ukládání zabezpečených zápisů a identit. Je možné propojit správce hesel s webovými prohlížeči a tím si usnadnit přístup do webových stránek vyžadujících autorizaci.

Dalšími funkcemi správce hesel je vytvoření přenosné verze, díky které můžeme používat v něm uložená hesla kdekoliv, a vygenerování náhodného bezpečného hesla, včetně speciálních znaků, až do délky 99 znaků.

5.5.3 Šifrování dat

Pro lepší ochranu dat je možné vytvořit si na lokálním disku kontejner, který se bude chovat jako virtuální mechanika. Tento kontejner bude po odpojení zašifrován. Veškerá data, která do tohoto kontejneru přesuneme, pak budou zašifrovaná a bez přístupového hesla nebude možné se k nim dostat.

5.5.4 Virtuální klávesnice

Pokud zvolíme virtuální klávesnici, objeví se na displeji klávesnice, kterou můžeme používat myší. Tento nástroj slouží jako možná prevence v případě, že se obáváme, že máme na disku Keylogger nebo nějaký podobný škodlivý software, který by si mohl poznamenat naše hesla.

5.5.5 Další nástroje

Pod položkou Další nástroje se vyskytují nástroje pro optimalizaci funkčnosti webového prohlížeče Internet Explorer, odstranění závad v nastavení Microsoft Windows, vytvoření záchranného disku, trvalého odstranění dat a vymazání nepoužívaných souborů.

5.6 Centrum správy

Centrum správy slouží ke vzdálené správě počítačů ve firemní síti. Aby bylo možné spravovat zabezpečení na všech počítačích ve firemní síti, je nutné, aby každý počítač měl nainstalován stejný bezpečnostní software a aby v něm měl nastavené povolení vzdáleného spravování zabezpečení.

Po provedení základní konfigurace na počítači, který bude fungovat jako centrální počítač pro správu zabezpečení ostatních počítačů v síti, je možné si z tohoto stroje zobrazit informace o stavu a nastavení zabezpečení na všech počítačích v síti. Centrální počítač může vzdálené upravovat konfiguraci zabezpečení na jednotlivých strojích, spouštět či plánovat kontrolu na zařízení a spouštět aktualizaci na všech strojích současně, aby měli všechny stroje stejnou verzi databáze.

5.7 Správa zásad webových stránek

Pro každý vytvořený účet v systému je možné nastavit pravidla používání zařízení. Pokud se rozhodneme nastavit jednotlivým účtům tato pravidla, pak můžeme omezovat nejenom, k jakým datům bude uživatel mít přístup, ale také to, jak dlouho bude moct uživatel Internet používat nebo i jak dlouho bude moci používat samotný počítač. Pokud by správce systému chtěl, pak zde může kompletně omezit pohyb uživatele v počítači i na Internetu.

6 Nastavení systému

V první části praktické části bakalářské práce se zabývám instalací a nastavením softwaru Kaspersky Small Office Security. Praktická část byla prováděna na stroji Dell OptiPlex 9010. Hardwarová specifikace stroje: čtyřjádrový procesor Intel i5-3570 3,4Ghz, 2 harddisky o velikosti 500MB. Na tomto stroji běží, za pomoci systému VMware vspere 5hypervisor, virtuální stroje. Virtuální stroj, na kterém jsem vypracoval praktickou část bakalářské práce, měl zaveden OS Windows Server 2008 ve zkušební verzi.

6.1 Instalace softwaru

Instalace programu probíhá klasickým způsobem. Na začátku si uživatel zvolí, jestli chce nainstalovat systém automaticky, se standardním nastavením, či jestli si chce instalaci uzpůsobit podle svých preferencí. Stejně, jako u jakéhokoliv jiného programu, jsem si zvolil vlastní instalaci. Po odsouhlasení licenčního ujednání, jsem si zvolil umístění cílové složky pro instalaci programu. V dalším kroku jsem zvolil, že budu využívat firewall z antiviru místo standardní firewallu ve Windows. Není dobré používat oba dva najednou, mohlo by docházet ke kolizím. Následně dojde k samotné instalaci programu. Na konci instalace se program dožaduje licence pro užívání. Zvolil jsem si tedy zkušební třiceti denní verzi, ve které mám přístupné všechny služby a funkce. Po zvolení licence, mne program požádal o zvolení hesla správce a ke zvolení akcí, které budou toto heslo vyžadovat. Na dalších několika stránkách jsem zvolil, že si přeji rozhodovat o bezpečnostních akcích sám, tedy že nenechám program, aby rozhodoval za mne, že aktualizace budou probíhat pouze jednou týdně ve mnou zvolený čas.

6.2 Nastavení zabezpečení

V této podkapitole se budu zabývat nastavením zabezpečení, které software bude poskytovat. Každou službu ochrany je možné mít spuštěnou či vypnout podle toho, jaké služby chci používat. V rámci nastavování a pozdějšího testování bezpečnosti jsem spustil všechny služby. Funkčnost jednotlivých služeb je popsána v kapitole 5.1.

6.2.1 Obecné nastavení

Důležité je zmínit hned první položku v Centru ochrany a tou je Obecné nastavení. Obecné nastavení totiž obsahuje položku „Povolit ochranu“ a pokud není tato položka zaškrtnuta, pak je jedno, jak nastavíte ostatní služby ochrany, protože i přes to, že jednotlivé služby budou zapnuté, vám nebudou moci poskytnout slibovanou ochranu. Zároveň je možné si zde zvolit, jestli má program automaticky řešit hrozby. Nemám rád, když za mne jakýkoliv software rozhoduje a proto jsem tuto položku nechal neoznačenou.

6.2.2 File Anti-Virus

U některých služeb je možné nastavit, jakou úroveň ochrany budou poskytovat. U souborového antiviru jsem nastavil vysokou úroveň, protože později budu testovat, zda program odchytí mnou spouštěný infikovaný soubor. Nastavil jsem, aby program používal jak analýzu podle databáze tak i Heuristickou analýzu se střední úrovní kontroly. Heuristická

analýza je popsána v kapitole 3.6. Dále bude antivir kontrolovat všechny soubory včetně nových archivů, instalačních balíčků a všechny vložené OLE objekty. V rozšířeném nastavení, pro složené soubory, jsem rozhodl, že antivir bude kontrolovat složené soubory na pozadí a nezávisle na jejich velikosti.

6.2.3 Mail Anti-Virus

Antiviru, zaměřenému na emailovou komunikaci, jsem přikázal kontrolovat jak příchozí tak i odchozí poštu a to přes protokoly POP3, SMTP, NNTP i IMAP. V kontrole emailů se dá nastavit filtrování příloh, ale dá se nastavit pouze to, jaké přílohy nemá antivirus kontrolovat. Tato volba byla nežádoucí, protože požaduji, aby kontroloval veškeré přílohy v emailech. Antivirus poskytuje zásuvný modul pro MS Outlook. Funkčnost tohoto antiviru jsem později vyzkoušel při pokusech o prolomení.

6.2.4 Web Anti-Virus a IM Anti-Virus

Tyto dvě služby mají podobnou konfiguraci. Obě dvě jsem nastavil na střední úroveň kontroly a řekl jsem jim, aby kontrolovaly, zda se URL odkazů nevyskytují v databázi podezřelých či podvodných adres. Web antiviru jsem navíc přiřadil blokování nebezpečných skriptů.

6.2.5 Brána firewall

Brána firewall řídí chování paketů dle jejich směru, protokolu, portu a cílové adresy. Při nastavování brány, máme možnost toto chování změnit a to jak centrálně pro danou síťovou službu či pro danou aplikaci. Pokud chceme tato pravidla nastavit, zobrazí se nové okno s listem všech důvěryhodných aplikací a těmto aplikacím můžeme nastavit chování příchozích paketů. Vytvořil jsem tedy nové pravidlo pro aplikaci VLC (multimediální přehrávač, který umí přijímat televizní vysílání ze sítě) a povolil mu příchozí a odchozí UDP proudy.

6.2.6 Proaktivní ochrana

Proaktivní ochrana nabízí mimo jiné i sledování systémových procesů. Tuto službu testuji později pomocí programu Trojan simulator. Výsledek tohoto testu je popsán níže.

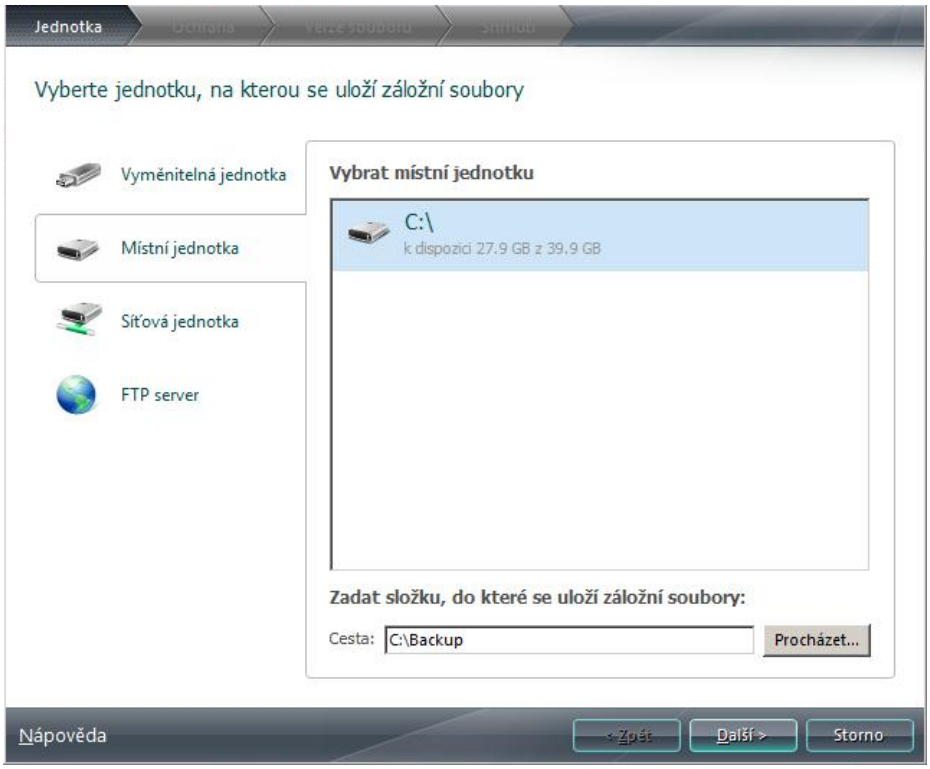
6.2.7 Anti-Spam

Zde si mohu nastavit, jaké zprávy jsou považovány za spam. Za spam jsem označil zprávy, které obsahují podvodné prvky a obsahují URL, které je v databázi podvodných adres. Nastavil jsem Anti-Spam, aby využíval k filtrování algoritmy Heuristické analýzy, technologie GSG (rozpoznávání grafické nevyžádané pošty) a algoritmus iBayes (samoučící algoritmus, který třídí nevyžádanou poštu podle charakteristických slov, vyskytujících se ve spamu). Rozhodl jsem, že spam bude vyhledávat u protokolů POP3, SMTP a IMAP. Zároveň jsem zvolil formu zásuvného modulu pro aplikaci MS Outlook.

6.3 Záloha dat a správce hesel

6.3.1 Zálohování

Nejdříve bylo potřeba vytvořit si datové úložiště, do kterého se budou všechny budoucí aktualizace tohoto stroje ukládat. Z nabídky jsem si zvolil místní jednotku a určil cestu do adresáře na lokálním disku, ve kterém bude úložiště vytvořené. V dalších krocích, vytváření datového úložiště, jsem přiřadil úložišti heslo pro přístup, zvolil, že se bude vždy uchovávat pouze jedna jediná verze ukládaného souboru a zvolil název pro mé nově vytvořené datové úložiště.



Obrázek 3 - Vytvoření datového úložiště

Pro vytvoření zálohy jsem nejdříve zvolil data, která si přeji zálohovat a mnou, v předchozím kroku, vytvořené datové úložiště. V dalším kroku jsem si zvolil, že si přeji, aby se zálohování provedlo jednou týdně ve čtvrtek, jednu minutu po poledni. V případě, že by stroj v dané chvíli nebyl spuštěn, by se záloha provedla ihned po spuštění stroje. Abych vyzkoušel plnou funkčnost programu, smazal jsem právě zálohovaná data a zkusil jsem je obnovit z právě vytvořené zálohy. Vše proběhlo bez problémů a ve velmi krátké době.

6.3.2 Správce hesel

Na počátku byly všechny funkce správce hesel nepřístupné a bylo zapotřebí provést konfiguraci přístupu do správce hesel. Při spuštění konfigurace se zapne samotná aplikace, která funguje nezávisle na softwaru, který aplikaci spustil. Jako první věc je zapotřebí nastavit heslo pro přístup do správce hesel a způsob, kterým bude prováděna autorizace pro přístup. Nastavil jsem tedy heslo a jako autorizační metodu jsem si zvolil ochranu heslem. Následovala možnost volby automatického zamknutí přístupu do aplikace v případě, že je

počítač po určitý časový interval nečinný. Zvolil jsem si interval 10 minut. Posledním nastavením bylo volba aplikací, které si nainstalují správce hesel jako doplněk, aby bylo možné hesla automaticky vyplňovat, za pomocí aplikace. Jelikož jsem na systému měl absolutní minimum programů, nebylo z čeho vybírat a tak jsem tento krok přeskočil. Po dokončení konfigurace se odemkli všechny funkce spojené s touto aplikací. Zároveň se mi na pozadí spustil správce hesel a běžel samostatně. Veškeré funkce pro správce hesel přístupné z antiviru je možné provést i přes samotnou aplikaci.

Vložení hesla: K přidání hesla do databáze je zapotřebí vytvořit v aplikaci účet, ke kterému se toto heslo pojí. Rozhodl jsem se vložit do databáze heslo pro webový účet a zadal adresu http://www.seznam.cz. Do formuláře na další stránce jsem vložil své přihlašovací jméno a heslo. Poté už zbývalo pouze odklepnout vytvořit účet. Následně jsem se odhlásil ze svého účtu na www.seznam.cz a nechal stránku znovu načíst. Když jsem se chtěl znovu přihlásit, správce hesel automaticky doplnil údaje ze své databáze do stránky a přihlášení proběhlo bez problému.

6.4 Nastavení vzdálené správy

Abych mohl spravovat bezpečnostní software Kaspersky i na jiném počítači, než na kterém jsem právě pracoval, bylo zapotřebí nejdříve nainstalovat tento software na cílovém stroji. Bohužel program neumožňuje nainstalovat software na vzdáleném, dosud nezabezpečeném, stroji a proto bylo potřeba nainstalovat na tomto stroji software ručně. Po instalaci programu na vzdáleném stroji bylo potřeba provést konfiguraci konzole pro správu. Jako síť, ve které budu vyhledávat zařízení, která chci vzdáleně spravovat, jsem si vybral síť LAN. Program se následně pokusil vyhledat všechna zařízení, která se na dané síti vyskytují. Stejně jako i u jiného softwaru, který se snaží nalézt na síti veškerá, zde se vyskytující zařízení, i zde byl problém s tím, že software nedokázal nalézt úplně všechna zařízení, která jsou do sítě připojená. Zadal jsem tedy vyhledávání zařízení dle IP adresy a přes příkazovou řádku jsem si zjistil adresu stroje, jehož software chci vzdáleně spravovat. Po zadání IP adresy stroje, se program snažil spojit se zařízením, nacházejícím se na dané adrese, a zjistit, jestli daný stroj má nainstalovaný požadovaný software.

Vzdálený počítač potvrdil, že má nainstalovaný požadovaný software a že je možné jej vzdáleně spravovat. Přešel jsem proto k dalšímu kroku konfigurace a nastavil, že stroj, na kterém se právě nacházím, má fungovat jako zdroj aktualizací pro ostatní počítače v síti a dokončil konfiguraci konzole pro správu.

Po spuštění Konzole pro správu se objevilo okno s informacemi o všech strojích vyskytujících se v síti. Zvolil jsem si počítač, který jsem před chvíli zpřístupnil pro vzdálenou správu, a aktivoval jsem mu na dálku všechny předtím vypnuté služby. Při pokusu o vzdálené spuštění aktualizace jsem zjistil, že aktualizace se už spustila sama od sebe, zřejmě zvolením mého stroje jako výchozího aktualizačního bodu pro všechny počítače v síti. Bohužel nebylo možné nechat zálohovat data na vzdáleném stroji, jelikož software

nepovoluje vytváření nových zálohovacích úloh na vzdálených strojích. Vytvořil jsem proto na vzdáleném stroji zálohovací úložiště a úlohu zálohování mnou zvolených souborů, která se bude dát spustit pouze na přímý příkaz. Po vytvoření této úlohy, bylo možné danou úlohu vzdáleně spustit.

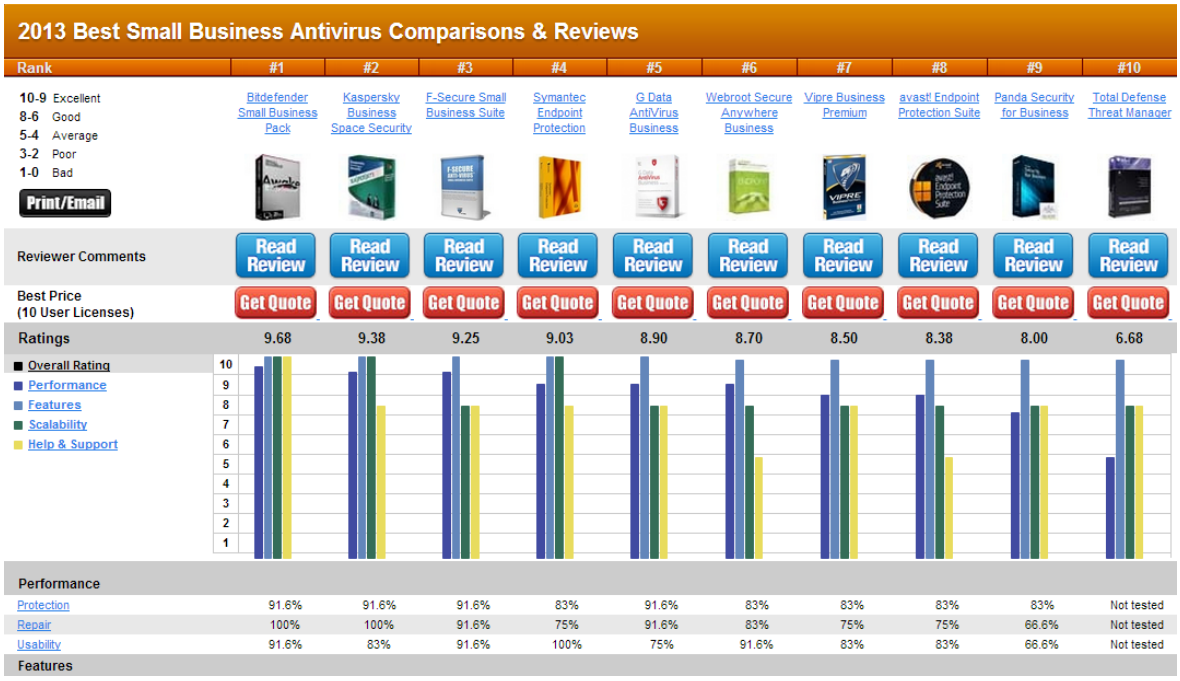
Na konec jsem spustil na všech strojích zároveň antivirovou kontrolu. Antivirová kontrola začala na všech strojích současně a proběhla bez problémů.

7 Porovnání s jinými produkty na trhu

V této kapitole bych rád porovnal systém Kaspersky Small Office Security s podobnými produkty na trhu. Pro porovnávání jsem se snažil zvolit pouze produkty určené pro malé firmy maximálně do deseti počítačů. Na trhu se vyskytuje velké množství bezpečnostních softwarů s různým stupněm efektivity ochrany. Testy jsem já sám neprováděl, jde pouze o testy a hodnocení přenesené z internetu.

7.1 Vyhodnocení funkčnosti podle AV-Test [9]

AV-Test je německý nezávislý institut pohybující se na poli antivirového výzkumu a antivirové ochrany přes 15 let. Hlavní náplní institutu je nalézání nejnovějšího škodlivého softwaru, analyzování škodlivého softwaru nejnovějšími metodami a upozorňování zákazníků o získaných výsledcích. Dalším cílem institutu je testování a certifikace bezpečnostních softwarů pro domácí uživatele a malé firmy. V oboru testování a certifikace se jedná o jeden z nejuznávanějších subjektů na trhu.



Obrázek 4 - Porovnání produktů na trhu

K testování softwarů došlo v červnu roku 2012 na platformě Windows 7. Na prvním místě skončil software od společnosti Bitdefender, který získal bodové ohodnocení 9.68/10. Oproti antiviru od firmy Kaspersky měl lepší pouze online podporu a pomoc. Na druhém místě se umístil antivir od firmy Kaspersky s hodnocením 9.38/10. Na třetím místě skončil antivir Small Business Suite od firmy F-Secure s bodovým ohodnocením 9.25/10. Nevýhodou antiviru od F-Secure je menší počet platforem, které podporuje.

8 Pokusy o prolomení

V 6. kapitole jsem popsal nastavení programu, které jsem provedl. V této kapitole se pokusím provést útok na systém a zjistit, jestli bude program schopný těmto útokům předejít či je zablokovat. Vypnul jsem jakékoliv další obrany, které se v systému vyskytovaly (Windows Firewall, ochranu ve webovém prohlížeči).

Na webových stránkách Eicar.org [12] je volně ke stažení soubor, popř. archivy obsahující tento soubor, který na svém počátku obsahuje jednoduchý text o 28 znacích: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*. Pokud využijete soubory dostupné na webových stránkách, anebo tento kus kódu vložíte na začátek souboru, který bude mít velikost přesně 68 bytů, antivirový program by měl tyto soubory nalézt jako potenciální hrozbu a dotázat se, co s nimi má udělat.

První test probíhal zcela jednoduše. Stáhnul jsem soubor eicar.com. Jakmile webový prohlížeč stáhnul soubor, antivir tento soubor zachytil a prohlásil ho za závadný. Postupně jsem stahoval další soubory z těchto stránek, které obsahují onen kus kódu. Antivir zachytil soubor eicar.com.txt, který se liší akorát jinou koncovkou, knihovnu eicar.zip, ve které se vyskytoval pouze zabalený soubor eicar.com, a zachytil i na dvakrát zabalený archiv eicar.zip, který v sobě obsahoval předchozí archiv. Při pokusu o prozkoumání archivu, mi byl odepřen přístup a musel jsem několik minut počkat, než jsem se mohl do infikovaného archivu podívat. V tu chvíli už byl infikovaný soubor smazán a archiv byl prázdný. Vyzkoušel jsem tedy, jestli archiv smaže pouze infikované soubory a jiné soubory v archivu nechá. Do dvakrát zabaleného archivu jsem tedy přibalil několik neinfikovaných souborů na různé úrovně a archiv nahrál na Internet. Po zapnutí antiviru jsem daný archiv znovu stáhl a podíval se, jestli smazal kompletní obsah archivu. Neinfikované soubory se v archivu stále vyskytovaly.

Dalším pokusem bylo simulování trojského koně v systému za pomoci programu Trojan Simulator staženého ze stránek Softpedia [13]. Z webové stránky si stáhnete archiv, který obsahuje program simulující proces trojského koně. Ve staženém archivu se vyskytují dva soubory: TrojanSimulator.exe a TSServ.exe. Po spuštění souboru TrojanSimulator.exe spustíte instalaci. Instalace nainstaluje demo trojského koně. Toto demo simuluje proces skutečného trojského koně. Simulace serveru funguje na bázi skrytí hlavního okna a zápisu do registrů. Tento trojský kůň se dá stejným programem odinstalovat (odebere i zápis z registrů). Po instalaci se objeví okno s informacemi, o spuštěném procesu v systému, spolu s jeho PID. Je tedy možné sledovat, jestli antivir odhalí onen proces a jestli ho zneškodní. Poté, co jsem spustil TrojanSimulator.exe a nainstaloval simulátor do systému, jsem si otevřel Správce úloh, našel si onen proces pomocí jeho PID a čekal, co se stane. Bohužel ani po deseti minutách antivir na tento proces nijak nereagoval. Spustil jsem tedy antivirovou kontrolu nad složkou, obsahující rozbalený archiv simulatoru. Ani tentokrát antivir nic nenašel. Spustil jsem tedy kompletní kontrolu systému, a když po zhruba hodině doběhl, tak nic špatného neobjevil. Došel jsem tedy k závěru, že program buďto tuto hrozbu nedokázal

identifikovat, to by bylo selhání antiviru, nebo proces simulující trojského koně našel a nevyhodnotil ho jako hrozbu, protože daný program zná a ví, že není škodlivý.

Tím jsem skončil s částí testování prolomení, ve které jsem zkoušel pouze simulovat hrozby na systém, a rozhodl se, že je na čase, zkusit jak si povede antivir s hrozbami na Internetu. Zde bych velmi rád zmínil, že ač je v dnešní době docela snadné nechat si infikovat nezabezpečený počítač neuváženým pohybem na Internetu, tak úmyslně sehnat nějaký vir, abyste si mohli otestovat obranyschopnost vašeho softwaru, je složitější, než by se mohlo na první pohled znát. Úmyslné šíření škodlivého softwaru, za jakýmkoliv účelem, je totiž nezákonné, a pokud ho chcete sehnat pouze za účelem otestování, není možné se k němu kdekoliv volně dostat. Naštěstí se mi podařilo najít několik diskuzních fór, na kterých se dají nalézt odkazy, na dosud živé, infikované stránky.

Abych otestoval antivir na ochranu proti dalšímu malwaru, zkusil jsem nainstalovat software Ardamax Keylogger 4.0.3. Po instalaci se objevilo upozornění na nebezpečí trojského koně a to přesně na: Trojan.Win32.Monder.oaay a HEUR:Trojan.Win32.Generic.12815508. silent.hw_22032013. Program byl tedy zachycen jako škodlivý a nebyl správně nainstalován.

Na webových stránkách Astalavista.com v části diskuzního fóra jsem narazil na odkaz, který měl obsahovat trojského koně. Po rozkliknuti onoho odkazu, mě ihned software informoval o nebezpečí ve formě trojského koně Trojan-spy.win32.keylogger.laf.

Ve dřívějších dobách existovali programy, které byly namířeny na odstraňování pouze jednoho jediného viru nebo trojského koně. Tyto programy mnohdy většinou, místo odstranění onoho škodlivého softwaru, nainstalovaly další tři jiné viry do počítače. Po chvíli hledání se mi podařilo jeden takovýto program, na odstraňování trojských koní, nalézt [14]. Při instalaci tohoto programu vyskočilo varovné okno informující o případné hrozbě Trojan.Win32.Generic!BT.

Další službu, kterou jsem otestoval, byl anti-banner. Postupně jsem vyzkoušel několik webových stránek, obsahujících vyskakující okna s reklamou. Nejjednodušší způsob, jak takovouto stránku najít, je projít adresář se spamem v emailové schránce a kliknout na odkazy, které obsahují pornografii nebo něco zadarmo. Pouze pro úplnost uvádím dva zástupce stránek, které obsahovali reklamu, a to: myrls.eu a chaturbate.com. Při testování služby Anti-Banner, se mi dostalo smíšených výsledků. Tato služba neblokuje 100% reklam, které se na webových stánkách vyskytují. Po bližším průzkumu jsem zjistil, že to asi není ani možné. Existují totiž skripty, pomocí kterých se tyto funkce dají obejít.

Při procházení spamu jsem narazil i na email, ve kterém byl odkaz s údajnou zprávou na adrese http://www.datingraha.ru/?0628EA=9B113B184B5810DECF3. Při pokusu o návštěvu této webové stránky došlo k zablokování přesměrování a stránka se nezobrazila. Při bližším prozkoumání důvodu zablokování stránky, jsem narazil na informaci, že byla nalezena hrozba Win32:Downloader-TBH.

V poslední části testování jsem zkusil za využití programu Metasploit obejít ochranu firewallu a zkusit se zmocnit systému. Na webové stránce youtube.com se vyskytuje video návod [15]. Pro ulehčení pojmenuji zdrojový systém, ze kterého je prováděn útok, systémem č. 1 a napadený systém, systémem č. 2. Útočník si v systému č. 1 pomocí příkazového řádku vytvoří soubor, kterým se pokusí ovládnout cílový systém. Poté si otevře zadní vrátka a naslouchá na portu 4444 na příchozí komunikaci. Na systému č. 2 zadá útočník adresu, na které systém č. 1 naslouchá, a stáhne soubor, určený pro ovládnutí systému č. 2. Útočník se poté vrátí na systém č. 1 a přes program Metasploit za pomoci programu, který je již stažen na systému č. 2, změní pozadí na napadeném systému. Tento pokus jsem se pokusil replikovat, ale bohužel se mi nepovedlo překonat ochranu firewallu a útok tak byl neúspěšný. Vzhledem k tomu, že toto video je už přes půl roku staré, mohu dojít jedině k názoru, že už tuto bezpečnostní chybu napravili a tím tento typ útoku znemožnili.

Pokusil jsem se provést několik útoků, abych vyzkoušel obranyschopnost systému, s nainstalovaným programem Kaspersky Small Office Security, a žádnému z mých útoků se nepodařilo překonat ochranu. Mohu tedy pouze konstatovat, že program si skutečně zaslouží svou reputaci, jako jeden z nejlepších ochranných softwarů na trhu.

9 Závěr

Tématem této bakalářské práce je „Zabezpečení Windows Server 2008 pomocí systému Kaspersky“. Jejím hlavním cílem bylo nastavit program Kaspersky Small Office Security a otestovat ho.

V úvodní části práce jsou uvedeny typy škodlivého softwaru, se kterými se v dnešní době běžně setkáváme. Jednotlivé typy byly blíže popsány a rozděleny podle jejich typického chování a nebezpečí, které mohou způsobit. U každého typu byl popsán způsob šíření a způsob infikování počítače.

Ve druhé části byly popsány způsoby obrany proti jednotlivým typům škodlivého softwaru. U jednotlivých programů byla popsána jejich funkčnost a techniky, které používají pro boj se škodlivým softwarem. U technik, které programy využívají, byly popsány jejich výhody a nevýhody.

V další části byla přiblížena společnost Kaspersky Lab, její zaměření a produkty, které vytvářejí pro zabezpečení rozdílných systémů. Jednotlivé produkty byly rozděleny do skupin podle typu zákazníka, pro kterého jsou zaměřené. U každého produktu bylo dále zjištěno, které služby poskytují a na co jsou zaměřené.

V hlavní části byl představen program Kaspersky Small Office Security. Byly rozebrány jednotlivé služby a nástroje, které program poskytuje. Zároveň zda byla provedena první praktická část bakalářské práce, ve které byl program nainstalován na virtuálním stroji a nastaven pro co nejlepší funkčnost.

V předposlední části byl program krátce srovnán s jinými produkty na trhu a byly vypsány jejich hlavní klady a zápory oproti tomuto programu.

V poslední části byla provedena druhá praktická část bakalářské práce. Byly zde provedeny útoky na systém a pokusy o prolomení obrany. Obrana byla otestována a program se všem pokusům o útok ubránil.

Neustále se mluví o tom, jak by měl být uživatel počítače obeznámen se základními hrozbami, které na něj všude na Internetu číhají. Mluví se o tom, jak by si měli uživatelé dávat pozor na to, jaké programy a soubory si do počítače stahují a instalují, jaké emaily lidé otevírají a že nemají otevírat přílohy u elektronických zpráv, jejichž odesílatele neznají. Pokud ale budou i nadále vytvářeny programy, jako je Kaspersky Small Office Security, nebude možná nutné, aby běžný uživatel vůbec o těchto nebezpečích věděl. Program je velmi jednoduchý na základní nastavení a poskytuje výbornou ochranu před všemi možnými hrozbami.

Práce pro mne byla velmi přínosná hlavně z důvodu zájmu o bezpečnost. Vždycky se v této oblasti rád něco nového naučím. Mám zájem se v budoucnosti problematice bezpečnosti blíže věnovat a tohle byl určitě zajímavý pohled na to, jak by takový bezpečnostní software měl fungovat.

Zdroje

[1] Úvod do antivirové problematiky: Jak dělíme počítačové viry. TRUSTPORT A.S. *TrustPort* [online]. ©2010 [cit. 2013-05-08]. Dostupné z: http://www.trustport.com/manuals/antivirus/csy/techvirsdiv.htm

[2] Typologie různých virů. SYMANTEC CORPORATION. *Symantec: Club Symantec* [online]. ©1995 - 2006 [cit. 2013-05-08]. Dostupné z: http://www.symantec.com/region/cz/clubsymantec/viruses.html

[3] Rootkity? Raději nepřehlížet. NYKODÝMOVÁ, Helena. *Lupa.cz* [online]. 10. 7. 2006 [cit. 2013-05-08]. Dostupné z: http://www.lupa.cz/clanky/rootkity-radeji-neprehlizet/

[4] CO JE TO PHISHING. DŽUBÁK, Josef. HOAX.CZ. *AntiviruWorld* [online]. © 2000-2013 [cit. 2013-05-08]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[5] Firewall - obrňte své počítače... MARTIN, Kuchař. *Pctuning* [online]. 2.2.2005 [cit. 2013-05-08]. Dostupné z: http://pctuning.tyden.cz/software/ochrana-pocitace/4296-firewall-obrnte_sve_pocitace

[6] How does anti-virus software work?. ANTIVIRUSWORLD. *AntiviruWorld* [online]. 12.12. 2008 [cit. 2013-05-08]. Dostupné z: http://www.antivirusworld.com/articles/antivirus.php

[7] KASPERSKY LAB. *Kaspersky* [online]. © 1997 – 2013 [cit. 2013-05-08]. Dostupné z: http://www.kaspersky.com/

[8] Významná změna v právní úpravě SPAMu od 1.1.2012. MALIŠ, Petr a Josef DŽUBÁK. *PravoIT* [online]. 06.02.2012 [cit. 2013-05-08]. Dostupné z: http://www.pravoit.cz/article/vyznamna-zmena-v-pravni-uprave-spamu-od-1-1-2012

[9] Anti-spam and spam filtering techniques. DARMANIN, Jesmond. *AllSpammedUp.com* [online]. 11. 10. 2011 [cit. 2013-05-08]. Dostupné z: http://www.allspammedup.com/anti-spam/

[10] *Eicar e.V.* [online]. © 1998-2013 [cit. 2013-05-08]. Dostupné z: http://www.eicar.org/

[11] ZACHAR, Martin. Co je to: Adware, Spyware, ... *Magazin.stahuj.centrum.cz* [online]. 29. 03. 2009 [cit. 2013-05-08]. Dostupné z: http://magazin.stahuj.centrum.cz/co-je-to-adware-spyware-/

[12] 2013 Best Small Business Antivirus Comparisons & Reviews. TOPTENREVIEWS. *Toptenreviews.com* [online]. © 2013 [cit. 2013-05-08]. Dostupné z: http://anti-virus-software-review.toptenreviews.com/small-business-antivirus/

[13] CIRNEALA, S. Trojan Simulator 1.0. *Softpedia* [online]. 10. 11. 2004 [cit. 2013-05-08]. Dostupné z: http://www.softpedia.com/get/Antivirus/Trojan-Simulator.shtml

[14] Anti Trojan Elite. *Download25.com* [online]. © 2005-2013 [cit. 2013-05-08]. Dostupné z: http://www.download25.com/install/anti-trojan-elite.html

[15] MUSE, Mike. Bypassing kaspersky. *Youtube* [online]. 5. 10. 2012 [cit. 2013-05-08]. Dostupné z: http://www.youtube.com/watch?v=EQAaDqqF1rc