Projektové řešení zabezpečení firemní sítě dle BS7799

Project solution for corporate network security by BS7799

Bc. Jan Stanovský

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan STANOVSKÝ**
Osobní číslo:	**A09429**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Projektové řešení zabezpečení firemní sítě dle BS7799**

Zásady pro vypracování:

1. **Proveďte literární rešerši k danému tématu.**
2. **Analyzujte možnosti zabezpečení sítí dle norem a standardů v oblasti informační bezpečnosti.**
3. **Formou projektu navrhněte a realizujte replikovatelné řešení.**
4. **Proveďte diskusi nad řešeným problémem.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KRÁL, Mojmír. Bezpečnost domácího počítače :prakticky a názorně. 1. vyd. [s.l.] : Grada, 2006. 334 s. ISBN 80-247-1408-6.**
2. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. [s.l.]: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.**
3. **JAŠEK, Roman. Informační a datová bezpečnost. 1. vyd. [s.l.]: Academia centrum UTB, 2006. 140 s. ISBN 80-731-8456-7.**
4. **THOMAS M., Thomas. Zabezpečení počítačových sítí bez předchozích znalostí. 1. vyd. [s.l.]: Computer Press, 2005. 338 s. ISBN 80-251-0417-6.**
5. **ANDREW, Lockhart. Bezpečnost sítí na maximum: 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě . 1. vyd. [s.l.] : Computer Press, 2005. 280 s. ISBN 80-251-0805-8.**
6. **STREBE, Matthew; PERKINS, Charles. Firewally a proxy-servery: praktický průvodce. 1. vyd. [s.l.]: Computer Press, 2003. 472 s. ISBN 80-722-6983-6.**
7. **LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. [s.l.]: Computer Media, 2008. 98 s. ISBN 80-866-8635-3.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **13. června 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je poskytnout informace z oblasti softwarového zabezpečení počítačové sítě. V teoretické části jsou popsány druhy škodlivého softwaru, příznaky napadení počítače a nejznámější zástupci jednotlivých druhů malwaru. Dále jsou zde popsány způsoby softwarové ochrany počítače, metody používané k detekování malwaru a srovnávací testy antivirových systémů. V praktické části se nachází návrh řešení softwarového zabezpečení firemní sítě.

Klíčová slova:

Antivirový systém, firewall, antispyware, malware, software, počítačový virus, červ, trojský kůň, bezpečnost sítě, ochrana počítače, Internet, útok.

ABSTRACT

The aim of this work is to provide information referring to corporate network software security. Types of malware, signs of computer infection and the most famous specimen of malware are described in the theoretical part of this work. Software security methods, malware detection methods and antivirus system comparative tests are described here as well. Design of solution for corporate network security is described in practical part of this work.

Keywords:

Antivirus system, firewall, antispyware, malware, software, computer virus, worm, trojan horse, network security, computer security, Internet, attack.

PODĚKOVÁNÍ

Chtěl bych poděkovat vedoucímu mé diplomové práce panu doc. Mgr. Romanu Jaškovi, Ph.D. za připomínky a poskytnutí cenných informací a zdrojů k této diplomové práci. Dále bych chtěl poděkovat své rodině a přítelkyni, kteří mě podporovali jak po celou dobu studia, tak při psaní této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

V dnešní době je problematika škodlivého softwaru a ochrana před ním stále více aktuální a nabývá na důležitosti. Připojení k Internetu je již dstupné téměř v každé domácnosti, firmě nebo škole, s čímž souvisí i riziko napadení počítače či dokonce celé vnitřní sítě. Proto je nutné svá data adekvátně chránit. Po Internetu koluje obrovské množství všech možných virů, červů, trojských koní, spywaru, backdoor aplikací a jiného škodlivého kódu, který může infikovat systém, poškodit data na disku, odcizit důvěrné informace či dokonce poškodit samotný počítač. Vhodným způsobem, jak se proti této hrozbě zabezpečit je instalace antivirového systému, který poskytuje komplexní ochranu proti všem druhům útoku. Společnosti vyvíjející tento software svádí neustálý boj s autory škodlivého kódu, aby zamezili možným škodám způsobených jejich výtvory.

K výběru tohoto tématu mne vedl zájem o bezpečnost a počítačové sítě jako takové. Tato problematika je navíc velmi diskutovaná a její zpracování mi může přinést mnoho nových zkušeností a poznatků. Práce si klade za cíl přiblížit čtenáři nebezpečnost ukrývající se v síti Internet a navrhnout možné řešení otázky ochrany před těmito hrozbami. Mou snahou je poukázat na nejčastější případy napadení počítače a chyby uživatelů. Hlavním cílem však je navrhnout řešení, které by dokázalo ochránit firemní síť před jakýkoliv druhem malwaru.

I. TEORETICKÁ ČÁST

1 MALWARE

Pod pojmem malware, který vznikl spojením dvou anglických slov - malicious (zákeřný) a software (programové vybavení) - rozumíme souhrnné označení pro veškerý škodlivý kód jako jsou viry, trojští koně, spyware, adware nebo jakýkoliv jiný program, který svým spuštěním zahájí činnost škodící systému, ve kterém se nachází. Tento pojem definuje spíše záměr jeho autora než samotné vlastnosti programu.

1.1 Počítačové viry

Počítačový virus je malý softwarový program, který napadá soubory na disku nebo systémové prvky. Obvykle se dostane do počítače, aniž by o tom uživatel věděl. Platí zde nejenom to, že se vir dostane do počítače bež vědomí či přání jeho uživatele, ale i samotná činnost viru je uživateli skryta. Virus nelze ani najít ve výpisu adresáře či disku. Viry jsou schopné množit sebe sama, k tomu ale potřebují jiný soubor, popř. program nebo místo na paměťovém médiu, do kterých zapíše svůj kód nebo jeho funkční část. Po spuštění takového souboru se virus dále šíří a takto se cyklus opakuje. Takovému procesu šíření se říká nakažení nebo infekce a napadenému souboru hostitel. Tyto označení pocházejí z analogie s termíny používanými pro biologické viry.

Účel virů je jasný - napadnout co nejvíce programů/počítačů a provádět škodlivé akce. Škody způsobené počítačovým virem mohou být různé - od poškození dat až po smazání celého obsahu pevného disku. Existují ale také viry, které neškodí ve smylu mazání dat, ale svými žertovnými zvuky, grafickými efekty nebo jinými způsoby zpomalují chod systému nebo znemožňují provoz některých programů.

Způsobů, jak se může dostat virus do počítače, je hned několik. V dřívější době, kdy ještě nebyl Internet tolik rozšířený, se nejčastěji dostal virus do počítače ze zavirované

diskety. S příchodem nových typů médií se staly nositely virů CD a DVD disky. Způsob přenesení do počítače byl přitom velice jednoduchý - nakažený program se i s virem zkopíroval bez jakýchkoliv problémů do počítače. V dnešní době se viry přenášejí zejména přes celosvětovou síť Internet a přes lokální sítě. Přenesením do počítače se ovšem tento nestává infikovaným. K nákaze dojde až po spuštění hostitele viru. Mechanismus nákazy a činnost prováděná virem mohou být popsány následovně (neplatí striktně pro všechny viry, některé kroky mohou být vynechány nebo provedeny v jiném pořadí):

1. Infikovaný program/soubor je přenesen do počítače
2. Po spuštění programu/souboru se nejdříve spustí virus v něm obsažený (virus přesměroval zaváděcí adresu nebo skok na sebe) a převezme kontrolu nad procesorem
3. Virus zkontroluje aktuální stav prostředí
4. Usídlí se v operační paměti počítače
5. Přesměruje přerušení
6. Provede test na podmínku spuštění škodlivé akce (specifické datum - virus Černobyl, počet spuštění atd.)
7. Provede škodlivou činnost
8. Najde vhodné místo pro vytvoření svojí kopie
9. Virus napadne další programy/soubory na pevném disku a předá řízení původnímu programu

Obecně lze říct, že činnost virů se skládá ze dvou hlavních akcí - šíření sebe sama do ostatních souborů na disku (ať už náhodně nebo podle určitého vzorce) a vykonávání své vlastní škodlivé činnosti. Viry mají zpravidla tendenci maskovat svoji přítomnost a nezřídka se stává, že jsou postupem času infikovány téměř všechny soubory na disku, které uživatel spustil. Je-li navíc vložena do napadeného počítače disketa s programem, případně na ni nějaký program nahráváme, stává se infikovanou i tato.

1.1.1 Dělení počítačových virů

Hledisek, podle kterých můžeme počítačové viry dělit, existuje více. Může to být způsob, jak se virus v počítači chová, jaké objekty napadá nebo jak je v počítači umístěný.

Podle cílového objektu infekce můžeme viry dělit do následujících skupin:

- Souborové viry - jsou uloženy ve spustitelných souborech typu COM, EXE, SYS nebo v souborech typu BIN a dalších obsahujících spustitelný kód. Soubor je napaden tak, že je k jeho vlastnímu kódu připsán kód viru, případně může být část kódu přepsána tím virovým. Funkčnost původního program ovšem zůstane zachována. Virus se pak spouští s každým spuštěním programu, vytváří své kopie a vkládá je do ostatních souborů.
- Boot viry - tento typ viru sídlí v boot sektoru diskety nebo v MBR pevného disku. Do počítače se rozšíří pouze v případě, zavedeme-li systém z infikované spouštěcí diskety. Samotné napadení diskety nebo MBR tabulky probíhá nahrazením originálního boot sektoru vlastním programem viru. Zároveň se virus načte do paměti a poté se může samovolně šířit na další diskety nebo pevné disky bez nutnosti přenosu kopírováním souborů.
- Cluster viry - tyto viry upravují FAT nebo NTFS tabulku přesměrováním ukazatele na kód viru. Tento typ viru je obzvlášť nebezpečný, jelikož nijak nemění délku ani obsahu souboru a je tedy hůře detekovatelný.
- Makroviry - tento typ virů využívá toho, že moderní aplikace ve svých datových souborech uchovávají kromě čistých dat i nástroje na jejich další zpracování, jako jsou například makra v programu MS Word. Makra jsou uložena ve stejném dokumentu jako text a spousta z nich může být spuštěna spolu se spuštěním Wordu, popřípadně s otevřením dokumentu. Některé makroviry mohou být spojené s tlačítky na nástrojové liště, položkami menu nebo určitou klávesou. Makro může být poměrně jednoduše zkopírováno z dokumentu do globální šablony a odtud může být poté vir aktivován při každém použití Wordu. Naštěstí díky důkladné lokalizaci Wordu většina makrovirů v české verzi nefunguje.

Další hledisko, podle kterého viry rozdělujeme, je způsob setrvávání v počítači:

- Rezidentní viry - při spuštění napadeného programu se virus uloží do operační paměti, kde setrvává až do vypnutí počítače. Po celou dobu pak napadá veškeré uživatelem spuštěné programy.
- Nerezidentní viry - tyto viry nezůstávají v operační paměti, po spuštění svého hostitele (a tím i kódu samotného viru) obvykle nakazí soubory v aktuálním adresáři.

1.1.2 Příznaky napadení virem

Příznaků, které ukazují na přítomnost viru, existuje spousta. Ne vždy se ale nutně musí jednat o vir, který tyto potíže způsobuje. Níže popsané příznaky mohou značit jiné, například hardwarově nebo softwarově založené problémy. Nicméně následující situace patří mezi nejčastější ukazatele na napadení počítače virem:

- Počítač přestává reagovat, často dochází k jeho zablokování
- Na obrazovce se objevují neobyvklé chybové zprávy
- Po zobrazení chybového okna se počítač samovolně restartuje
- Počítač je zpomalený, běžné úkony trvají mnohem déle než obvykle
- Programy nefungují správně, nejdou spustit
- Ze systray zmizela ikona antivirového programu, program nelze spustit
- Nelze nainstalovat antivirové program
- Nelze spustit správce úloh
- Některé disky nebo diskové jednotky nejsou k dispozici
- Nelze správně vytisknout dokumenty
- Z počítače samovolně zmizí program
- Na ploše se objevují nové ikony
- Z reproduktorů se ozývají neznámé zvuky nebo hudba

- Na disku je čim dál tím méně volného místa
- Upozornění systému na nedostatek operační paměti

1.1.3 Nejznámější počítačové viry

Od roku 1986, kdy spatřil světlo počítačového světa první opravdový počítačový virus, vzniklo již několik stovek milionů zástupců tohoto druhu malwaru. Ovšem pouze malá část z nich způsobila antivirovým programům nemalé problémy a dokázala proslavit své tvůrce. Zde je chronologický přehled těch nejznámějších virů za 25 let jejich existence:

- V roce 1983 sestrojil Dr. Frederick Cohen první program, který se začal označovat jako vir. Jednalo se ale o zcela neškodný kód, který se uměl pouze sám množit.
- Brain (1986) - bratři Basid a Amjad Farooq Alvi z Pakistánu naprogramovali první počítačový vir, který mohl nějak škodit. Autoři byli prodejci softwaru a pomocí viru chtěli zmapovat rozsah počítačového pirátství v Pakistánu. Vir se ovšem téměř okamžitě rozšířil po celém světe. Šířil se pomocí infikovaných disket a bylo obtížné jej detekovat. V podstatě se jednalo o první stealth vir, jelikož dokázal maskovat svou přítomnost tím, že při pokusu operačního systému číst z infikovaného sektoru jej vir nahradil původním čistým.
- Christmas tree (1987) - první síťový virus, který dokázal zpsobit epidemii. Vir nejprve pronikl do sítě jedné západoněmecké univerzity, poté se rozšířil do sítě evropského akademického výzkumu a do IBM. Za čtyři dny vir zaplnil síť svými kopiemi a tím ji paralyzoval. Po spuštění zobrazil vir na obrazovku vánoční stromek a odeslal svou kopii všem uživatelům, jejichž adresy byly uložené v počítači.
- Jerusalem (1987) - pravděpodobně jeden z prvních virů pod MS-DOS, který způsobil opravdovou pandemii. Napadeno bylo několik společností a univerzit z celého světa, zprávy o napadených počítačích se objevovaly z Evropy, Ameriky a ze Středního východu. Virus se aktivoval každý pátek 13. a mazal veškeré programy, které byly v ten den spuštěny.

- Michelangelo (1992) - tento vir byl podobný viru Jerusalem - setrvával v počítači a aktivoval se každý rok 6. března (datum narození světoznámého renesančního umělce). Pokud byl počítač v tento den spuštěn, přepsal virus prvních 100 sektorů pevného disku nulami a navíc přesunul MBR záznam na jiný sektor disku. Poté, co se informace o viru dostaly na veřejnost, vypukla hysterie způsobená přehnanými tvrzeními o řádově až milionech napadených počítačů. Avšak zaznamenaný počet napadení tímto virem byl pouhých 10 až 20 tisíc. Díky tomuto rozruchu vydělaly některé antivirové společnosti. V následujících letech virus ztratil na nebezpečnosti, jelikož stačilo v inkriminovaný den nezapínat počítač.
- Černobyl / CIH (1998) - asi nejznámější virus díky svému masivnímu rozšíření a míře poškození, kterou způsoboval. Virus měl nastavený spouštěč na 26. dubna, tj. na výročí havárie černobylské jaderné elektrárny. Byl jedním z nejničivějších virů, jelikož v první fázi přepisoval prvních 1024 KB pevného disku nulami a zadruhé napadal a ničil určité druhy Flash BIOSu. To způsobovalo nefunkčnost počítače a pro laika to v podstatě znamenalo jeho zničení. V případě prvního důsledku činnosti viru byly přepsaná data ztracena. V určitých případech ale bylo možné je obnovit. Pokud se ovšem viru podařilo uskutečnit druhý krok, bylo nutné přeprogramovat, případně výměnit, Flash BIOS čip. V dnešní době už není virus rozšířen v takové míře, jako byl dříve, jelikož napadá pouze starší verze OS Windows (95, 98, Me).
- Melissa (1999) - tento makrovir nebyl určený k poškozování uživatelských dat nebo počítačů, účelem viru bylo způsobovat škody přetížením serverů. Virus se přenášel e-mailovými zprávami a byl obsažen v přiloženém souboru List.doc, který obsahoval hesla ke zpřístupnění webových stránek s pornografií. Virus se šířil skrze programy MS Word 97, 2000, MS Excel 97, 2000 a 2003. Dále se rozesílal pomocí poštovního klienta MS Outlook 97 a 98, kdy sesbíral prvních 50 adres v seznamu a odeslal na ně svou kopii.

1.2 Počítačoví červi

Červ (anglicky worm) je další z mnoha zástupců malwaru a někdy je označován jako podtřída viru. Tento jednoduchý škodlivý program se, narozdíl od viru, dokáže samostatně šířit v počítači a rozesílat přes síť své kopie ostatním počítačům. Nejčastějším způsobem přenosu jsou e-mailové zprávy, respektive přílohy v nich obsažené. Samotný princip šíření červů je založen na zneužití bezpečnostních děr v operačním systému a úspešnost napadení je dáno rozšířením daného softwaru, který tuto bezpečnostní díru obsahuje. V počítači se obvykle červ rozmnožuje tak, že se zapíše do operační paměti a vytváří své kopie tak dlouho, dokud nezaplní paměť tak, že už v nich není prostor pro další programy. Tím způsobí zhroucení počítače. Další charakteristickou činností červa je zkopírování seznamu adres, které si uživatel eviduje, a rozeslání své kopie na tyto adresy. Předmět i název přílohy e-mailové zprávy obvykle uživatele láká na různé fotografie obnažených celebrit nebo hesla k pornografickým stránkám. Díky tomu je červ schopný se rozšířit během několika hodin na řádově miliony počítačů.

1.2.1 Dělení počítačových červů

Stejně tak jako dělíme počítačové viry, můžeme i červy rozdělit do několika skupiny podle toho, jakým způsobem se šíří:

- E-mailoví červi - ke svému šíření využívají elektronickou poštu. Po napadení počítače se rozešlou na e-mailové adresy uložené v uživatelově seznamu kontaktů nebo nalezené při prohledávání obsahu souborů na pevném disku. E-mailové zpráva obvykle obsahuje infikovanou přílohu nebo odkaz na webovou stránku, která je schopná infikovat počítač uživatele. Touto cestou často vznikají sítě botnet, které slouží k hromadnému rozesílání spamu, DDoS útokům nebo šíření spyware a adware. Úspěšnost šíření tohoto druhu červů spočívá ve zneužití e-mailového účtu oběti a rozeslání svých kopií z jeho adresy, díky čemuž působí zpráva pro příjemce důvěryhodně.
- Internetoví červi - tento typ červů využívá všechny dostupné síťové prostředky počítače ke skenování ostatních počítačů v síti. Jestliže najde zranitelný počítač

a dokáže této zranitelnosti využít, automaticky provede útok. Úspěch napadení závisí na závažnosti zranitelnosti, v ideálním případě je červ schopen spustit svůj škodlivý kód a infikovat systém. Nebezpečí tohoto typu červa spočíví ve schopnosti napadnout počítač bez vědomí a přičinění uživatele.

- IM a IRC červi - tento druh červů využívá ke svému šíření komunikaci v reálném čase, jako je například protokol ICQ nebo kanály IRC. V případě IM komunikace jsou rozesílány odkazy směřující na webové stránky schopné infikovat počítač. Nejčastěji se jedná o ruskojazyčné zprávy a odkazy s doménou RU. Dalším příznakem je přijetí zprávy od uživatele, který je offline (u některých typů ICQ klientů je ovšem možnost nastavení neviditelného stavu a v takovém případě se uživatel jeví jako odpojený). U IRC komunikace je situace o něco méně nebezpečná. Zde jsou rozesílány přímo infikované soubory v podobě spustitelného souboru. Aby došlo k napadení, musel by ovšem uživatel akceptovat přijetí tohoto souboru, uložit si jej do počítače a poté spustit. Výhodou tohoto způsobu šíření je opět zdání důvěryhodnosti, jelikož jsou odkazy a soubory odesílány z napadeného počítače některého z uživatelových kontaktů.
- Červi využívající sdíleného prostoru - červ tohoto typu se šíří za pomocí sdílení souborů. Červ ukládá své kopie v podobě spustitelného souboru na sdílená místa nebo na vzdálený úložný server a dává jej tak k dispozici ke stažení. Využívá přitom dnešního trendu sdílení nelegálního obsahu a při použití vhodného názvu souboru je možné jeho rozšíření ve velké míře.

1.2.2 Nejznámější počítačoví červi

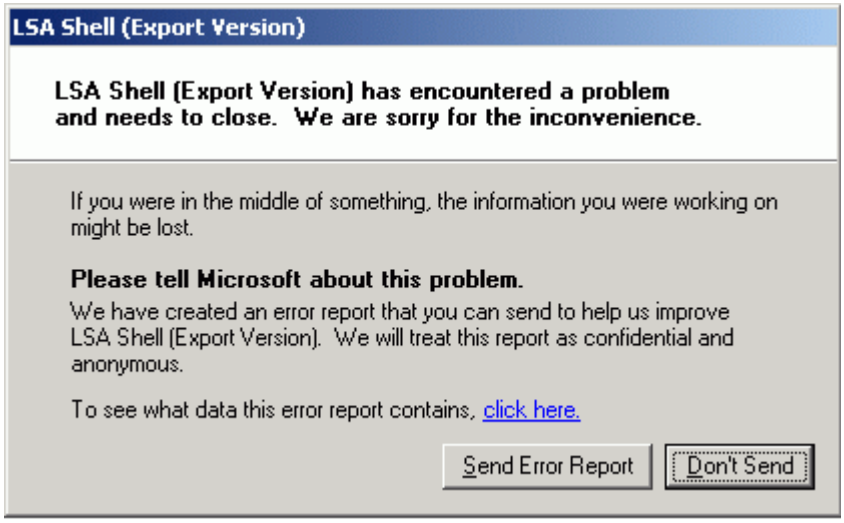
Mezi nejznámější počítačové červy, ať už z důvodu jejich masivního rozšíření nebo škod, které svým chováním způsobili, můžeme zařadit:

- Morris (1988) - student Robert Morris způsobil svým červem totální epidemii, bylo napadeno více než 6000 počítačových systémů v USA včetně NASA. Tento červ neomezeně rozesílal své kopie do ostatních sítí a kompletně paralyzoval všechny síťové zdroje. Způsobená škoda byla vyčíslena na 100 milionů dolarů. Červ navíc jako první sbíral uživatelská hesla.

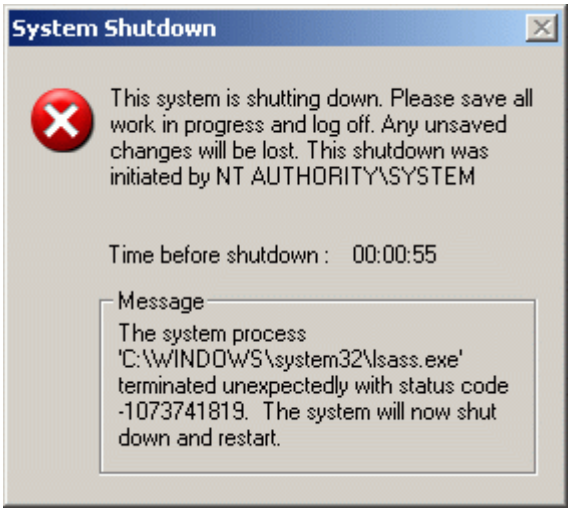
- I love you (2000) - tento červ se jako většina šířil v podobě přílohy e-mailové zprávy, dokázal napadnout desítky milionů počítačů po celém světě a způsobit škodu vyčíslenou na 5,5 miliardy dolarů. Zasaženy byly počítače Pentagonu, CIA, britského parlamentu nebo velkých korporací. Po otevření přílohy, která se tvářila jako běžný TXT dokument, ale ve skutečnosti se jednalo o soubor VBS, se nastavilo spouštění červa při každém startu počítače. Dále byly všechny soubory na disku s příponami JPG, JPEG, MP2, MP3, VBS, VBE, JS, JSE, CSS, WSH, SCT a HTA nahrazeny kopií červa. Nakonec se na všechny adresy uložené v seznamu programu MS Outlook odeslala kopie zprávy obsahující přílohu s červem.
- SQL Slammer (2003) - červ zneužíval bezpečnostní díru v MS SQL Serveru způsobenou podtečením zásobníku. Jestliže dorazil na port 1433 SQL Serveru UDP paket o specifické délce 376 B, došlo díky podteční zásobníku k jeho infekci. Následně se červ usídlil v paměti a začal rozesílat spoustu UDP paketů na náhodné IP adresy, čímž způsobil kolaps mnoha sítí. Propuknutí nákazy mělo exponenciální průběh, v počáteční fázi byl nárůst dvojnásobný s periodou 8,5 sekund, přičemž jeho zpomalení bylo zapříčiněno pouze díky pádu mnoha sítí z důvodu zahlcení způsobené DoS útokem. Během prvních 10 minut bylo napadeno 90% zranitelných strojů. Paradoxem je, že záplata ošetřující tuto díru byla vydána již půl roku před vypuknutím nákazy. Naštěstí nebyla aplikace MS SQL Server běžnou výbavou každého počítače. V opačném případě by byly důsledky nepředstavitelné.
- Blaster / Lovesan (2003) - tento červ se šířil v OS MS Windows XP a 2000, ve kterých nebyly nainstalované potřebné záplaty. Červ pronikl k uživatelům po celém světě, u kterých to bylo technicky možné ve významu struktury zapojení LAN sítě. Ve své době se jednalo o největší incident v historii Internetu. Příznakem napadení byl restartující se OS Windows s minutovým odpočtem a oznámení o chybě spojené s procesem SVCHOST.EXE. Červ by napáchal ještě větší škody, pokud by se mu podařil plánovaný DDoS útok na server windowsupdate.com. Útok měl být zahájen ze všech infikovaných počítačů, které měly server hromadně zahltit obrovským množstvím síťových paketů a znepřístupnit ho tak běžnému uživateli. Microsoft naštěstí dočasně server odpojil a přesměroval útok na jinou stránku, díky čemuž byly způsobené škody minimální.

- Sasser (2004) - tento červ, tak jako Blaster, napadal OS MS Windows XP a 2000, které nebyly aktualizované a obsahovaly bezpečností díru. Systémy Windows 95, 98 a ME nemohly být červem napadeny, ale mohly sloužit k jeho šíření. Do systému se Sasser dostal díky díře v zabezpečení síťového portu. Šířil se pomocí Internetu, ne však e-mailovou poštou. Po napadení systému si červ vytvořil v adresáři Windows spustitelný soubor a do registrů přidal jeho automatické spuštění po restartování počítače. Poté si vytvořil vlastní FTP server a na náhodně vygenerované IP adresy odeslal pomocí otevřených portů paket, který mu umožnil pracovat s počítačem oběti. Naštěstí nebyl virus destruktivní, ale pouze se zkopíroval na vzdálený počítač. Ukazatelem na přítomnost viru bylo značné zpomalení počítače, chybové hlášky spojené s LSASS.EXE a následné restartování systému (jak je možné vidět na Obr. 1 a Obr. 2), aktivní Internetové připojení při nečinnosti uživatele nebo otevřené porty 445, 5554 a 9996. Červ způsobil výpadek satelitní komunikace novinové agentury AFP, americká letecká společnost Delta Air Lines musela zrušit několik zaoceánských letů z důvodu zaplavení systémů tímto červem, britská pobřežní služba měla několik hodin zablokovanou elektronickou mapovací službu a i další instituce, jako například investiční bankovní společnost Goldman Sachs, přepravní skupina Deutsche Post nebo nadnárodní orgán Evropská komise, měly s tímto červem problémy. Společnost Microsoft vypsala odměnu 250 USD za informace vedoucí k dopadení jeho autora, na jejichž základě byl dopaden 18-letý německý student Sven Jaschan. Jaschan byl souzen jako nezletilý, jelikož v době, kdy červa vytvořil, mu bylo ještě 17 let. Byl shledán vinným z počítačové sabotáže a neoprávněné úpravy dat a byl mu udělen podmíněný trest na 21 měsíců.
- Mydoom (2004) - velice známý počítačový červ, jenž se šíří pomocí e-mailů a dodnes se vyskytuje na Internetu v několika variantách. Napadá 32-bitové verze OS MS Windows 95, 98, ME, 2000, NT, Server 2003 a XP. V případě napadení počítače červ otevře porty, čímž jsou útočníkovi zpřístupněny soubory oběti, pomocí DDoS útoku se zamezí přístup k serverům společnosti Microsoft a červ je automaticky rozeslán dále. Mydoom se šíří jako příloha elektronické pošty v podobě souboru ve formátu EXE, BAT, CMD, PIF, SCR nebo jako archiv ZIP, RAR, CAB a jiné. Jsou známy tři varianty - Mydoom.A, Mydoom.B a Mydoom.C.

První varianta červa otevíra TCP porty a vyhledává v souborech HTM, PHP, ASP, TXT atd. E-mailové adresy, na které se následně rozešle. Druhá varianta zabraňuje přístup k serverům společnosti Microsoft a k některým dalším serverům antivirových společností, navíc vytváří kopie sebe sama. Poslední varianta C vyhledá ty počítače, které již byly napadeny variantou A a upraví je na verzi B. V případě varianty A a B stačil na zneškodnění červa spolehlivý antivirový program, v případě varianty C jej bylo možné odstranit manuálně pomocí čtyř poměrně jednoduchých kroků, které dokázal dle zadaných instrukcí provést i běžný uživatel.



Obr. 1 - Oznámení o ukončení LSA Shell způsobené červem Sasser



Obr. 2 - Varovné okno oznamující restart systému zapříčiněný červem Sasser

1.3 Trojské koně

Trojský kůň (Trojan) je typ malwaru, který se tváří jako užitečný, nejčastěji jako hra, spořič obrazovky nebo jiný jednoduchý nástroj, ve skutečnosti ale obsahuje také škodlivý program - odtud pochází i jeho název z důvodu analogie se známou řeckou pověstí. Trojské koně mají často nejhorší projevy a mohou způsobit značné škody v systému či úplně zničit data na pevném disku. Narozdíl od virů není trojský kůň schopný sám sebe replikovat nebo infikovat jiné soubory. Nejčastěji se vyskytuje v podobě spustitelného EXE souboru, který obsahuje tělo trojského koně. Trojské koně využívají skutečnosti, že řada programů, včetně systémového prohlížeče souborů, skrývá přípony souborů. V takovém případě stačí připsat k názvu souboru požadovanou příponu a ten se pak jeví jako obrázek, spořič obrazovky, komprimovaný soubor atd. Záleží pouze na tom, za jaký typ souboru jej chce autor vydávat. Z těchto faktů plyne, že jediným možným způsobem, jak může být počítač napaden, je zavinění uživatele, který inkriminovaný soubor sám spustí a nevědomky tak umožní činnost trojského koně. Ale ne každý trojský kůň se vyskytuje v podobě spustitelného souboru. Někteří z nich jsou šířené pomocí červů, který dotyčného koně do napadeného počítače nainstaluje, popřípadně je trojský kůň součástí běžného, volně dostupného programu.

1.3.1 Činnost trojských koní

Typů trojských koní existuje mnoho a liší se nejen činností, kterou v napadeném počítači provádí, ale i mírou škodlivosti. Mezi nejčastější formy tohoto škodlivého softwaru patří:

- Sniffer - program, který dokáže sledovat a logovat provoz na digitální síti nebo části sítě. Sniffer zachytí každý paket putující datovým tokem v síti a podle potřeby je schopný dekódovat data v něm uložená a zobrazit jednotlivé hodnoty. Z těchto dat může získat přístupová jména a hesla uživatele, čísla kreditních akret apod.
- Keylogger - software, který sleduje a ukládá jednotlivé znaky zadané z klávesnice. Tyto poté odesílá na dané e-mailové adresy patřící nejčastěji autorům keyloggerů. Ti tak mohou získat velice citlivé údaje, jako jsou přistupová hesla apod.
- Spyware - tento druh malwaru shromažďuje bez vědomí uživatele různé informace o jeho činnosti a odesílá jej na předem zadané místo v Internetu, kde jsou tyto informace zpracovávány. Mezi tyto informace patří nejčastěji návyky uživatele při surfování Internetem, historie navštívených webových stránek, obsah stažených souborů, charakter vědomě otevřených reklam atd. Mnoho spyware aplikací zobrazuje reklamu, ať už v podobě pop-up oken nebo pozměněné domovské stránky webového prohlížeče. Spyware je často šířen společně s jiným programem, nejčastěji freee nebo shareware, jehož autoři o této skutečnosti často vědí. Problém spyware spočívá v tom, že nikdo není schopný zaručit, aby tato metoda shromažďování dat nebyla nikým zneužita. Navíc se již obejvily případy, kdy byla pomocí spywaru odcizena přístupová hesla či bankovní informace. Jiné zaznamenaná případy popisují přesměrování vytáčeného připojení na několikanásobně dražší telefonní linku. Proto je spyware uživateli považován za nežádoucí a jsou vyvíjeny programy, tzv. antispyware, které slouží k jeho detekování a odstranění. Běžné antiviry totiž často nejsou schopny spyware v počítači zjistit. Bohužel existují i falešné antispyware programy, které však ve skutečnosti spyware neodstraňují, ale naopak jej šíří. Mezi takové patří například AntiVirus 360, Spysheriff, UltimateCleaner a další.
- Backdoor („zadní vrátka) - speciální typ trojského koně obsahujícího síťovou službu, která umožňuje útočníkovi skrytý neautorizovaný přístup k systému

napadeného počítače. Ve své podstatě se jedná o aplikaci typu klient-server pro vzdálenou správu počítače. Ačkoliv tato správa nemusí být škodlivého charakteru, řadíme backdoor mezi malware. Klientská část je reprezentována útočníkem a serverová část napadeným počítačem. Klient vysílá požadavky na server a ten je plní, případně odesílá požadovaná data zpět klientovi. Backdoory se často šíří společně s viry a v takovém případě je útočník schopen získat celou síť počítačů, pomocí kterých může dále rozesílat spam, provádět útoky typu DDoS nebo další škodlivou činnost. Některé backdoory využívají IRC sítě ke komunikaci s útočníkem, kdy se zkouší připojit na určený kanál. Zde vystupuje jako bot budící dojem skutečného chatujícího uživatele. Útočník tak má pohromadě všechny napadené stanice a po zalogování se může ovládat kteroukoliv z nich.

1.3.2 Příklady trojských koní

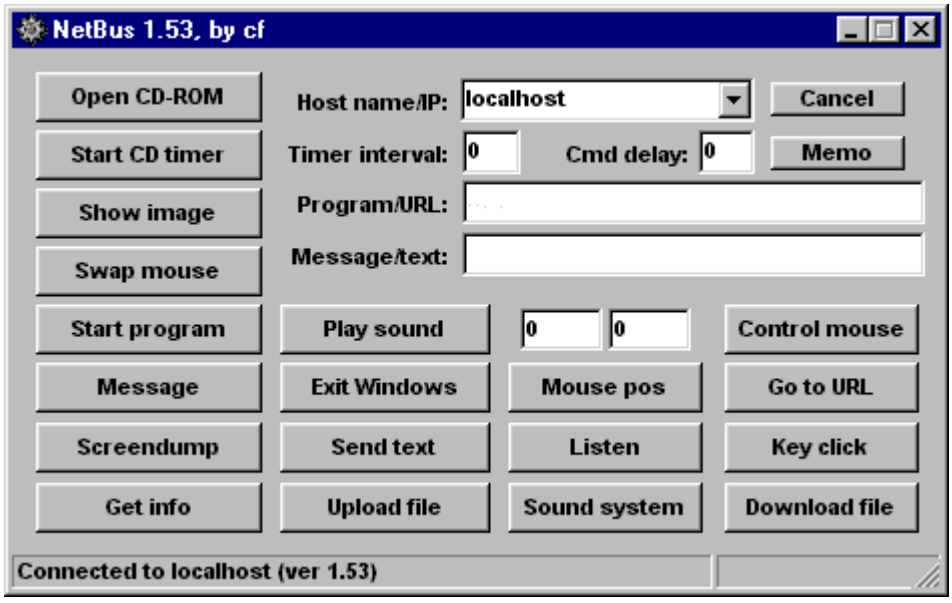
Za dobu své existence vzniklo již mnoho zástupců tohoto zákeřného typu softwaru. Zde jsou uvedeny ty, které se v počítačovém světě proslavily nejvíce.

NetBus

Dílo švédského programátora vzniklo v roce 1998 a veřejností bylo považováno za velice kontroverzní pro svůj nebezpečný potenciál spočívající v možném zneužití jako backdoor aplikace. Autor tvrdil, že byl program vytvořen pouze pro žertovné účely, ne jako nástroj pro ilegální infiltraci počítačů. Avšak v roce 1999 byl program použit k vložení obrázků s dětskou pornografií do počítače jednoho ze zaměstnanců švédské univerzity, což zapříčinilo jeho obvinění a propuštění z univerzity. Následné zveřejnění jeho identity bylo důvodem jeho odchodu ze země a nutností vyhledat lékařskou pomoc při vyrovnávání se se stresem. Program byl navržen pro systémy MS Windows 95, 98, ME a NT 4.0, pozdější verze programu podporovala i systémy MS Windows 2000 a XP.

Program se skládal ze dvou komponent - klientské a serverové části. Serverovou část tvořil EXE soubor o velikosti cca 500 KB. Název a ikona souboru se lišily v závisloti na verzi. Běžná jména byla „Patch.exe“ nebo „SysEdit.exe“. Po spuštění se program

nainstaloval do počítače a upravil registry systému Windows tak, aby se automaticky spouštěl při každém startu systému. Server byl proces typu démon, což je označení pro program, který dlouhodobě běží na pozadí a vyčkává v nečinnosti na určitou událost, kterou posléze obslouží. Tím zajišťuje různé úkony bez nutnosti interakce s uživatelem. Klientskou část tvořil samostatný program s grafickém prostředím, který umožňoval útočníkovi provádět v napadeném počítači množství činností. Okno programu s nabídkou činností je znázorněno na Obr. 3. Možnosti programu spočívaly jak v neškodných operacích, tak v potenciálně škodlivých. Mezi ty bezpečné, spíše až žertovné, patřilo například otevření CD mechaniky, zobrazení určitého obrázku na monitoru, prohození tlačítek myši, zobrazení varovného/informačního okna s libovolnou zprávou nebo vytípnutí obrazovky napadeného počítače. K těm více nebezpečným patřila možnost nahrát do napadeného počítače libovolný soubor nebo naopak libovolný soubor stáhnout. Také možnost restartovat systém mohla být škodlivá, zejména pokud uživatel pracoval s důležitými daty, o které při ukončení systému přišel.



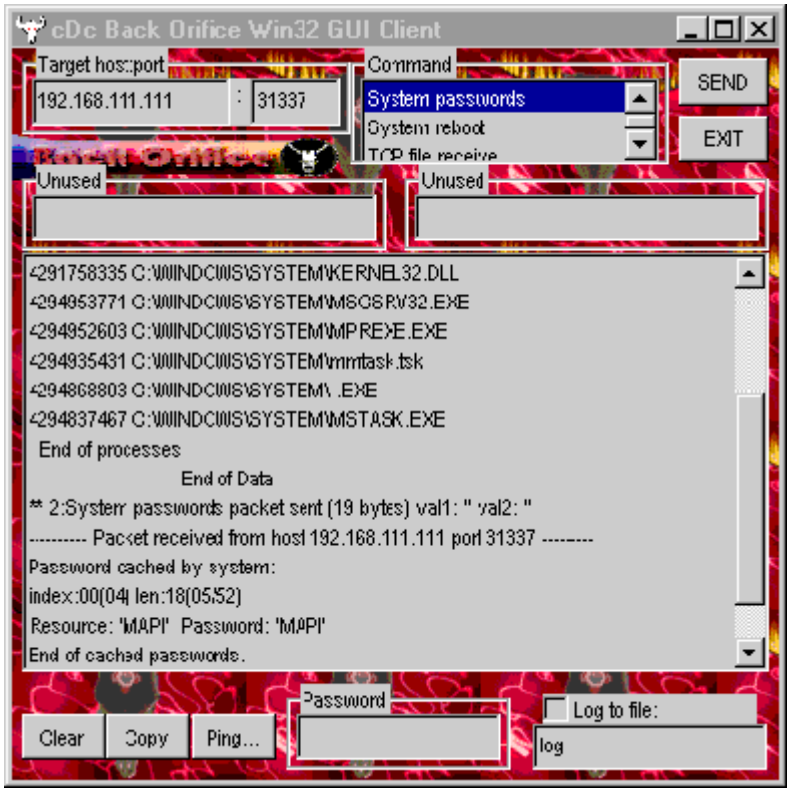
Obr. 3 - Program NetBus 1.53 s nabídkou možných činností

Odstranit NetBus, respektive jeho serverovou část, bylo možné ukončením procesu ve správci úloh systému a následným vymazáním příslušného záznamu v registru systému Windows. Konkrétně se jednalo o položku „NBSrv.exe“ (případně jí podobnou) v adresáři HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Druhou možností bylo použití solidního antivirového programu nebo speciálního nástroje vytvořeného k odstranění této aplikace.

Back Orifice

Tento program se poprvé objevil roku 1998 na každoroční mezinárodní hackerské konferenci DEFCON. Autorem programu je Josh Buchbinder aka Sir Dystic, bývalý člen skupiny „Cult of the dead cow“. Back Orifice běží pod systémy MS Windows 95 a 98 a je velice podobný programu NetBus co se prováděných činností týče. Jeho ovládání nebylo tak pohodlné jako u NetBusu, přesto s ním dokázal manipulovat i méně zkušený uživatel. Funkce programu byly podobné těm u NetBusu. Útočník mohl restartovat systém napadeného počítače, vypsat seznam přístupových hesel, mapovat porty, přidat nebo odebrat sdílení souborů, spustit nebo ukončit libovolný proces, upravovat registr systému, přehrát zvukový soubor, zachytit video z obrazovky a v neposlední řadě jakkoli manipulovat se soubory na lokálním disku napadeného počítače. Ačkoliv byl program Back Orifice vytvořen pro legitimní účely jako je vzdálená správa počítače, antivirové společnosti jej okamžitě kategorizovaly jako malware a přidaly na seznam souborů patřících do karantény. Grafické prostředí klienta programu Back Orifice je znázorněno na Obr. 4. Odstranit program bylo možné dvěma způsoby. První možnost byla použít jednoduchý program BODetect, druhá možnost bylo odstranit jej manuálně. K tomu stačilo otevřít stejný adresář v editoru registrů jako u programu NetBus a smazat z něj záznam „bovwin32.exe“. Poté restartovat systém, otevřít příkazový řádek a spustit příkaz „del c:\windows\system\exe~1“.



Obr. 4 - Klient programu Back Orifice

2 OCHRANA PROTI MALWARU

Potřeba chránit svá data před jakýmkoliv útokem či nebezpečím zvenčí vedla k vytváření různých neutralizačních programů, které se později vyvinuly v antivirové a antispyware programy, personální firewally a utility čistící počítač od ostatních druhů malwaru.

Za prvního předchůdce antivirového softwaru můžeme považovat výtvor Berndta Fixe z roku 1987, který dokázal zneškodit virus Vienna. O rok později vytvořil Briton Alan Solomon první antivirový software nazvaný Solomon's Anti-Virus Toolkit. Roku 1990 již bylo na trhu devatenáct bezpečnostních programů, mezi kterými byl i Norton AntiVirus nebo McAfee Virus Scan. Od té doby se na trhu objevila řada bezpečnostního softwaru a ochrana proti malwaru se stala výnosnům byznysem.

2.1 Prevence

Nejjednodušším způsobem, jak se chránit proti nákaze nebezpečným softwarem, je prevence a zdravý rozum. Trochu jiná pravidla platí v případě, že je počítač připojen k nějaké LAN síti nebo Internetu, a jiná platí, je-li naopak od okolí izolován. Jestliže není počítač připojen k Internetu či lokální síti, je třeba si dávat pozor pouze na data obsažená na disketách a CD nebo DVD discích. Proto by měl každý uživatel dbát na to, z jakého zdroje dané médium pochází a do jaké míry mu může důvěřovat. Avšak přítomnost antivirového programu nebo osobního firewallu je v dnešní době nutností. Kromě toho by měl každý uživatel dodržovat následující preventivní opatření:

- Nepůjčovat si od ostatních diskety, CD nebo DVD bez kontroly obsahu
- Nevěřit všemu a neklikat na vše, co nás zaujme
- Pravidelně zálohovat data na pevném disku

- Pravidelně kontrolovat data na pevném disku, flash disku a jiných vyměnitelných médiích na přítomnost malwaru
- Udržovat svůj bezpečnostní software aktuální
- Pravidelně kontrolovat a instalovat důležité bezpečnostní aktualizace systému Windows
- Nepouštět ke svému počítači cizí osoby
- Pravidelně aktualizovat další, běžně používané produkty, jako je webový prohlížeč, IM klient nebo java a flash pluginy
- Chránit svůj systémový uživatelský účet heslem
- Nespouštět na počítači neznámé nebo podezřelé programy
- Nezavádět bezdůvodně systém z bootovací diskety

2.2 Antivirové systémy

Ochrana pomocí antivirového softwaru je v dnešní době tím nejčastějším způsobem ochrany před škodlivým kódem. Od roku 1988, kdy byl vytvořen první antivirový software, již vznikla velká řada více či méně spolehlivých antivirových programů. Také funkce, které jsou schopny vykonávat, se postupem času rozšířily od běžné detekce virů až po komplexní ochranu.

2.2.1 On-demand scan

Základní funkce antivirového programu. Jedná se o kontrolu počítače „na vyžádání“, tzn. kontrolu spuštěnou uživatelem. Zpravidla je možné kontrolovat celý počítač nebo zvolit konkrétní disk, adresář či soubor. Většina programů také umožňuje kontrolovat pouze běžící procesy, systémové soubory nebo operační paměť. Tento typ kontroly má své uplatnění zejména při dezinfekci již napadených počítačů. Zvláštní

skupinou jsou pak tzv. on-line scannery, které umožňují vyhledat viry bez nutnosti instalace jakéhokoliv softwaru. Takové scannery bývají zdarma k dispozici na webových stránkách výrobců. Příkladem může být ESET Online Scanner dostupný na stránce http://www.eset.com/cz/domacnosti/produkty/online-scanner/, který umožňuje rychle a efektivně zkontrolovat systém a odstranit všechny druhy počítačových hrozeb.

2.2.2 Rezidentní štít

Rezidentní štít neboli on-access scanner je v současnosti běžnou součástí všech antivirových systémů. Princip je následující - antivir je rezidentně zaveden do paměti počítače a v reálném čase kontroluje veškerou činnost, která v systému probíhá. Program například kontroluje zápis na disk, obsah souborů stažených z internetu, otevírané soubory nebo spouštěné rezidentní aplikace. Také automaticky kontroluje vyměnitelná média a disky vložené do počítače. Při detekování hrozby provede předem nadefinovanou činnost (přesun souboru do karantény, smazání souboru, pokus o vyléčení souboru) a zobrazí uživateli oznámení a proběhlé akci.

2.2.3 Antispyware

Dříve tvořily samostatnou skupinu softwaru, který dokázal detekovat, zablokovat a případně i odstranit spyware uložený v počítači. Dnes již tuto funkci obsahuje řada antivirů, příkladem mohou být produkty společnosti Symantec (Norton), Grisoft (AVG), Alwil (Avast!), ESET (NOD32) a jiné.

2.2.4 Personální firewall

Velmi důležitou funkcí současných antivirových systémů je i personální brána firewall. Tu je možné nakonfigurovat přesně podle požadavků konkrétního uživatele. Složitost konfigurace takového firewallu je u jednotlivých produktů odlišná. U některého softwaru stačí nastavit odpovídající, předem nadefinovaný profil a o zbytek se postará program automaticky. Jiný software zpravidla veškerou komunikaci blokuje a teprve v průběhu času si uživatel definuje bezpečnostní pravidla podle toho, zda-li chce daný

proces/program povolit, nebo zablokovat. V takovém případě je zapotřebí určitá úroveň znalostí uživatele, jinak hrozí nebezpečí, že umožní činnost nebezpečného programu, nebo naopak zablokuje zcela neškodný program.

2.2.5 Metody detekce

Techniky používané k odhalování přítomnosti škodlivého kódu se u jednotlivých antivirových programů liší, zpravidla je ale můžeme rozdělit do následujících čtyř skupin:

1. Virové databáze - na této metodě je založena většina současných antivirů. Program obsahuje databázi vzorků známých virů. Vzorky jsou tvořeny řetězci z těla virů vybraných charakteristických sekvencí. Při kontrole pak program porovnává soubory s těmito vzorky. To umožňuje rozpoznat napadený program ještě před tím, než jej začneme používat. Pro jeden virus je navíc používáno více různých sekvencí, čímž se zvyšuje šance na zachycení nové varianty viru a zároveň se snižuje pravděpodobnost falešného poplachu. Pro správnou funkci softwaru je ale nutné udržovat virovou databázi v aktuálním stavu. Tvůrci virů se však snaží být neustále napřed, a proto vytváří různé polymorfní a metamorfní viry. Tyto viry jsou schopné samy sebe šifrovat nebo jinak upravovat vlastní kód, čimž se maskují před rozpoznáním virovou databází.
2. Kontrola integrity - tato metoda spočívá v porovnávání aktuálního stavu důležitých programů s informacemi, které si o nich antivirový program uložil při jejich příchodu do systému nebo při své instalaci. Jestliže virus napadne počítač, změní obsah některého z kontrolovaných objektů a následně je detekován. Díky tomu je možné zachytit i ty viry, které ještě nejsou popsány a jejichž vzorek chybí ve virové databázi. Pro správnou funkci kontroly integrity je třeba uložit kontrolované objekty v době, kdy je systém prokazatelně čistý. Problém s touto metodou může nastat u spustitelných souborů, které si samy zapisují do svého těla určité údaje a modifikují tak svůj obsah. Další nevýhodou je fakt, že kontrola integrity nezjistí typ nalezeného viru, ale pouze detekuje změnu souboru. Proto je tato metoda využívána jako doplněk jiných technik detekce škodlivého kódu.
3. Heuristická analýza - při této metodě vytváří antivir jakýsi virtuální počítač, na kterém spustí testovaný soubor a zkoumá všechny neobvyklé činnosti, které

se program pokouší vykonat. To umožní programu simulovat, co se stane v případě spuštění podezřelého programu, přičemž je škodlivý kód zachován izolovaný od reálného stroje. Jestliže je po analýze prováděných příkazů zjištěn jeden či více případů virového chování, označí program daný soubor jako podezřelý a informuje uživatele. Nevýhodou této metody je větší pravděpodobnost falešných poplachů, jelikož i běžné programy mohou pro svoji činnost využívat sekvence typické pro škodlivé kódy. V dnešní době bývá heuristická analýza většinou součástí virových databází, samostatně se využívá minimálně.

4. Monitorovací program - obecně hlídá změny v nastavení systému, chrání jej před množením škodlivého kódu díky neustálé kontrole prováděných operací a blokuje případné nelegální akce. Mezi ty může patřit například zápis do chráněných souborů nebo změna tabulky vektorů přerušení. I v tomto případě ale může dojít k falešnému poplachu, neboť i neškodné aplikace mohou provádět tyto operace. Z toho vyplývá, že ke správné funkci monitorovacích programů je třeba nejen jejich správné nastavení, ale i určitá znalost uživatel. Ten musí totiž v případě detekce podezřelé akce posoudit, zda se jedná o falešný poplach, nebo činnost malwaru.

2.3 Srovnávací testy antivirů

Na trhu antivirových ochran se nacházíe velké množství tohoto softwaru a pro běžného uživatele může být výběr toho adekvátního docela složitý. Z tohoto důvodu existují nezávislé testy prováděné certifikovanými společnostmi, které pravidelně porovnávají jednotlivé produkty z různých hledisek. Díky těmto testům jsme schopni vybrat si kvalitní produkt, jenž přesně odpovídá našim požadavkům.

Jednou ze společností provádějících nezávislé srovnávací testy antivirových programů je rakouská nezisková organizace AV-Comparatives. Na jejich stránkách

http://av-comparatives.org/ jsou veřejnosti zdarma k dispozici výsledky testů známých antivirových programů. Hodnocení produktů se skládá z následujících testů:

- Detekční test udává poměr nalezeného malwaru k celkovému počtu malwaru za poslední měsíce.
- Retrospektivní test testuje produkty na nový neznámý malware a hodnotí tak jejich schopnost proaktivní detekce.
- Výkonostní test určuje dopad programu na výkon počítače.
- Dlouhodobý komplexní test programu posuzuje jeho schopnosti v „reálném světě“ ve výchozím nastavení.
- Čistící testy hodnotí schopnost programu odstranit malware. Pro tyto testy jsou využívány vzorky z napadených počítačů uživatelů.

Výsledky testů jsou rozdělené do několika kategorií. Nalezneme zde recenze produktů podle jejich výrobců, samostatné recenze, recenze balíků pro zabezpečení mobilních zařízení a samozřejmě souhrnné výsledky celoročních testů. Na základě nejlepších výsledků pak uděluje vítězným produktům ocenění. Tabulka na Obr. 5 znázorňuje výsledky celoročního testu za rok 2010. Nejvyšší možné dosažené hodnocení je ADV+, nejnižší pak šedě vyplněné pole. Šedé pole s popiskem N/A značí, že výrobce nechtěl být v tomto testu hodnocen a černé pole s tímtéž popisem značí, že se výrobce daného produktu tohoto testu nezúčastnil. Na adrese http://wwww.av-comparatives.org/images/stories/test/summary/summary2010.pdf se pak nachází kompletní výsledek tohoto souhrnného testu. Obsahuje stručný přehled jednotlivých kategorií testů a jejich vítěze, recenze všech produktů včetně popisu instalace a deinstalace, uživatelského prostředí a bonusových funkcí.

	On-Demand Test February 2010	**Retrospective Test** February 2010	**On-Demand Test** August 2010	**Retrospective Test** August 2010	**Performance Test** November 2010	**PUP-Test** November 2010	**Dynamic Test** August-November 2010
avast!	ADV+	ADV	ADV+	ADV	ADV+	ADV	ADV
AVG	ADV	ADV	ADV	N/A	ADV+	N/A	ADV
AVIRA	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+
BitDefender	ADV+	ADV+	ADV+	ADV+	STD	ADV+	ADV
eScan	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	*N/A*
ESET NOD32	ADV+	ADV+	ADV+	ADV+	ADV+	ADV	ADV
F-Secure	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+
G DATA	ADV+	ADV+	ADV+	ADV+	ADV	ADV+	ADV
K7	STD	ADV	STD	ADV	ADV+	ADV	*N/A*
Kaspersky	ADV+	ADV+	ADV	ADV	ADV	ADV	ADV+
Kingsoft				N/A	ADV+		
McAfee	ADV	STD	ADV	N/A	ADV+	ADV+	*N/A*
Microsoft	ADV	ADV+	ADV	ADV+	ADV+	STD	*N/A*
Norman		STD	STD	N/A	STD	STD	STD
Panda	ADV	ADV	ADV	ADV	ADV+	ADV+	ADV
PC Tools	ADV+	STD	ADV+	ADV	STD	ADV+	ADV
Sophos	ADV	ADV	ADV	ADV+	ADV+	N/A	*N/A*
Symantec	ADV+	ADV	ADV+	ADV+	ADV+	ADV+	ADV+
Trend Micro		STD		N/A	STD	ADV	ADV
TrustPort	ADV+	ADV+	ADV	ADV	ADV+	ADV+	*N/A*

Obr. 5 - Výsledky celoročního testu antivirových programů

Za loňský rok dosáhly nejlepšího možného hodnocení ve všech kategoriích tyto dva produkty:

- AVIRA Premium Security Suite
- F-Secure Internet Security

Celkovým vítězem se pak stal a titul „Produkt roku 2010“ získal software F-Secure Internet Security.

II. PRAKTICKÁ ČÁST

3 BEZPEČNOSTNÍ SOFTWARE

Pro řešení zabezpečení firemní sítě jsem z rozsáhlé nabídky bezpečnostního softwaru zvolil dva zástupce, kteří pravidelně dosahují jedněch z nejlepších výsledků ve srovnávacích testech prováděných společností AV-Comparatives. Jedná se o produkty Internet Security 2011 od společnosti F-Secure a Norton Internet Security 2011 od společnosti Symantec. Obě verze jsou volně stažitelné z webu výrobce a ve své 30-denní zkušební variantě jsou dostupné zdarma.

3.1 Symantec Norton Internet Security 2011

3.1.1 Instalace a popis programu

Program, respektive jeho 30-denní trial verze, je volně ke stažení na adrese http://cz.norton.com/downloads/trialsoftware/download.jsp?pvid=nis2011 a podporuje češtinu, což je velice vítané vzhledem k další práci s programem, nastavením apod. Instalace programu je velice snadná - je třeba zvolit pouze lokaci pro rozbalení instalačních souborů a poté už se program sám automaticky nainstaluje na systémový disk do adresáře Program Files\Norton Internet Security. Po dokončení instalace je třeba, jak už tomu u podobných programů bývá, restartovat systém. Po opětovném spuštění systému již program bez problémů běží a ikonka v pravém dolním rohu obrazovky (v systémové liště) symbolizuje jeho činnost (Obr. 6). Cena licence programu na 1 rok začíná na 1325 Kč včetně DPH.

Obr. 6 - Ikona oznamující činnost programu

Prostředí programu Norton Internet Security 2011 (dále jen NIS) je jednoduché a přehledné (Obr. 7). Okno se skládá ze dvou hlavních ovládacích částí:

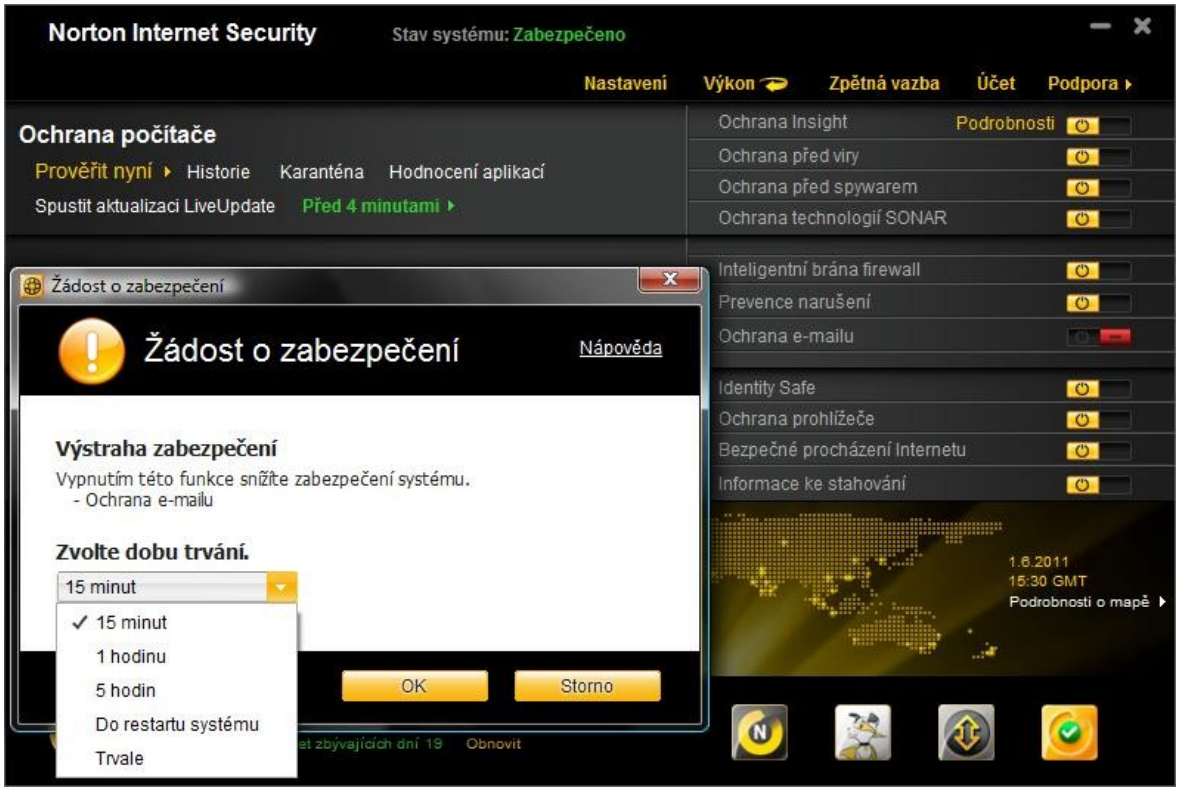
1. Horní ovládací panel
2. Hlavní okno s nabídkami

Obr. 7 - Prostředí programu Norton Internet Security 2011

V horním panelu se nachází tlačítka pro vstup do nastavení programu, přepnutí na okno moniturující výkon počítače/programu a historii akcí, které proběhly v počítači. Dále je zde odkaz na webové stránky produktu se zpětnou vazbou umožňující uživateli podělit se o své zkušenosti s programem, odkaz na uživatelský účet na webových stránkách a tlačítko Podpora obsahující nápovědu, informace o programu, možnost kontroly nové verze a další.

Hlavní nabídka je rozdělená do tří skupin. Každá skupina je určena jinému druhu ochrany a v její pravé části se nachází seznam služeb, které jsou pro tuto k dispozici.

Užitečná je i možnost vypnout/zapnout kteroukoliv ze služeb jedním kliknutím přímo z tohoto okna bez nutnosti zasahovat do nastavení programu. Po stisku tlačítka pro vypnutí služby vyskočí varovné okno, kde je možné nastavit dobu trvání, po kterou má být služba neaktivní (Obr. 8). Tato možnost se mi jeví jako velice užitečná, zejména pokud potřebujeme z jakéhokoliv důvodu dočasně deaktivovat některou ze služeb a nechceme zapomenout na její opětovné spuštění.



Obr. 8 - Okno upozorňující na deaktivaci služby

3.1.2 Nastavení programu

Možnost nastavení NIS je velice rozsáhlá a poskytuje tak uživateli širokou škálu bezpečnostních funkcí. Menu s nastavením se skládá z následujících záložek:

- Nastavení počítače
- Nastavení sítě
- Nastavení webu

- Různé možnosti nastavení
- Rodičovský zámek

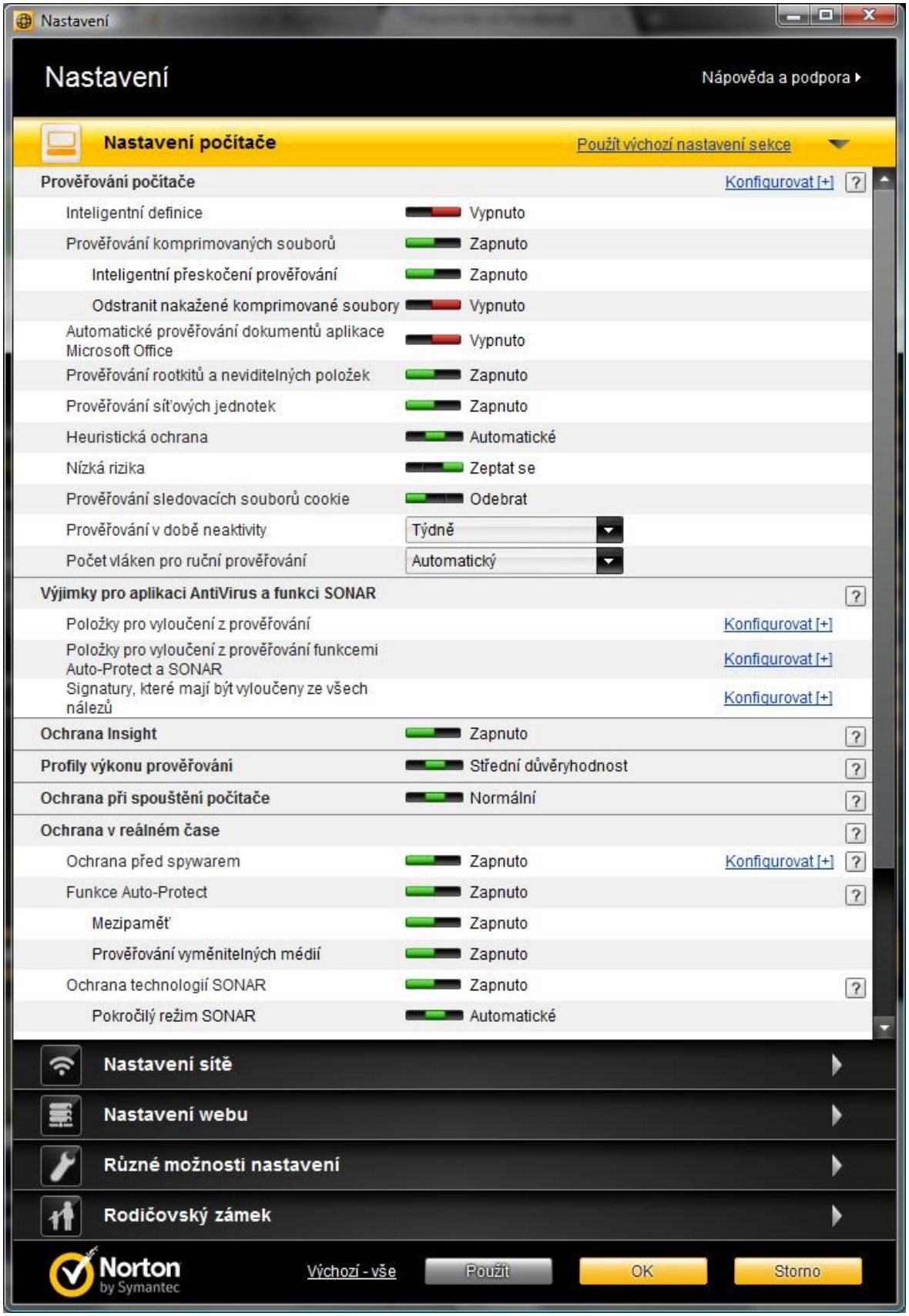
V první záložce nalezneme veškeré volby související s antivirovou ochranou počítače, na kterém se program nachází. Jedná se např. o hloubku skenování, zapnutí/vypnutí určitých podslužeb nebo nastavení automatických aktualizací. Přehled tohoto nastavení, které se mi jeví jako optimální, se nachází na Obr. 9.

Další záložka (Obr. 10) se zabývá nastavením sítě, do kterého patří napr. kontrola e-mailových zpráv a antispamová ochrana nebo brána firewall. Ta umožňuje spravovat pravidla pro jednotlivé síťové protokoly, chování programů při navazování síťového spojení a další.

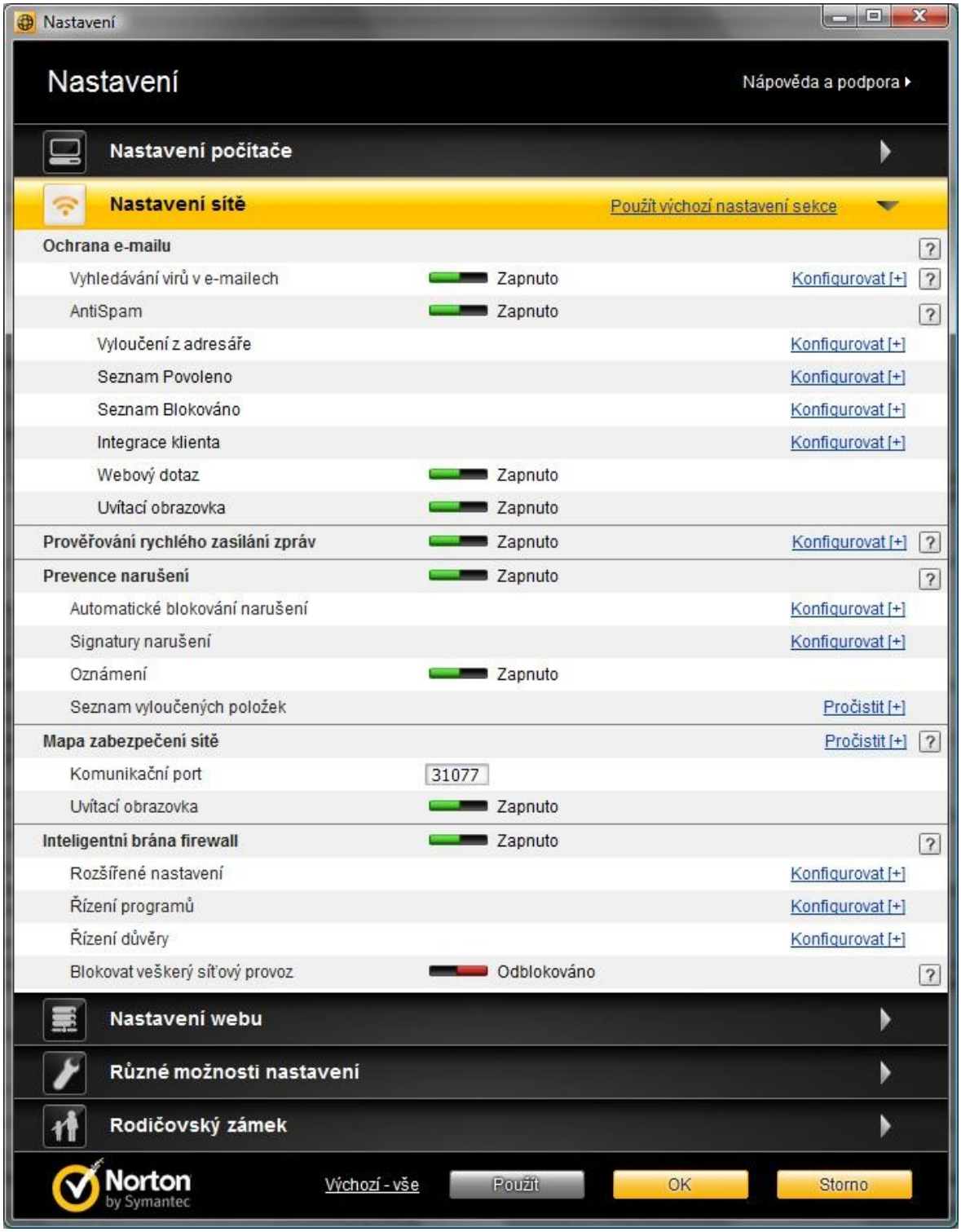
Třetí záložka (Obr. 11) obsahuje nastavení bezpečnosti týkající se internetového prohlížeče a procházení internetu obecně. Mezi takové služby patří kromě standardní ochrany internetového prohlížeče (bohužel pouze pro IE verze 6.0 nebo novější a Mozilla Firefox 3.0 nebo novější) i možnost využít aplikaci Identity Safe, která poskytuje úložiště pro citlivé informace, jako jsou přihlašovací informace uživatele, osobní informace, číslo účtu apod. Tyto údaje a veškerá nastavení aplikace Identity Safe jsou uchovány v místním profilu, který je dostupný pouze z uživatelského účtu systému Windows, ve kterém byly vytvořeny. Tato citlivá data lze také pomocí služby přenosných profilů uložit na externí jednotku a bezpečně s nimi pracovat na kterémkoliv počítači s nainstalovaným programem Norton Internet Security.

Předposlední záložka (Obr. 12) obsahuje různá další nastavení, jako je sledování výkonu počítače s možností úpozornění při vysokém zatížení, úsporu energie při napájení z baterie notebooku, zabezpečení samotného programu před nežádanou modifikací nebo nastavení tichého režimu, při kterém jsou dočasně vypnuty výstrahy a oznámení zobrazované v pravém dolním rohu obrazovky.

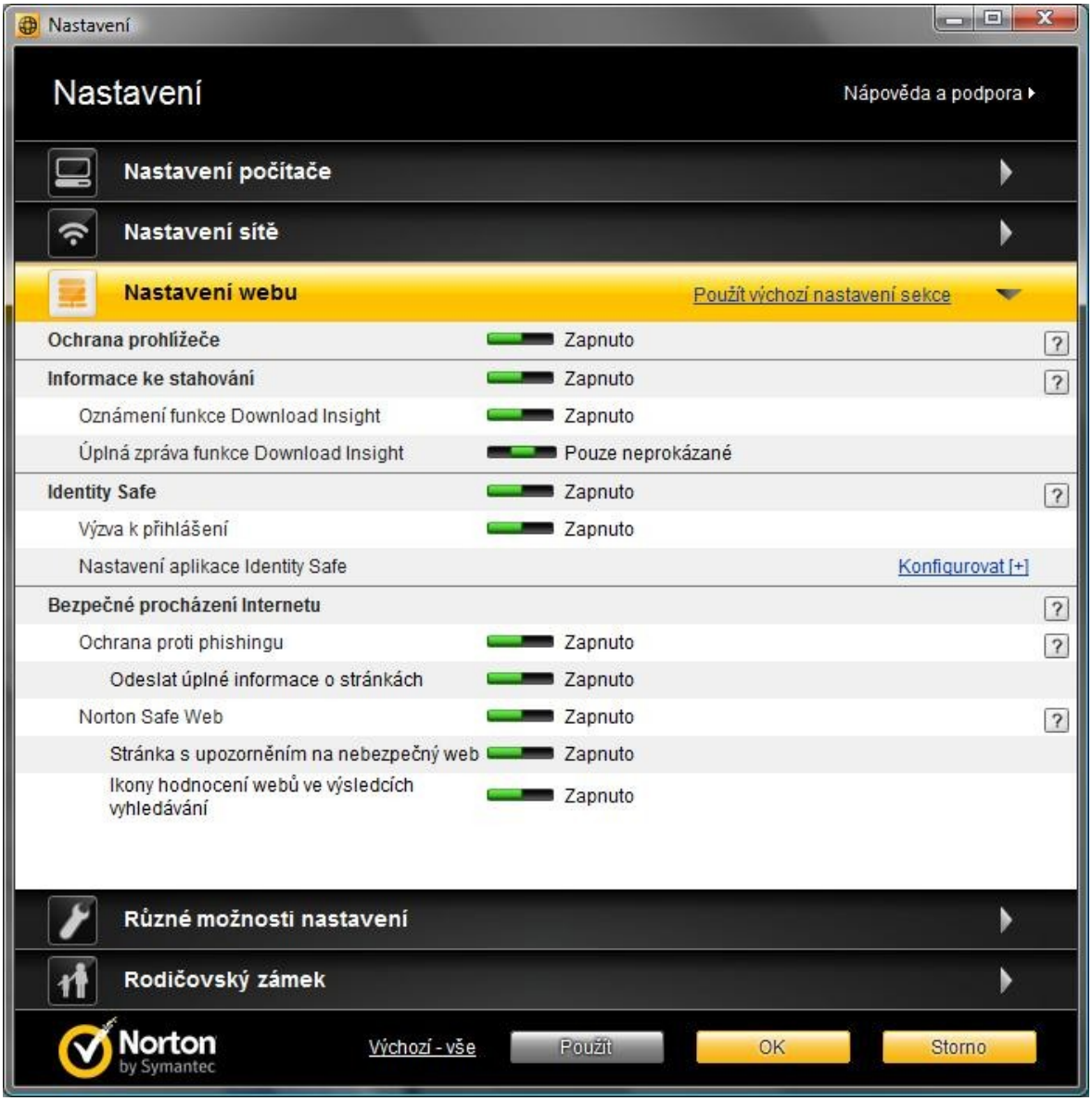
Poslední záložka obsahuje pouze nastavení rodičovského zámku, který chrání před nechtěnou změnou nastavení druhou osobou.



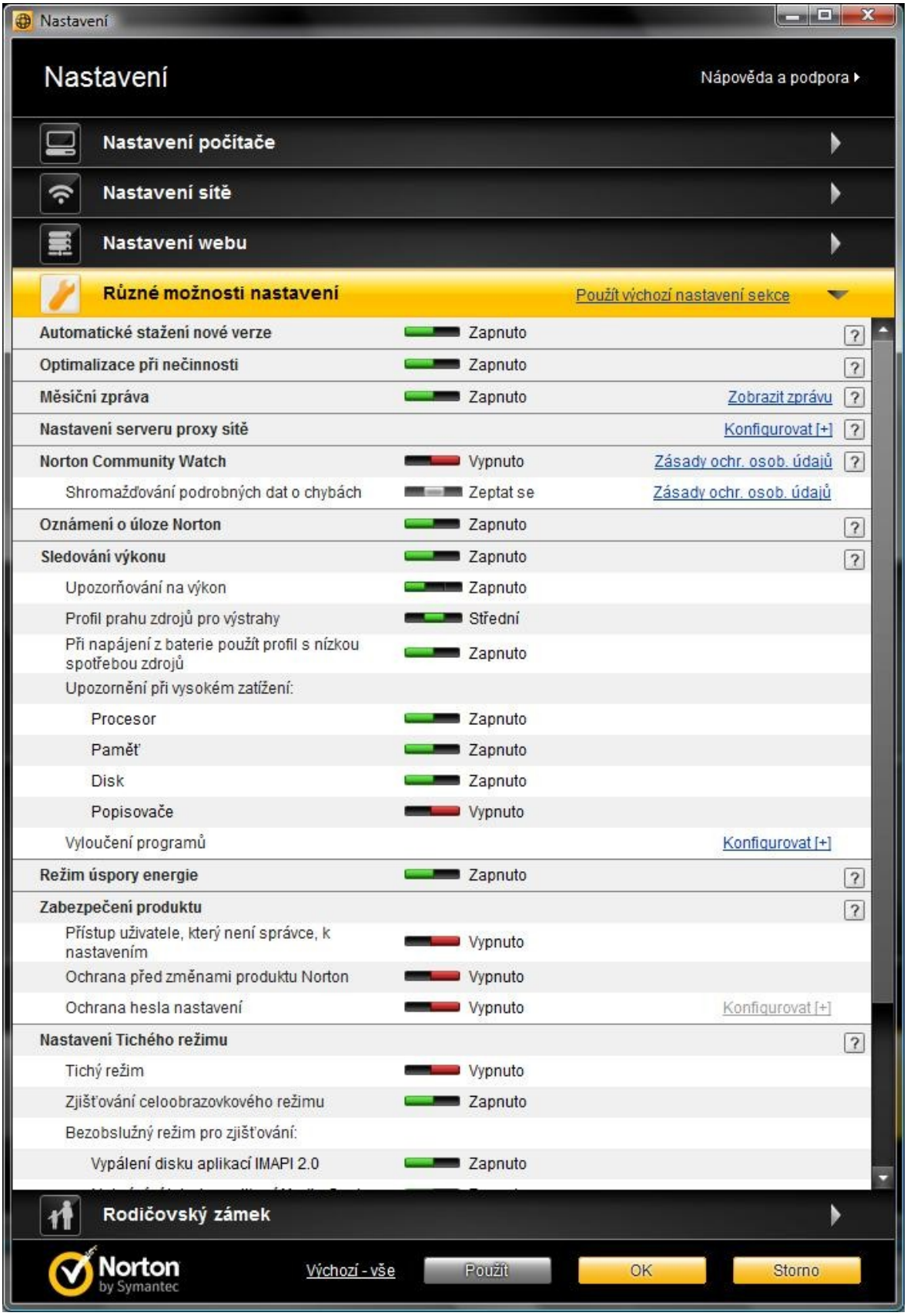
Obr. 9 - Nastavení zabezpečení počítače



Obr. 10 - Nastavení zabezpečení sítě



Obr. 11 - Nastavení bezpečnosti webu



Obr. 12 - Různé možnosti nastavení zabezpečení

Další velice užitečnou součástí NIS je nabídka Výkon nacházející se taktéž na horním ovládacím panelu. Tomuto oknu dominují dva grafy znázorněné na Obr. 13. První z nich monitoruje důležité činnosti prováděné v systému. Mezi tyto činnosti patří instalace programů, stažení souborů, detekce hrozeb, výstrahy výkonu, rychlé prověření systému a další. V tomtu grafu jsou uloženy události, které proběhly za poslední tři měsíce. U tohoto grafu je také možnost spuštění optimaliazce. Jedná se v podstatě o defragmentaci disku. Této funkci lze také nastavit automatické spuštění při nečinnosti systému. Druhý graf zobrazuje procentuální vytížení procesoru (s možností přepnutí na graf využití paměti) a samotného programu. U tohoto grafu lze přepínat rozsah časové osy od deseti minut po jeden měsíc.

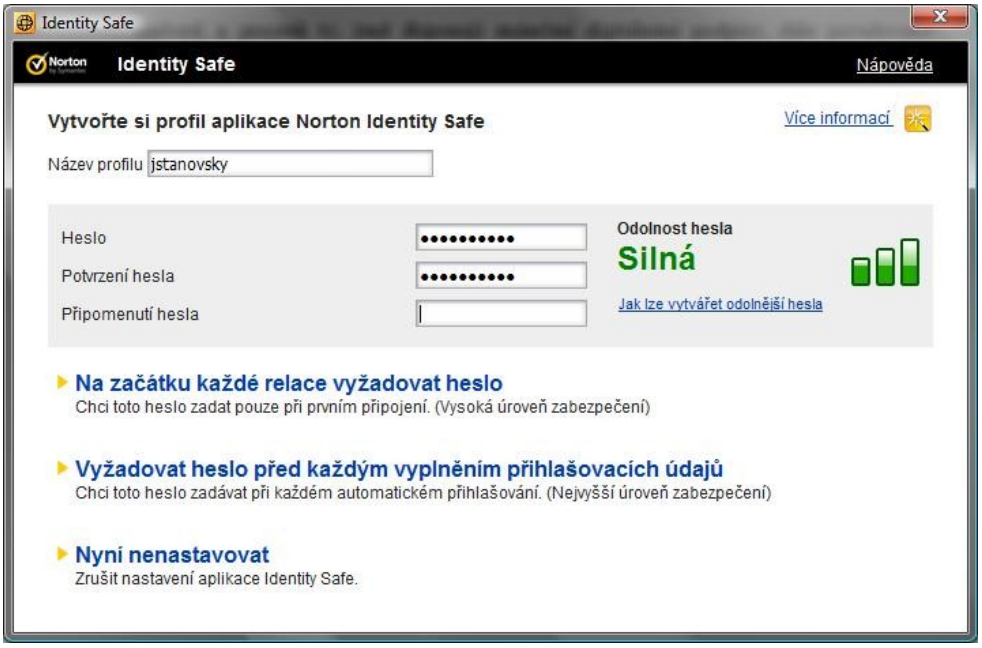
Obr. 13 - Okno „Výkon“ s grafy a probíhající optimalizací

Z tohoto okna lze dále otevřít přehled souborů a procesů v systému s jejich úrovní důvěryhodnosti. Ty soubory a aplikace, které dosahují požadované úrovně, není třeba při kontrole prověřovat, čímž se zvýší výkon počítače. Nechybí zde možnost tuto úroveň změnit podle požadavků uživatele na bezpečnost svého počítače. Já jsem, po prozkoumání

tohoto seznamu, zvolil střední důvěryhodnost, která vylučuje ze seznamu prověřovaných souborů a procesů ty, které byly uznány jako důvěryhodné komunitou Norton.

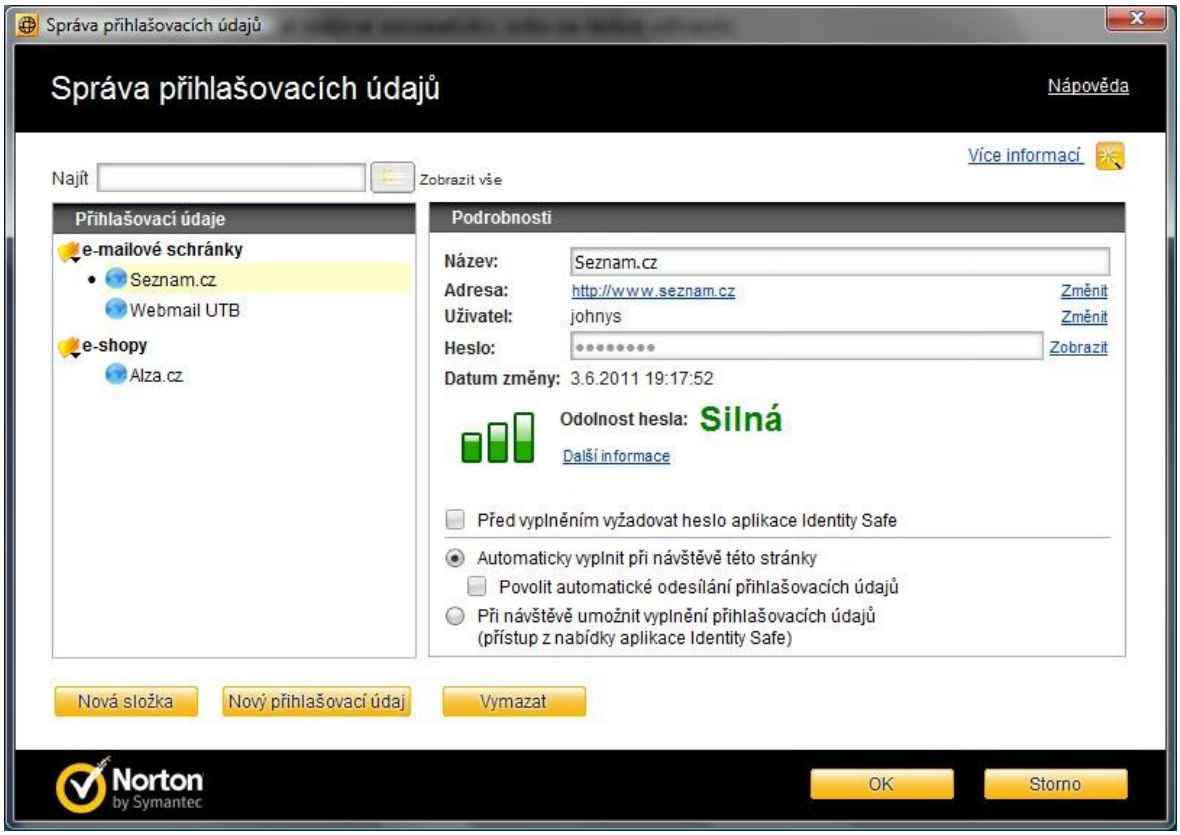
3.1.3 Identity Safe

Jak jsem již zmínil výše, funkce Identity Safe uchovává veškerá citlivá data uživatele jako jsou přihlašovací údaje, adresa, datum narození, číslo platební karty a hesla a mimo to také vyplňuje formuláře na důvěryhodných serverech. Tato funkce se spouští z hlavního okna programu. Nejprve nás program vyzve k založení nového profilu. Po potvrzení se objeví okno (Obr. 14), kam zadáme název profilu a heslo. Grafické znázornění odolnosti daného hesla nám pomůže zvolit takové, které je dostatečně odolné. Já jsem, dle doporučení v nápovědě pro tvorbu silných hesel, zvolil odpovídající kombinaci velkých a malých písmen, speciálních znaků a číslic. Poslední kolonka slouží k zadání pomocné věty nebo fráze v případě zapomenutí hesla. Nakonec jsem zvolil požadavek na zadání tohoto hesla pouze na začátku relace. Úroveň zabezpečení zůstane vysoká a odpadne tím neustálé vyplňování hesla před každým přihlášením na serveru.



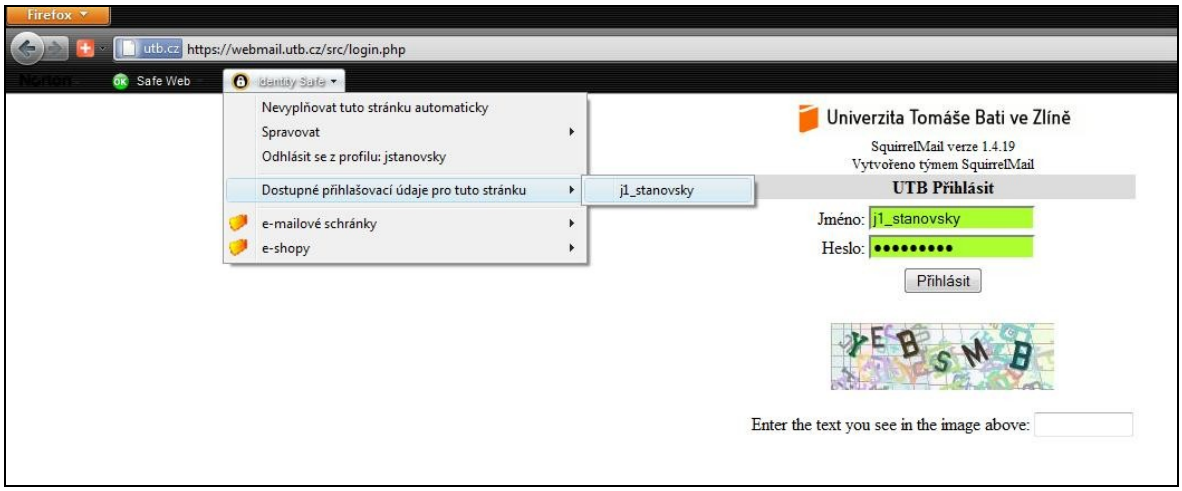
Obr. 14 - Okno pro zadání základních údajů profilu Identity Safe

Následuje okno, kde si můžeme zvolit, jestli chceme importovat přihlašovací údaje uložené v aplikaci Internet Explorer. Další okno již obsahuje samotnou správu přihlašovacích údajů. Zde je možné vytvořit záznamy pro jednotlivé webové stránky a také je rozčlenit pomocí složek do přehledných skupin. Každý záznam obsahuje WWW adresu stránky, login uživatele a heslo. Na výběr je způsob zadávání přihlašovacích údajů, tzn. mají-li se zadávat automaticky, nebo na žádost uživatele. Bohužel, tato služba není dostupná pro jiné prohlížeče než Internet Explorer a Mozilla Firefox. Okno s vytvořenými záznamy je znázorněno na Obr. 15.



Obr. 15 - Okno pro správu přihlašovacích údajů služby Identity Safe

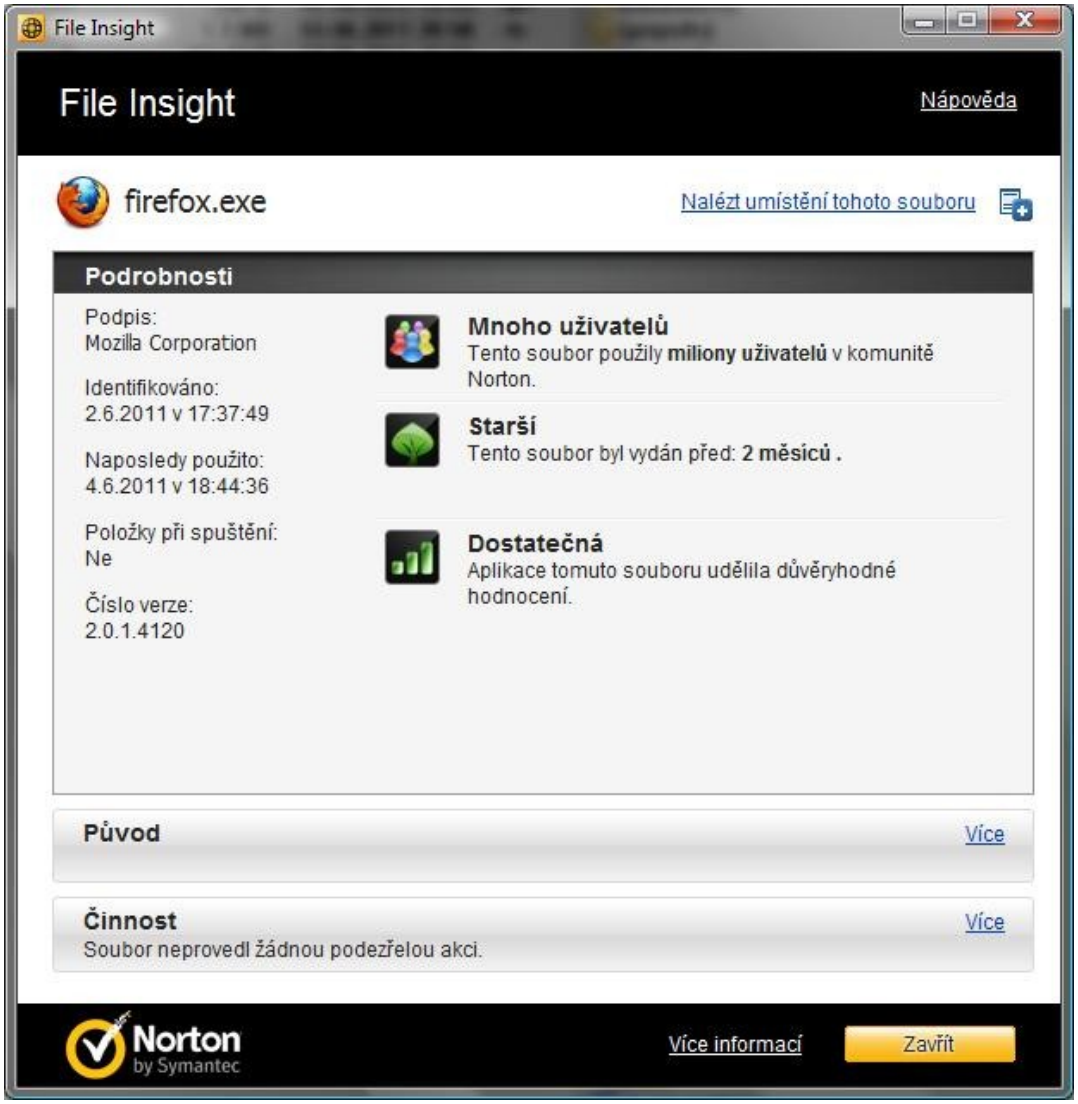
Funkce Identity Safe je do internetového prohlížeče (testováno pouze pro software Mozilla Firefox 4.0.1) implementována v podobě tlačítka na nástrojové liště. Po kliknutí se objeví klasické drop down menu, které nabízí správu celého systému, přihlášení uživatele na základě uložených údajů a také přechod na kteroukoliv jinou stránku v databázi Identity Safe. Tato nabídka se je vyobrazena níže na Obr. 16.



Obr. 16 - Přihlašovací stránka s vyplněnými údaji e-mailové schránky UTB ve Zlíně

3.1.4 File Insight

Funkce File Insight je užitečná utilita umožňující otestovat důvěryhodnost kteréhokoliv spustitelného souboru v počítači. Tato služba je integrovaná do kontextového menu systému Windows, ale funguje i jako real-time ochrana nově stažených souborů. Po kliknutí pravým tlačítkem myši na soubor v počítači stačí vybrat položku „Norton File Insight“. Okno, které se objeví, obsahuje tři záložky - „Podrobnosti“, „Původ“ a „Činnost“. První z nich nám říká, kolik uživatelů z komunity Norton již tento soubor použilo, jak je soubor starý a samozřejmě obsahuje informaci o důvěryhodnosti tohoto souboru (Obr. 17). Záložka „Původ“ informuje o původu souboru, respektive jeho zdrojovém souboru a poslední záložka „Činnost“ ukazuje, jak daný soubor využíval procesor a paměť a případně jaká akce byla se souborem provedena.



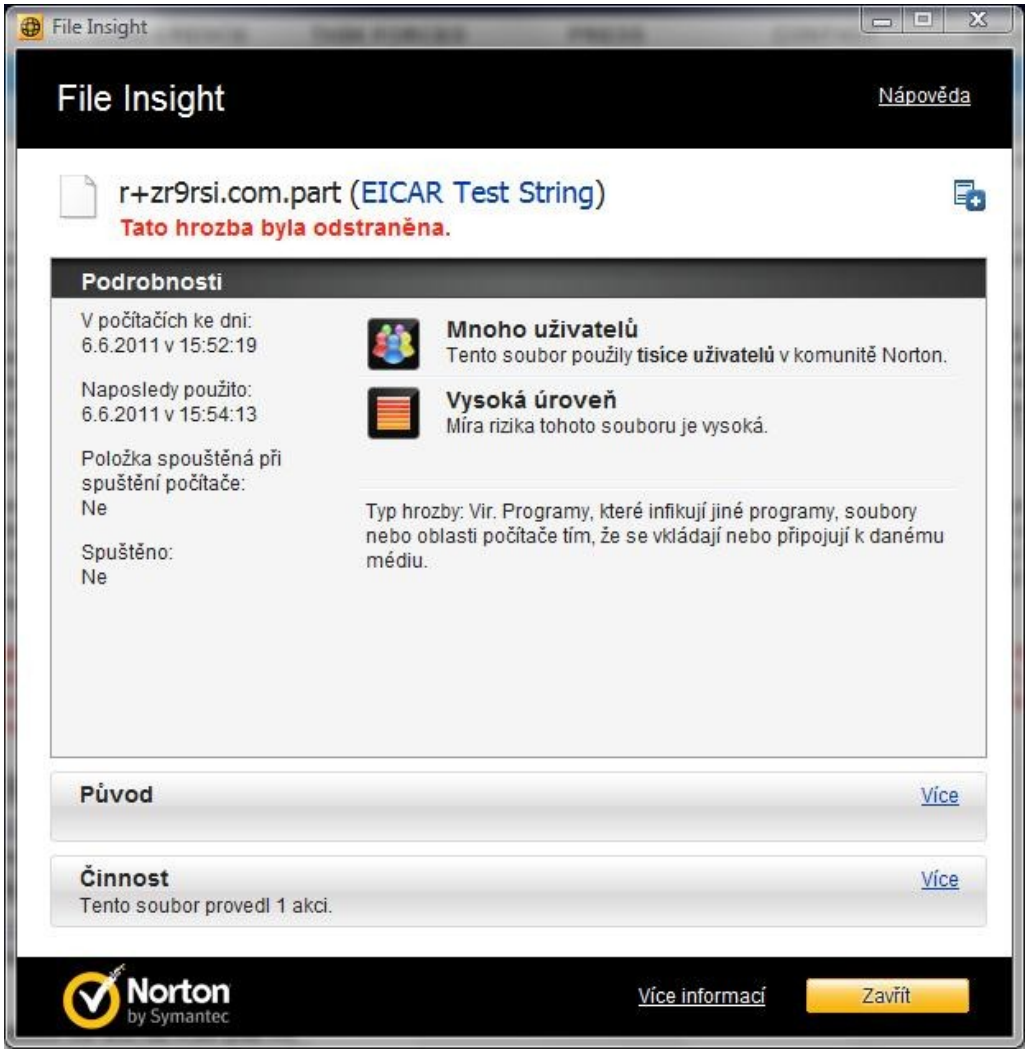
Obr. 17 - Inspekce souboru pomocí funkce File Insight

3.1.5 Testy bezpečnosti

Pro otestování správné funkce NIS jsem využil testovacích souborů na stránkách Evropského institutu pro výzkum počítačových antivirů (EICAR) http://eicar.org. Zde se nachází několik typů testovacích souborů jak pro standardní protokol HTTP, tak pro jeho zabezpečenou verzi HTTPS. Při pokusu o otevření/uložení souboru „eicar.com“ se objevilo v rohu obrazovky upozornění (Obr. 18), následné rozkliknutí podrobností odhalilo hrozbu (Obr. 19). Totéž platilo i pro zabezpečený protokol HTTPS.

Obr. 18 - Upozornění

na hrozbu



Obr. 19 - Podrobnosti o „infikovaném“ souboru

Uložení komprimovaných souborů eicar.com.zip a eicarcom2.zip (dvakrát komprimovaný) NIS povolil, jejich následné otevření ovšem dokázal zablokovat (Obr. 20), opět pro oba protokoly.

Obr. 20 - Info o zablokovaném pokusu o otevření souboru

Jediný soubor, jehož uložení ani otevření nedokázal NIS zabránit, byl textový soubor eicar.com.txt obsahující krátký textový řetězec simulující nežádoucí kód. Avšak při mnou spuštěné kontrole byl již soubor správně identifikován a odstraněn.

Další testy jsem provedl na stránce http://test.bezpecnosti.cz/. Zde jsou k dipozici testy založené na analýze otevřených portů síťového rozhraní počítače nebo firewallu. První test byl založen na analýze nejrozšířenějších síťových služeb jako je FTP, WWW, POP3 a další. Výsledek tohoto testu dopadl uspokojivě - ani jedna ze služeb nebyla vyhodnocena jako napadnutelná. Podrobný výpis se nachází na Obr. 21. Druhý test byl zaměřen na trojské koně, respektive byly testovány porty, které jsou nejčastěji tímto druhem malwaru využívány. Výsledek byl i v tomto případě negativní - všech 30 testovaných portů bylo vyhodnoceno jako zabezpečených.

Poslední ze série testů provedených na NIS byl tzv. leak test (leak = angl. trhlina). Jedná se o testování schopnosti firewallu zamezit nežádané odchozí komunikaci. Program se pokouší spojit s webovým serverem, odeslat textový řetězec a simulovat tak například odcizení citlivých údajů. Podaří-li se mu data odeslat, nefunguje firewall správně. Pro otestování funkčnosti jsem použil jednoduchý program PCFlank Leaktest 1.0 stažený z webových stránek http://www.pcflank.com/. Po spuštění se objeví obrazovka s informacemi o principu testu. Na další obrazovce nás program vyzve ke spuštění prohlížeče Internet Explorer. Jakmile je prohlížeč spuštěn, objeví se další obrazovka

s informacemi a textovým polem. Do něj vepíšeme libovolný textový řetězec a potvrdíme. V tomtu testu bohužel, jak je možné vidět na Obr. 22, NIS selhal, jelikož nedokázal zachytit pokus o odchozí komunikaci a umožnil odeslat data na server.

Port	Služba	Bezpečnostní význam	Stav
21	FTP	Veřejný FTP server. Slouží ke kopírování dat. Hackeři jej často používají ke stahování dat a zakódovaných databází hesel.	Zabezpečeno nebo vypnuto
23	Telnet	Nekódované terminálové spojení --- dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokoušet připojit k serveru...	Zabezpečeno nebo vypnuto
25	SMTP pošta	Služba pro příjem pošty. Pokud je špatně nastavena, umožní z vašeho počítače jednoduše udělat zdroj spamů (nevyžádaných e-mailů). Pokud máte poštovní server bez posledních aktualizací, je zde možnost i server ovládnout!	Zabezpečeno nebo vypnuto
80	WWW server	Na vašem počítači, popř. serveru, běží veřejný internetový server. Vaše linka do Internetu je sdílena s uživateli vašich stránek. Pokud není webový server dobře nastaven a aktualizován, lze jej napadnout. Je to hackery nejvíc napadaná služba.	Zabezpečeno nebo vypnuto
110	POP3 pošta	Služba pro stahování pošty. Lze odposlouchávat nebo provést slovníkový útok nebo útok brutální silou, v případě úspěchu má útočník přístup k vaší poště. V případě, že váš účet slouží i ke vzdálenému přístupu k firemní síti, jde o velký bezpečnostní incident.	Zabezpečeno nebo vypnuto
135	RPC Microsoft	Služba Microsoftu pro volání vzdálených procedur. Hackeři přes ni dokážou například zablokovat počítač.	Zabezpečeno nebo vypnuto
137	NetBIOS Name	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	Zabezpečeno nebo vypnuto
139	NetBIOS Sesion	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	Zabezpečeno nebo vypnuto
143	IMAP Pošta	Služba poštovního serveru. Popis viz POP3.	Zabezpečeno nebo vypnuto
161	SNMP	Protokol SNMP (Simple Network Management Protocol) --- řízení síťových prvků. Může to být také služba běžící pod Windows. Útočník může získat z registru Windows neocenitelné informace, které může dál použít k následným útokům.	Zabezpečeno nebo vypnuto
443	HTTPS WWW	Kódovaný veřejný WWW server. Je lepší než obyčejný WWW server, nejde odposlouchávat. Může být stále napadnutelný špatnou konfigurací nebo bezpečnostními dírami (Musí se aktualizovat!).	Zabezpečeno nebo vypnuto
445	WIN NT/2000 SMB	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem nebo získat vaše hesla.	Zabezpečeno nebo vypnuto
1080	SOCKS	Proxy služba, slouží pro přístup z vnitřní sítě na Internet, přístupná z vnější strany, umožnuje hackerům vydávat se za vás.	Zabezpečeno nebo vypnuto
1494	Citrix	Služba používaná pro vzdálené ovládání plochy aplikačního serveru.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	Zabezpečeno nebo vypnuto
1723	PPTP tunel	Vzdálený přístup do podnikové sítě z domácího PC nebo např. laptopu obchodníka, prostřednictvím VPN. Pokud je služba povolena z jakékoli IP adresy, muže provést útočník útok brutální silou nebo slovníkový útok a tím se dostat do firemní sítě.	Zabezpečeno nebo vypnuto
3389	Vzdálená plocha	Služba pro připojení se k serveru nebo stanici prostřednictvím grafického terminálu. Přes tuto službu je možno pracovat s PC, jako by u něj někdo seděl osobně.	Zabezpečeno nebo vypnuto
5900	VNC server	Služby používaná pro vzdálené ovládání plochy PC. Spojení je nešifrované, lze odposlochávat --- velmi nebezpečné !	Zabezpečeno nebo vypnuto
5000	UPnP	Služba pro komunikaci s UPnP (Universal Plug and Play) zařízeními připojenými do vaší sítě	Zabezpečeno nebo vypnuto
5631	PC Anywhere	Služby používaná pro vzdálené ovládání plochy PC.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	Zabezpečeno nebo vypnuto

Obr. 21 - Kompletní výsledek testu na základní síťové služby

Obr. 22 - Neúspěšný výsledek testu firewallu v zablokování odchozí komunikace

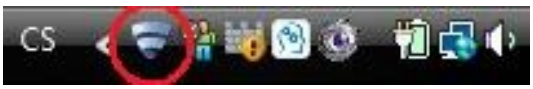
3.2 F-Secure Internet Security 2011

3.2.1 Instalace a popis programu

Podobně jako předchozí je i tento software ve své zkušební verzi dostupný z webových stránek https://my.f-secure.com/en/home/-/subscribe/GLOBAL/FCI1/trial. Pro stažení je třeba vyplnit jméno, příjmení a e-mailovou adresu. Po spuštění instalace nás průvodce vyzve k volbě jazyka (včetně češtiny) a přijmutí licenční smlouvy. Po odsouhlasení můžeme zadat registrační klíč, v mém případě jsem ponechal pole nevyplněné a aktivoval tak zmíněnou zkušební verzi. V následujícím okně máme na výběr dvě služby:

- 30 dní produktu F-Secure Internet Security 2011
- 30 dní produktu F-Secure Anti-Virus 2011

Zvolil jsem tedy první z možností, dále vybral podrobný postup instalace a úplnou instalaci bez rodičovské kontroly, která je v tomto případě zbytečná. Po výběru instalační složky se produkt nainstaluje a automaticky vyhledá dostupné aktualizace (Obr. 23). Po dokončení instalace se objeví v liště ikona programu (Obr. 24). Cena licence programu na 1 rok začíná na 1023 Kč (při kurzu 25 Kč za 1 €) včetně DPH.



Obr. 23 - Ikona programu F-Secure Internet Security 2011

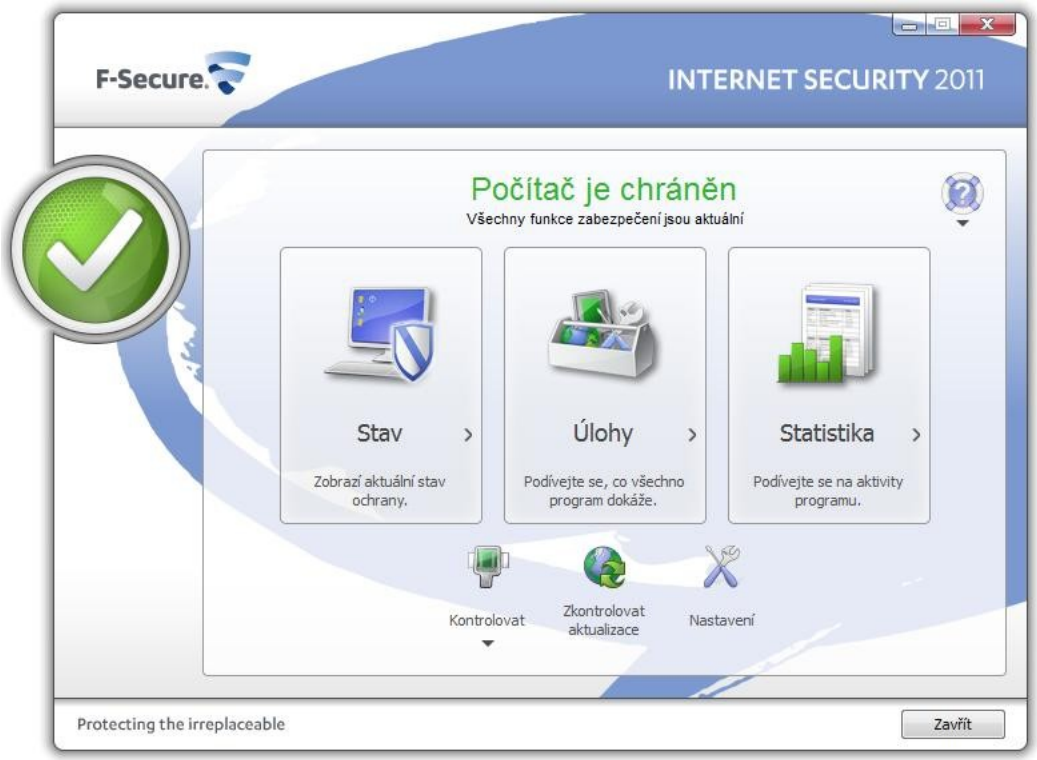
Obr. 24 - Aktualizace programu F-Secure Internet Security 2011

Prostředí programu (znázorněno na Obr. 25) je velice jednoduché a snadno se v něm orientuje. Funkce programu jsou rozdělené do tří nabídek:

- Stav - zobrazí aktuální stav jednotlivých funkcí zabezpečení počítače, síťového připojení a Internetu (Obr. 26). Jednotlivé služby lze snadno (de)aktivovat

kliknutím na přepínač vpravo. U položky firewall lze navíc nastavit profil brány, tzn. upravovat úroveň zabezpečení od povolení všeho až po úplné blokování. U většiny možností lze také přidávat vlastní pravidla.

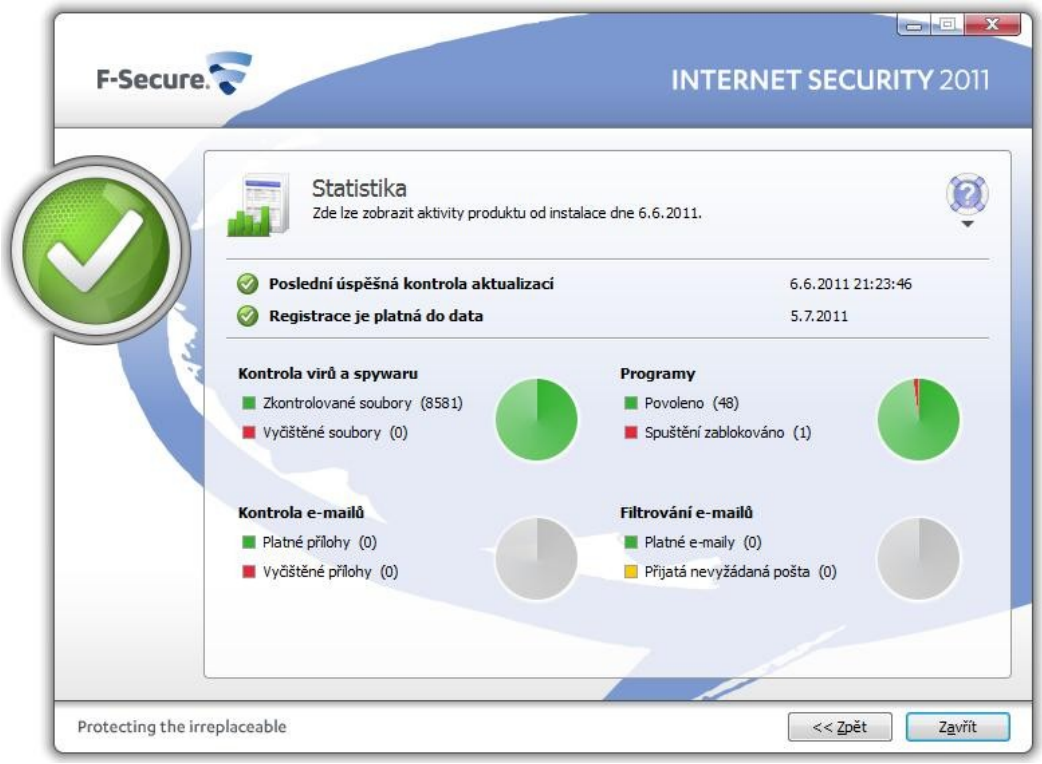
- Úlohy - z této nabídky (Obr. 27) lze spouštět funkce programu jako je kontrola počítače na přítomnost malwaru, aktualizace softwaru, nastavení programu apod.
- Statistika - obsahuje informace o aktivitách programu od jeho instalace (Obr. 28). Nalezneme zde počet zkontrolovaných souborů, počet povolených a zablokovaných programů, akceptovaných a odstraněných příloh e-mailu a další.



Obr. 25 - Prostředí programu Internet Security 2011

Obr. 26 - Nabídka „Stav“ programu Internet Security 2011

Obr. 27 - Nabídka „Úlohy“ programu Internet Security 2011



Obr. 28 - Okno „Statistika“ programu Internet Security 2011

3.2.2 Nastavení programu

Menu Nastavení je oproti NIS jednodušší, ale vhodně rozčleněné a dobře se v něm orientuje. Skládá z těchto záložek:

- Počítač
- Síťová připojení
- Internet
- Další nastavení

V záložce „Počítač“ nalezneme nastavení anitivirové a antispyware kontroly v reálném čase, funkci „DeepGuard“ monitorující procesy a programy v systému a v neposlední řadě nastavení plánované a ruční kontroly. Pro účely zabezpečení firemní sítě jsem nastavil všechny bezpečnostní služby jako aktivní, v případě nalezení viru

nebo nebezpečného programu jsem zvolil možnost dotázání při nejasnosti a spuštění pravidelné kontroly jsem nastavil na každé pondělí při nečinnosti déle jak 10 minut.

Pod záložkou „Síťová připojení“ se nachází nastavení brány firewall, kde je možné přidávat a upravovat pravidla síťového provozu, sledovat aktivitu jednotlivých procesů nebo spravovat síťové služby včetně protokolů a portů, které využívají.

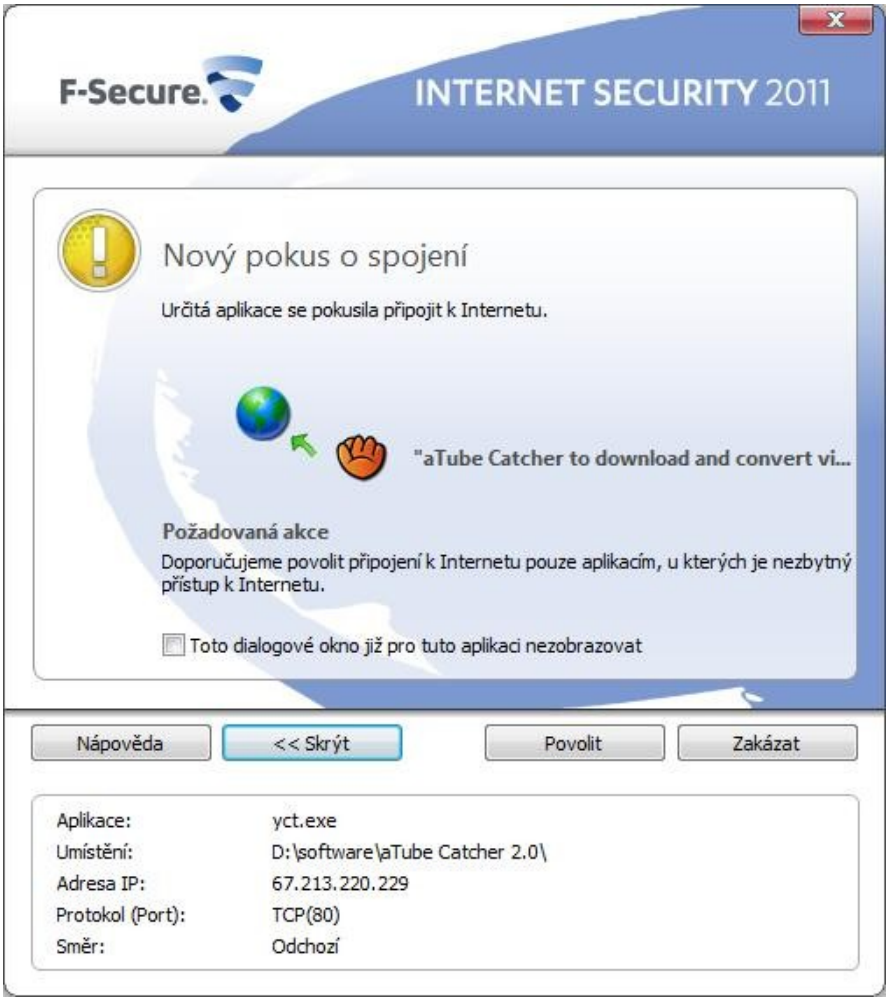
Velmi užitečnou službou v nabídce je real-time ochrana aplikací, která sleduje pokusy aplikací o navázání příchozího/odchozího spojení a umožní uživateli toto povolit nebo zakázat. Pravidla pro tuto ochranu lze nadefinovat dopředu v této záložce nebo postupně, jak se aplikace pokouší navázat spojení (musí být nastavena volba „Výzva pro nové programy“), jak je znázorněno na Obr. 29. Z vybrané nabídky profilů brány jsem zvolil profil „Kancelář“. Tato úroveň zabezpečení povoluje veškerý odchozí přenos TCP a příjem souborů pomocí protokolu FTP. Vše ostatní je ve výchozím nastavení zakázáno a výstrahy vygenerují pouze pokusy o nebezpečné připojení. Mohou být však přidána místní pravidla povolující nové síťové funkce.

Další důležitou funkcí v této záložce je prevence proti neoprávněnému vniknutí. Při pokusu o vniknutí jsem nastavil možnost pokusit se akci zablokovat a protokolovat včetně zobrazení výstrahy na obrazovce.

Poslední položky v záložce jsou kontrola vytáčení a protokolování. První z nich se týká telefonických připojení, kde můžeme, podobně jako u ochrany aplikací, definovat povolená/zakázaná čísla, druhá nám umožní sledovat a zaznamenávat síťové pakety.

První ze dvou funkcí v záložce Internet je ochrana procházení webových stránek. Zde jsem ponechal standardní nastavení, tj. zablokovat přístup, obsahuje-li stránka zneužití nebo je označena za nebezpečnou. Zobrazení hodnocení pro výsledky vyhledávacích webů (např. Google) jsem také nechal aktivní.

U druhé funkce v této záložce - filtrování e-mailů - jsem váhal, mám-li nechat tuto službu aktivní, jelikož v dnešní době má téměř každý provozovatel e-mailových schránek implementovanou svou vlastní ochranu proti spamu. Nakonec jsem ale tuto službu ponechal zaplou, ovšem pouze ve středním režimu místo agresivního.



Obr. 29 - Výstraha při novém pokusu o navázání spojení

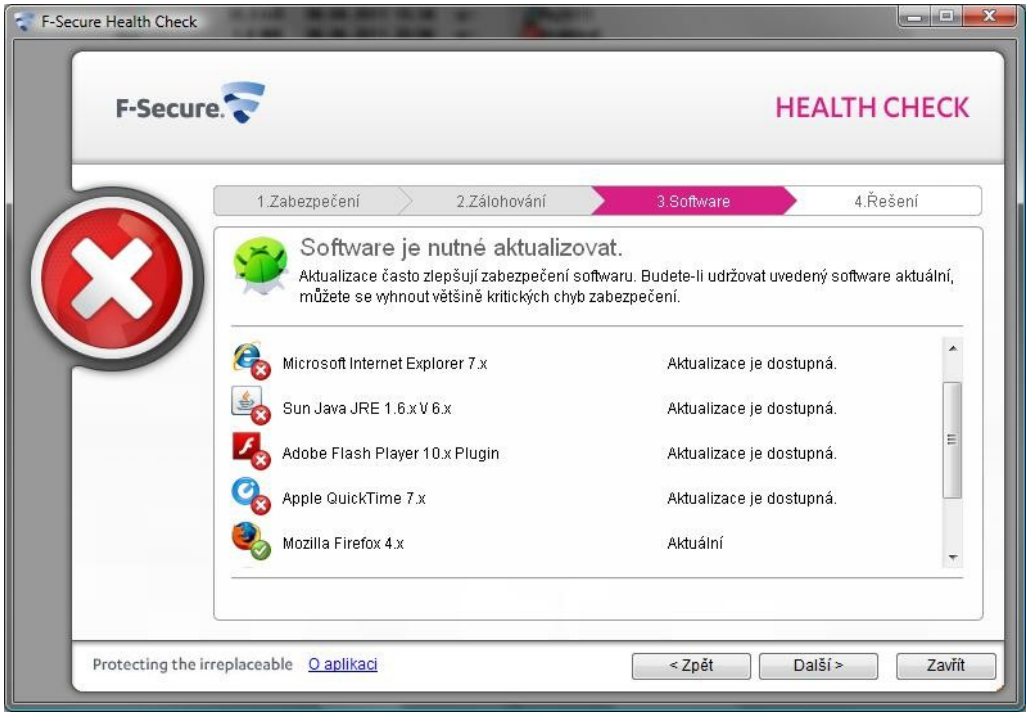
V poslední záložce se nachází nastavení a přehled stažených a nainstalovaných aktualizací produktu, nastavení připojení k Internetu a serveru HTTP proxy nebo stav registrace.

3.2.3 F-Secure Health Check

Tato funkce se nachází pod ikonou otazníku (Obr. 30) a je dostupná z kterékoliv nabídky hlavní okna programu. Po kliknutí se otevře webová stránka výrobce, na které se nachází spouštěcí aplikace. Stačí zvolit jazyk, zatrhnout souhlas s licenčními podmínkami a spustit kontrolu.

Jedná se o službu, která v několika krocích zkontroluje aktuálnost bezpečnostního softwaru v počítači, je-li aktivní služba pro zálohování souborů a také zjistí aktuálnost běžného softwaru (Obr. 31) jako je webový prohlížeč, Java, Flash přehrávač nebo samotný operační systém. V posledním kroku se nachází přehled výsledků celé kontroly a je nám nabídnuto řešení zjištěných nedostatků.

Obr. 30 - Přístup ke službě Health Check

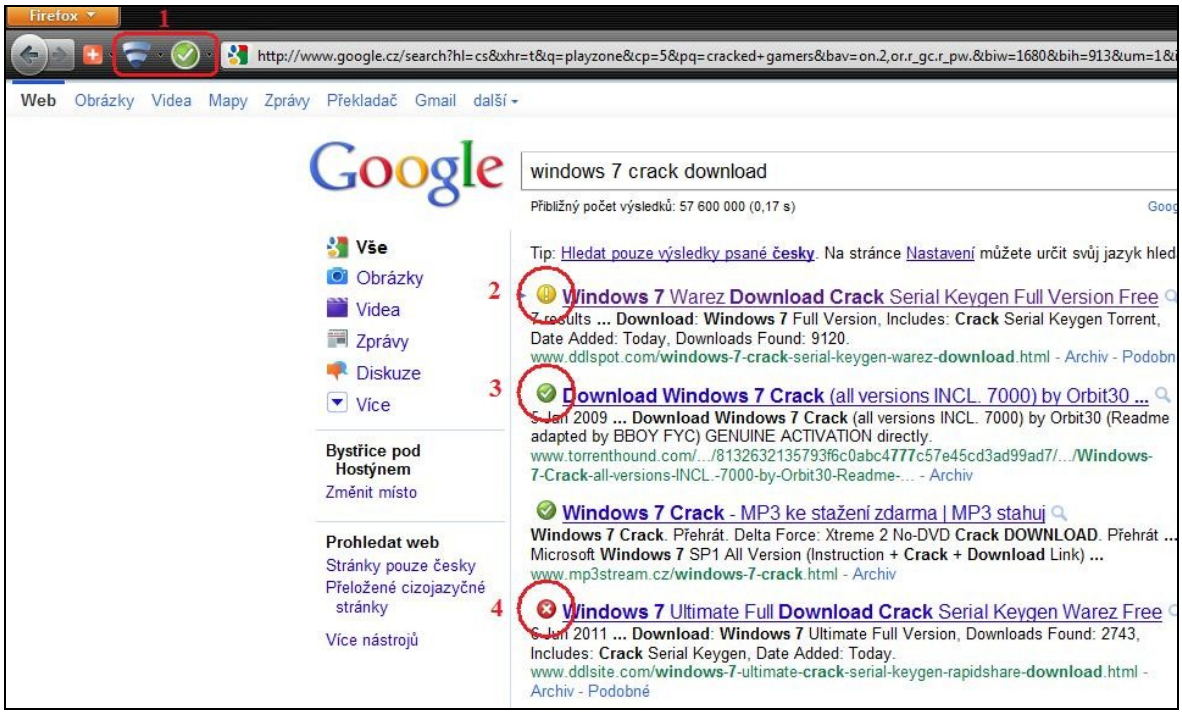


Obr. 31 - Okno zobrazující aktuálnost softwaru v počítači

3.2.4 Implementace v prohlížeči

Podobně jako to bylo u NIS je i Internet Security 2011 implementován do webových prohlížečů Internet Explorer a Mozilla Firefox (Google Chrome není podporován, ostatní nebyly testovány). V obou prohlížečích běží hodnocení výsledků vyhledáčů. Z nejznámějších podporovaných vyhledávačů je to Google a Yahoo, český Seznam bohužel podporován není. Implementaci této funkce v prohlížeči Mozilla Firefox bych rád demonstroval na následujícím obrázku (Obr. 32):

1. Ovládací tlačítka v nástrojové liště umožňují zobrazit bezpečnostní přehled o aktuální stránce a sdělit uživatelův názor na její obsah. Samotná ikona tlačítka vpravo signalizuje, zda-li je stránka bezpečná či ne.
2. Ikona symbolizující, že je daná stránka podezřelá, avšak program přístup na tuto nezablokuje. Pouze se změní vzhled tlačítka v nástrojové liště na vykřičník ve žlutém poli.
3. Tato ikona symbolizuje, že je daná stránka bezpečná.
4. Tento typ ikony značí nebezpečnou stránku a program přístup na ni zablokuje.



Obr. 32 - Implementace ochrany prohlížení a hodnocení výsledků vyhledávače

3.2.5 Testy bezpečnosti

Bezpečnostní testy, které jsem provedl na softwaru Internet Security 2011 byly z důvodu porovnání obou produktů totžné jako u Norton Internet Security 2011.

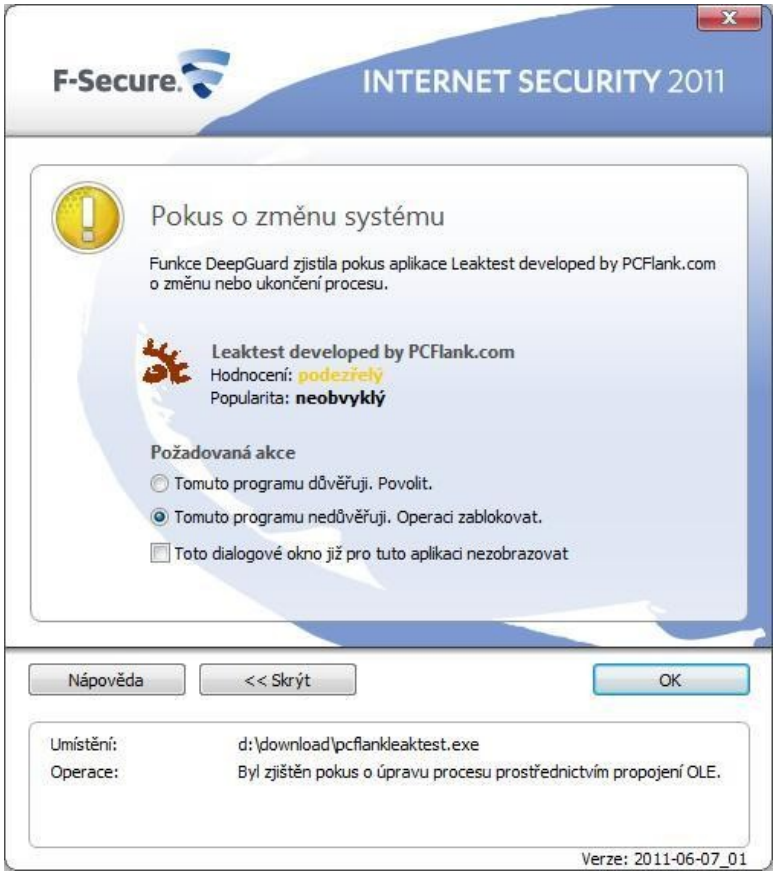
Jako první jsem otestoval reakci softwaru na testovací soubory na stránce http://eicar.org/. První typ souboru se podařilo uložit, ale následná automatická kontrola jej zachytila a zablokovala. V pop-up okně s výstrahou (Obr. 33) stačilo zvolit automatické zpracování a soubor byl odstraněn, což bylo signalizováno informací v rohu obrazovky. U textového souboru s řetězcem symbolizujícím škodlivý kód byla byla situace stejná jako u NIS, tj. soubor se podařilo uložit i otevřít, ale následná vyžádaná kontrola odhalila hrozbu a po nabídnutí činnosti byl soubor úspěšně odstraněn. U komprimovaných souborů se situace opět shodovala. Všechny soubory ve formátu ZIP šly otevřít, ale jejich obsah - soubor eicam.com - již nikoliv. Program je dokázal zachytit, zablokovat přístup a odstranit. Uvedené skutečnosti platí pro oba protokoly HTTP i HTTPS.

Test základních síťových služeb na adrese http://test.bezpecnosti.cz/ dopadl ve prospěch programu. V průběhu testu nebyla nalezena žádná veřejně dostupná služba nebo služba, která je používaná, ale odmítá přijmout požadavek z výše uvedeného serveru. Naopak všechny služby byly vyhodnoceny jako zabezpečené.

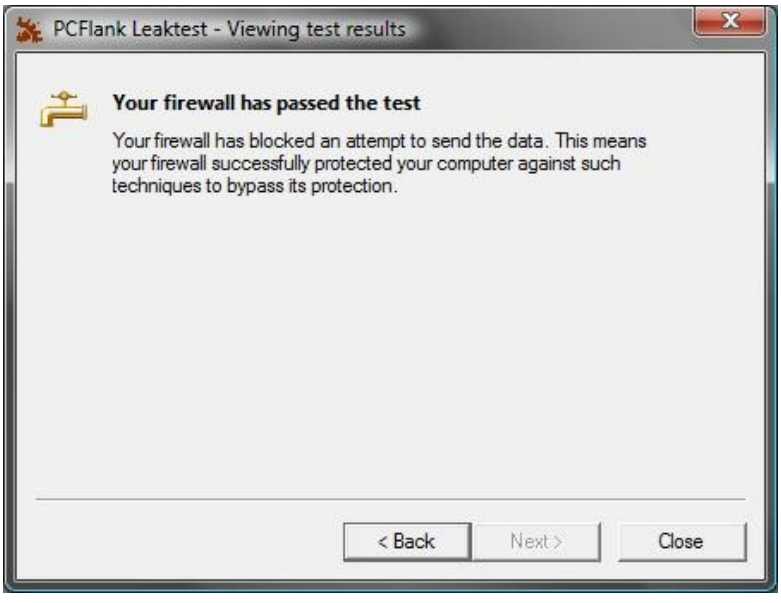
Druhý test na přítomnost trojských koní, respektive napadnutelnost systému tímto malwarem dopadl taktéž výborně. Ani jeden z 30ti otestovaných portů, které jsou nejčastěji trojskými koňmi využívány, nebyl vyhodnocen jako běžící.

Poslední test na schopnost firewallu zamezit nežádané odchozí komunikaci byl proveden pomocí programu PCFlank Leaktest 1.0. Při pokusu o odeslání dat zachytila funkce DeepGuard tento proces, jak je znázorněno na Obr. 34. Na toto upozornění jsem reagoval zablokováním operace, program Internet Security tedy dokázal zamezit odchozí komunikaci v tomto testu uspěl (Obr. 35).

Obr. 33 - Pop-up okno s upozorněním na soubor



Obr. 34 - Okno s výstrahou při pokusu o navázání odchozí komunikace



Obr. 35 - Úspěšný výsledek testu na zamezení odchozí komunikace

4 NÁVRH ŘEŠENÍ

Při rozhodování se, jaký software je pro návrh řešení zabezpečení firemní sítě vhodnější, jsem bral v potaz faktor míry zabezpečení, jednoduchosti práce s programem od jeho instalace až po nastavení, ceny a samozřejmě výsledku dosaženého ve srovnávacím testu společnosti AV-Comparatives. Oba dva programy měly snadný průběh instalace, který pozitivně ovlivnila i podpora českého jazyka. Při srovnání UI obou programů je pro mě přijatelnější produkt společnosti F-Secure, přestože jsou obě prostředí velice přehledné a snadno se v nich orientuje. Nastavení programu u produktu Norton Internet Security je více „user-friendly“ díky lepšímu grafickému zpracování, na druhou stranu je možností nastavení až příliš a méně zkušený uživatel z toho může být do jisté míry zmatený. Z tohoto hlediska je na tom software společnosti F-Secure lépe - menu nastavení je sice stručné, ale jasné, tudíž by s nastavením neměl mít problémy ani běžný uživatel.

Co se týče funkcí programů - ty jsou u obou srovnatelné. Dalo by se říct, že NIS těží z výhod funkce File Insight, která ve spolupráci s komunitou Norton poskytuje informace o důvěryhodnosti souborů. Také funkce Identity Safe je velmi užitečná, zejména pokud uživatel ke své práci používá webové stránky vyžadující zadávání přihlašovacích údajů. Obecně mohu říct, že software Norton Internet Security obsahuje oproti F-Secure Internet Security více dílčích služeb, ale hlavní zabezpečující funkce jsou na více méně srovnatelné úrovni.

Při testech zabezpečení počítače jednotlivými produkty se objevily do jisté míry důležité rozdíly. De facto se jednalo o rozdíl jediný, avšak o to významnější při konečném rozhodování. Na testovací soubory na webu společnosti EICAR reagovaly oba programy shodně a oba v tomto testu uspěly. Taktéž při testu zabezpečení základních síťových služeb i testu na trojské koně byly výsledky bezchybné a totožné pro oba softwary. Změna nastala až při provádění leak testu - testu na odchozí komunikaci. V tomto produkt společnosti Symantec ani po úpravě nastavení, narozdíl od produktu F-Secure, neuspěl. Ten dokázal pokusu o nežádanou odchozí komunikaci a tudíž i potenciální krádeži dat zabránit.

Dalším srovnávacím faktorem byla cena. I v tomto ohledu vychází lépe produkt F-Secure, který má možnost zakoupení výhodné licence pro více počítačů. Při zakoupení licence softwaru na 3 roky s možností instalace až na 3 počítače vychází cena na rok pro jeden počítač přibližně 340 Kč. Pro software Norton Internet Security 2011 vychází nejlevnější varianta (při zakoupení licence na 5 let) na zhruba 500 Kč na rok pro jeden počítač.

Jako poslední, ne však jako nejméně důležitý, jsem bral v potaz umístění programů ve srovnávacích testech za uplynulý rok 2010. V tom zvítězil produkt společnosti F-Secure a získal tak titul „Produkt roku 2010“.

Když zvážím všechna pro a proti obou produktů, vyjde mi jako nejlepší varianta pro dané řešení bezpečnosti software F-Secure Internet Security 2011.

ZÁVĚR

Cílem této práce bylo popsat problematiku daného tématu, zejména pak jednotlivé druhy škodlivého softwaru, jeho dopady na bezpečnost počítačů a možný způsob ochrany proti nim. Na základě těchto faktů pak navrhnout řešení, které bude schopné poskytnout optimální zabezpečení firemní sítě.

V teoretické části jsem se zabýval nejčastějšími typy škodlivého softwaru jako jsou počítačové viry, červi, trojské koně, spyware a další. Popsal jsem jejich rozdělení podle různých hledisek, příznaky jejich přítomnosti v počítači a nejznámější zástupce jednotlivých skupin. Dále jsem popsal možnosti prevence před škodlivým softwarem, ochranou pomocí antivirových systémů, jejich funkce a typy. Nakonec jsem v této části nastínil metody používané při srovnávacích testech antivirových produktů a jejich výsledky.

V praktické části jsem testoval dva zástupce antivirového softwaru, kteří v poslední době dosáhli vynikajících výsledků ve zmíněných testech. U obou programů jsem popsal jejich instalaci, grafické uživatelské prostředí, optimální nastavení programu, které vyhovuje požadavkům firemní sítě a zvláště užitečné funkce. Následně jsem provedl bezpečnostní testy obou programů. Jednalo se o test zabezpečení portů, test na detekci škodlivého programu a test proti nežádoucímu odchozímu spojení. Po vyhodnocení všech kritérií jsem dospěl k výsledku a navrhl řešení odpovídající požadavkům na bezpečnost firemní sítě.

Při psaní této práce jsem se naučil mnoho nového a i přes vynechání některých bodů, které jsem měl původně v plánu uskutečnit, si myslím, že výsledné řešení je vhodné pro současné standardy a dokáže účinně chránit síť i její uživatele před vnějšími hrozbami.

ZÁVĚR V ANGLIČTINĚ

The aim of this work was to describe the issues of given topic, especially particular types of malicious software, its impact on computer security and possible methods of defence. Based on this facts, I was supposed to design a solution for optimal corporate network security.

In the theoretical part of this work I dealt with most common types of malware such as computer viruses, worms, trojan horses, spyware and so on. I described the devision of malware according to various acpects, symptoms of computer infection and the most famous specimen of each type. I also described the possibilities of malware infection prevention, defence through the use of antivirus systems, its functions and types. At last I outlined the methods used in antivirus comparative tests and its results.

In the practical part I tested two pieces of antivirus software, which are the best-rated products in recent comparative tests. I described the process of instalation for both of the programs, its GUI, optimal settings that meets the requirements of corporate network and its special features. Afterwards I ran some security tests for both of the programs. It dealt with port protection, malware detection and detection of unwanted outgoing communication. After analyzing the test results I came to a verdict and designed the final solution matching the corporate network security requirements.

By working on this thesis I learned quite a lot of new things and even I omitted some task points I planned to dealth with, I think the solution I designed is suitable for today‘s standards and is capable of defending the network as well as its users.

SEZNAM POUŽITÉ LITERATURY

[1] POŽÁR, Josef. *Informační bezpečnost*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

[2] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[3] KLANDER, Lars. *Hacker Proof : váš počítač, vaše síť a vaše připojení na internet. Je to opravdu bezpečné?*. 1. vyd. Brno : UNIS, 1998. 648 s. ISBN 8086097153.

[4] SZOR, Peter. *Počítačové viry : analýza útoku a obrana*. Vyd. 1. Brno : Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.

[5] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.

[6] LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí*. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.

[7] HOVĚZÁK, Vít. Kyberman.wz.cz [online]. 2007 [cit. 2011-05-24]. Počítačové infiltrace. Dostupné z WWW: <http://www.kyberman.wz.cz/files/8_Viry.pdf>.

[8] Trojský kůň (program). In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 26.2.2009, last modified on 29.3.2011 [cit. 2011-05-25]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Trojsk%C3%BD_k%C5%AF%C5%88_(program)>.

[9] Antivirový program. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 19.11.2006, last modified on 5.4.2011 [cit. 2011-05-25]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Antivirov%C3%BD_program>.

[10] Počítačový červ. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 1.6.2006, last modified on 18.1.2011 [cit. 2011-05-26]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv>.

[11] Microsoft Corporation. *Web podpory Microsoft* [online]. 2011 [cit. 2011-05-28]. Počítačové viry: popis, prevence a obnovení. Dostupné z WWW: <http://support.microsoft.com/kb/129972/cs>.

[12] Microsoft Corporation. *Zabezpečení pro domácnosti* [online]. 2011 [cit. 2011-05-30]. Co je to virus, červ a trojský kůň?. Dostupné z WWW: <http://www.microsoft.com/cze/athome/security/viruses/virus101.mspx>.

[13] HÁK, Igor. *Viry.cz : Igiho stránka o virech* [online]. 1998 [cit. 2011-06-01]. Dostupné z WWW: <http://www.viry.cz/go.php>.

[14] *AV-Comparatives - Independent Tests of Anti-Virus Software - Welcome to AV-Comparatives.org* [online]. 2004 [cit. 2011-06-02]. Dostupné z WWW: <http://wwww.av-comparatives.org/>.

[15] PC Flank Ltd. *PC Flank: Make sure you're protected on all sides.* [online]. c2010 [cit. 2011-06-04]. Dostupné z WWW: <http://pcflank.com/>.

[16] Symantec Corporation. *Buďte v pohodě. Máte Norton* [online]. 1995 [cit. 2011-06-05]. Dostupné z WWW: <http://cz.norton.com/index.jsp>.

[17] F-Secure Corporation. *F-Secure - Home* [online]. c2011 [cit. 2011-06-07]. Dostupné z WWW: <http://www.f-secure.com/en/web/home_global/home>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AFP	Agence France-Presse
B	Byte
BAT	Batch File
BIN	Macbinary Encoded File
BIOS	Basic Input-Output System
CAB	Windows Cabinet File
CD	Compact Disc
CIA	Central Intelligence Agency
CMD	Windows Command File
COM	Component Object Model
CSS	Cascading Style Sheets
DEFCON	Defense Readiness Condition
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
DPH	Daň z Přidané Hodnoty
DVD	Digital Versatile Disc
€	Euro
EICAR	European Institute for Computer Antivirus Research
EXE	Executable
FAT	File Allocation Table
FTP	File Transfer Protocol
GUI	Graphic User Interface
HTA	HyperText Markup Language Application
HTM	HyperText Markup Language File

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
ICQ	I Seek You
IE	Internet Explorer
IP	Internet Protocol
IRC	International Relay Chat
IM	Instant Messaging
JPG	JPEG Image File
JPEG	Joint Photographic Experts Group
JS	JavaScript
JSE	JavaScript Encoded File
KB	KiloByte
Kč	Koruna česká
LAN	Local Area Network
MBR	Master Boot Record
ME	Millenium
MP2	MPEG-1 Audio Layer II
MP3	MPEG-1 Audio Layer III
MS	Microsoft
MS-DOS	Microsoft Disk Operating System
NASA	National Aeronautics and Space Administration
NIS	Norton Internet Security
NT	N-Ten
NTFS	New Technology File System

OS	Operační Systém
OVL	Overlay
PHP	Personal Home Page
PIF	Program Information File
POP3	Post Office Protocol version 3
RAR	Roshal Archive
SCR	Windows Screensaver
SCT	Scitex Continuous Tone File
SQL	Structured Query Language
SYS	Windows System File
TCP	Transmission Control Protocol
TXT	Plain Text File
UDP	User Datagram Protocol
UI	User Interface
USD	United States dollar
USA	United States of America
VBE	VESA BIOS Extensions
VBS	Visual Basic Script File
WSH	Windows Script Host
WWW	World Wide Web
XP	Experience
ZIP	Zipped File

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH