

Možnosti a hrozby elektronického monitoringu činnosti firmy XY

Vít Komárek

Bakalářská práce
2005



Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav informatiky a statistiky
akademický rok: 2004/2005

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Vít KOMÁREK**
Studijní program: **B 6208 Ekonomika a management**
Studijní obor: **Management a ekonomika**

Téma práce: **Možnosti a hrozby elektronického monitoringu
činnosti firmy XY**

Zásady pro vypracování:

- 1. Provedte průzkum dostupných informačních zdrojů týkajících se elektronického monitoringu.**
- 2. Konkretizujte aktuální ohrožení elektronického monitoringu pro danou firmu XY.**
- 3. Navrhněte opatření pro odstranění nedostatků a jejich realizaci.**

Rozsah práce: 40 stran
Rozsah příloh:
Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

Doseděl, Tomáš. Počítačová bezpečnost a ochrana dat. Praha : Computer Press, 2004. 200s. ISBN 8025101061

Anonymous. Maximální bezpečnost. Praha : Softpress, 2004. 984s. ISBN 8086497658

Musil, Rudolf. Ochrana utajovaných skutečností. Praha : Eurounion, s. r. o., 2001. 381s. ISBN 8085858932

Dostupné na World Wide Web : <<http://www.securityserver.cz>>

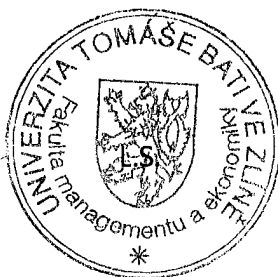
Dostupné na World Wide Web : <<http://www.spyware.cz>>

Další dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky
Datum zadání bakalářské práce: **14. března 2005**
Termín odevzdání bakalářské práce: **20. května 2005**

Ve Zlíně dne 14. března 2005


doc. PhDr. Václav Nováček, CSc.
děkan




doc. Ing. Rudolf Pomazal, CSc.
ředitel ústavu

ABSTRAKT

Abstrakt česky

Tato práce přibližuje důležitost bezpečnostní politiky pro firmu, přičemž popisuje způsob jejího vypracování, správnou strukturu i následnou implementaci do činnosti firmy. Blíže se věnuje vysoce rozvíjející se oblasti počítačové a komunikační bezpečnosti, kterou je spyware. Tato část je narozdíl od hrozby v podobě virů méně známá, avšak co do ohrožení firmy stejně nebezpečná, ne-li nebezpečnější. Je to dáno zejména neznalostí problematiky a v jejím důsledku nulovou ochranou před ní. Cílem práce je tento nedostatek odstranit a pomocí závěrů a doporučení z ní vyplývajících přispět k vyšší bezpečnosti firmy.

Abstrakt ve světovém jazyce

This thesis deals with the importance of the safety policy for a company and describes the process of its construction, its proper structure and following implementation into the company's activity. The thesis takes a closer look at the up-and-coming area of computers and communication safety, the "spyware". Unlike the threat of viruses, this area is not so widely known, yet equally or even more dangerous. That is mainly owing to the ignorance of these problems resulting in zero protection. The aim of this thesis is to eliminate this drawback and by conclusions and recommendations to also contribute to a higher level of the company's safety.

Rád bych poděkoval Mgr. Romanu Jaškovi, Ph.D. za poskytování cenných rad a připomínek při konzultování této bakalářské práce.

Dále bych chtěl poděkovat majiteli firmy XY za jeho připomínky, názory a zejména ochotu podílet se na mé práci.

OBSAH

OBSAH	6
ÚVOD.....	8
I. TEORETICKÁ ČÁST	9
1 INFORMAČNÍ BEZPEČNOST	10
1.1 POČÍTAČOVÁ A KOMUNIKAČNÍ BEZPEČNOST	10
1.2 ADMINISTRATIVNÍ BEZPEČNOST A ORGANIZAČNÍ OPATŘENÍ.....	11
1.3 PERSONÁLNÍ BEZPEČNOST	11
1.4 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU	12
2 BEZPEČNOSTNÍ POLITIKA.....	13
2.1 VYPRACOVÁNÍ BEZPEČNOSTNÍ POLITIKY	13
2.2 STRUKTURA BEZPEČNOSTNÍ POLITIKY	15
2.2.1 Předběžná studie.....	16
2.2.2 Zadání.....	16
2.2.3 Analýza rizik	17
2.2.4 Sepsání bezpečnostní politiky organizace.....	19
2.2.5 Realizace	20
3 SPYWARE	21
3.1 TYPY SPYWARE	22
3.1.1 Adware	23
3.1.2 Hijacker	23
3.1.3 Stealth networks	25
3.1.4 System moniors	25
3.1.5 Dialer	26
3.1.6 Backdoor trojans	28
3.1.7 Cookies.....	28
3.2 DOPADY SPYWARE	29
3.3 PROGRAMY K ODSTRANĚNÍ SPYWARE	30
II. PRAKTICKÁ ČÁST	32
4 TESTOVANÉ PROGRAMY	36
4.1 MICROSOFT ANTISPYWARE BETA	36
4.2 BAZOOKA™ ADWARE AND SPYWARE SCANNER.....	38
4.3 ADAWARE SE PERSONAL EDITION 1.05.....	40
4.4 SPYBOT - SEARCH & DESTROY 1.3.....	43
4.5 WEBROOT SPY SWEEPER 3.5	45
4.6 SPYREMOVER 2.33.....	47
4.7 SPYWAREBLASTER 3.3.....	48
4.8 SPYWARE DOCTOR 3.2	50

4.9	COUNTERSPY 1.0.29	52
4.10	ETrust PestPatrol Anti-Spyware 4.4	54
5	POROVNÁNÍ PROGRAMŮ	56
5.1	ZPŮSOB HODNOCENÍ.....	58
5.1.1	Vyhledávací engine	58
5.1.2	Ovládání	58
5.1.3	Rychlost.....	58
5.1.4	Podpora	58
5.1.5	Další funkce	58
5.1.6	Poměr cena/výkon.....	58
6	VÝSLEDKY TESTU A ZHODNOCENÍ PROGRAMŮ	60
	ZÁVĚR.....	62
	SEZNAM POUŽITÉ LITERATURY.....	64
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	67
	SEZNAM OBRÁZKŮ	68
	SEZNAM TABULEK.....	69
	SEZNAM PŘÍLOH.....	70

ÚVOD

Hodnotu čehokoliv člověk zpravidla pochopí až v okamžiku, kdy o to přijde. Zatímco ztráta hardwaru představuje (relativně) jednoduchý problém, ztráta počítačových dat mívá mnohem horší následky. Zrekonstruovat je v původní podobě je většinou náročné (časově i finančně) a často přímo nemožné. A navíc takováto ztráta může mít i další důsledky: jistě si dokážete představit, co asi udělá útočník, který získá přístup k heslům od Vašeho bankovního účtu. Co udělá konkurenční firma, která se dostane k budoucím plánům Vaší firmy. Co udělají zákazníci banky, která nedokáže ochránit jejich osobní údaje nebo která se stane obětí hackera. A takovýchto příkladů lze uvést více.

V dnešní době vysoce závislé na informačních technologiích je informační bezpečnost prvořadou záležitostí pro každou firmu nehlédě na její velikost či obor činnosti. Proto kvalitní bezpečnostní politika počínaje její tvorbu, stálou aktuálností až po její důsledné dodržování je jednou z podmínek úspěšné firmy nového tisíciletí.

Cílem této práce je podrobněji seznámit čtenáře s významem bezpečnostní politiky, její tvorbou a následnou implementací. Blíže se věnuje oblasti počítačové a komunikační bezpečnosti, která v poslední době zažívá nebývalý rozmach a tím je skupina "softwarových ohrožení", obvykle souhrnně nazývaná spyware. Naznačuje jeho dělení a popisuje nebezpečí, která může jeho přítomnost v podnikovém počítači způsobit. Praktická část je zaměřena na způsob jeho odstranění a pomocí důkladného popisu deseti programů zabývajících se jeho eliminací se snaží čtenáři ulehčit orientaci mezi širokou škálou nabízených programů. Z provedeného srovnávacího testu si každý může vybrat program, který nejvíce splňuje jím požadované nároky, jelikož někdo dá přednost výkonu před vzhledovou přívětivostí a pro jiného je přednější design a ovladatelnost, přičemž se spokojí s nižším výkonem.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ BEZPEČNOST

Ve snaze předcházet bezpečnostním incidentům, které by ohrožovaly hmotné i nehmotné aktiva firmy, se zrodila **informační bezpečnost**. Jejím cílem je zajistit, aby:

- K elektronickým datům měly přístup pouze oprávněné osoby a aby tato data nebyla vyzrazena.
- Nedocházelo ke zpracování zkreslených (poškozených, falšovaných apod.) dat.
- Bylo možné zjistit, kdo s daty manipuloval (tedy vytvořil, změnil nebo odstranil).
- Elektronická data byla v případě potřeby dostupná.

Požadavky kladené na informační bezpečnost jsou značně různorodé a proto zákonitě musí být různorodé také prostředky, jejichž pomocí je zajišťována. A aby to nebylo ani trochu jednoduché, různorodé jsou také způsoby, jimiž jsou elektronická data ohrožována a proti nimž je potřeba se bránit.

Každá firma, instituce nebo jen síť má své vlastní problémy, své vlastní slabiny, svá specifika. Pro přehlednost a podle specifických vlastností dělíme informační bezpečnost na následující části:

- Počítačová a komunikační bezpečnost
- Administrativní bezpečnost a organizační opatření
- Personální bezpečnost
- Fyzická bezpečnost informačního systému

1.1 Počítačová a komunikační bezpečnost

Tato oblast bezpečnosti se zabývá technickými a programovými prostředky zajištění bezpečnosti informačního systému a přenosu telekomunikačními kanály. Je to tedy hardware a software, který by nám měl zajistit (je-li správně navržen, konfigurován a provozuschopný) bezpečné připojení k internetu, bezpečnou komunikaci pomocí elektronické pošty, bezpečnou ochranu před počítačovými viry a dostatečnou kapacitu pro bezproblémový chod celého systému.

Pro zajištění této části celkové bezpečnosti slouží celá řada produktů odborných firem a specializovaných výrobců, nabízejících zabezpečení konkrétních komponent počítačové sítě.

1.2 Administrativní bezpečnost a organizační opatření

Jedná se o promyšlený systém bezpečnostních opatření, zásad, metod a postupů, který pamatuje na všechny reálné situace včetně katastrofických scénářů a dokáže zachovat za těchto okolností funkčnost a provoz systému. Dobře fungující, správně provozovaný soubor takových opatření pak představuje pojistku pro případy havárií, útoky zvenčí i zevnitř a další hrozby.

Administrativní bezpečnost a organizační opatření závisí především na lidech. Mohou být také nejlevnějším způsobem, jak efektivně vyřešit mnohé bezpečnostní požadavky, jde jen o jejich důsledné uplatňování. Jsou to zjednodušeně řečeno např. všechny dokumenty, které podepíše zaměstnanec ve chvíli, kdy byl seznámen s přístupem do sítě, kdy převzal klíče k určitým dveřím a že se zapovídá vynášet informace mimo oblast jeho činnosti.

Všechna tato opatření jsou vytvářena lidmi a pro lidi, kteří je musí dodržovat a být příslušně motivováni i nuceni k jejich dodržování, ať se jedná o zásady práce s technikou, sankce za nedodržování bezpečnostních předpisů nebo o důraznější prostředky. Někdy to spíše vypadá jako brzda a zbytečné zatěžování dalšími povinnostmi, může to dokonce působit jako nedůvěra vůči zaměstnancům. Všichni (i sami zaměstnanci) si však musí uvědomovat důležitost bezpečnostních opatření zejména v prevenci a zvyknout si na to, že je to přirozená součást každodenní práce.

1.3 Personální bezpečnost

V této oblasti bezpečnosti jde o pečlivý výběr zaměstnanců a uplatnění takových zásad, jež co možná nejvíce zúží pravděpodobnost výběru pracovníků, kteří jsou schopni zneužití informací. Něco zneužít se odhodlá člověk, který k tomu má své důvody, předpoklady, schopnosti a kterému je to především umožněno. Zásadou při přidělování přístupu k určitým informacím i při samotném výběru zaměstnanců, kteří budou informační systém používat (ne zneužívat), je jejich prověření. Prověření nově přijímaného pracovníka může obnášet například reference z bývalého zaměstnání, výpis z trestního rejstříku, psychologický posudek a další metody důsledných personalistů. A toto prvotní síto může

být následováno požadavky a opatřeními, jako například příslušnými dodatky k pracovní smlouvě o odpovědnosti a povinnostech zaměstnance. Dalším požadavkem na personální bezpečnost je školení zaměstnanců. K prvnímu školení dochází při nástupu do zaměstnání. Zaměstnanci by měli být seznámeni se všemi směrnicemi týkající se jejich odpovědnosti za bezpečné užívání informačního systému, kde je tyto směrnice možno najít a na koho se obrátit v případě nejasností. Zkušenosti ale ukazují, že nedílnou součástí prvotního školení by měly být i základy principů bezpečného chování – někteří zaměstnanci si například neuvědomují, že heslo je tajná informace, která se nesdílí se spolupracovníkům a nepoznamenává se na papírek přilepený pod klávesnicí. Poté by mělo docházet k pravidelným školením podle potřeby a aktuálních změn.

1.4 Fyzická bezpečnost informačního systému

Tato oblast zahrnuje veškerá opatření, která slouží k ochraně aktiv organizace před poškozením, zničením, odcizením apod. Představuje prvky objektové bezpečnosti stejně jako technická řešení. Jedná se tedy o

- zabezpečení všech objektů a místností zámky, případně bezpečnostními prvky na bázi vstupních čipových karet,
- ostrahu budov např. v podobě alarmů,
- bezpečné uložení hardwaru, záložních medií.

Implementaci informační bezpečnosti do firmy má za úkol kvalitní bezpečnostní politika.

2 BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika (dále BP) je základním dokumentem každé společnosti (z hlediska počítačové bezpečnosti). Jedná se o písemný dokument, který umožňuje koncepční a konzistentní budování bezpečnosti jak v oblasti informačních technologií, tak v ostatních oblastech. Tento dokument v obecné rovině popisuje základní požadavky organizace na zabezpečení a jeho cílem je ochrana veškerého hmotného i nehmotného majetku firmy, ochrana jejího dobrého jména a předmětu činnosti organizace.

Obsah BP musí pokrývat veškeré aspekty zabezpečení ochrany organizace, počínaje např. ochranou budov přes definování jednotlivých skupin zaměstnanců, zálohování dat až po plány obnovy činnosti. Tento obsah poté schvaluje vedení organizace a její schválená podoba je závazná pro všechny zaměstnance organizace. Prostřednictvím smluv s třetími stranami se pak jednotlivé relevantní požadavky BP přenášejí i na smluvní partnery organizace a jejich zaměstnance.

Samotná BP by měla být zpracována takovým způsobem, aby tento dokument nemusel být při organizačních změnách menší a střední úrovně nijak měněn. Avšak neměl by zůstat statickým dokumentem. Prostředí, ve kterém je informační systém umístěn, se v průběhu času mění. Je třeba čelit jiným hrozbám, chránit jiná aktiva apod.

Z pohledu standardizace BP se je v současné době možné opřít o standardy ISO, zejména ISO/IEC 17799:2000 IT: Code of Practice for Information Security Management. Tento standard pomáhá zejména při definici cílů a strategií BP, není však plnohodnotným návodem na její vypracování.

2.1 Vypracování bezpečnostní politiky

Při hledání odpovědi na otázku, kdo by měl pro organizaci BP vlastně vypracovat, máme na výběr ze tří možností:

- a) zaměstnanec organizace
- b) externí firma
- c) kombinace obou

První cestou je využití vlastních zdrojů. Z různých, převážně však finančních důvodů může organizace vypracovat BP a následnou dokumentaci prostřednictvím vlastních

zaměstnanců. Výhody tohoto řešení se zdají zpočátku jasné: nižší náklady a vyšší sepětí tvůrce s organizací. Nicméně pokud organizace nepatří do úzké skupiny firem, které zaměstnávají vlastního kvalitního bezpečnostního experta a jeho tým, začínají zprvu jasně viditelné výhody ustupovat – dá se tedy říci, že toto řešení přináší spíše některé podstatné nevýhody.

Běžný zaměstnanec běžné organizace nemá a ani nemůže mít komplexní přehled a dostatek zkušeností s tímto druhem práce. Nutně z toho vyplývá potřeba finančně nákladných školení či konzultací. Jejich počet nemusí být vůbec nízký, neboť určený pracovník organizace minimálně zpočátku nemusí vůbec tušit, co vlastně ke své práci potřebuje vědět a na co se ptát. To vede k postupnému zmizení výhody nízkých nákladů. Navíc i sebelepší školení je jen stále školení a praktické zkušenosti nenahradí. I školený pracovník potřebuje nutně spolupracovat se zkušeným kolegou. Ve většině organizací je navíc práce na BP chápána jako cosi navíc a členové týmu tento úkol řeší souběžně se svými běžnými povinnostmi. To pak vede k nesystematickým postupům a ve výsledku i k závažným chybám. Další nevýhodou tohoto řešení může být i nedostatek autority autorského týmu v očích vedení organizace, které by mělo vypracované řešení prosadit. Zde existuje efekt vyšší autority materiálu přicházejícího od specializované firmy zvenčí a podloženého jasně vyčíslitelnými náklady.

Druhou cestou je vypracování BP externí firmou. Tento případ lze považovat za protipól první varianty řešení. V tomto případě je zadána tvorba příslušné dokumentace externí firmě, v jejímž řešitelném týmu nefiguruje žádný přímý zástupce organizace, který by byl u tvorby od začátku do konce. V takovém případě nemusí být ani reakce pracovníků organizace při poskytování údajů formou různých interview ideální a jejich výsledky tak mohou být zkresleny. Nicméně hlavním rizikem tohoto způsobu je odchod know-how spojeného s projektem, ke kterému dochází s odchodem posledního zaměstnance externí firmy z organizace. Vynaložené prostředky tedy nejsou využity zcela efektivně a další rozvoj bezpečnostního povědomí a změny stávajícího stavu zabezpečení se nemusí kvalitně projevit ve změně bezpečnostní dokumentace a v zabezpečení aktiv oproti novým hrozbám či zvýšeným rizikům.

Jako optimální se tedy jeví varianta přípravy BP externí firmou za předpokladu, že je v pracovním týmu zařazen i dostatečný počet zaměstnanců organizace. Na tyto zaměstnance pak na základě uzavřené smlouvy přechází všechny znalosti potřebné

pro údržbu a rozvoj bezpečnosti organizace. Toto řešení zabezpečí i další z potřebných podmínek úspěšného řešení, totiž aby celé řešení bylo chápáno jako samostatný a plnohodnotný projekt organizace. Tím by mělo být zajištěno dodržování termínů, poskytnutí potřebných kapacit, potřebná podpora, autorita u ostatních pracovníků organizace a podobně.

Dalším krokem při řešení BP je určení osoby objednatele na straně organizace zodpovědné za realizaci projektu BP, tedy určitého garanta projektu. Jeho určení závisí na velikosti firmy.

V menších firmách, kde se většinou o oblast informačních technologií (dále IT) stará komplexně jeden či dva lidé, je nereálné kvůli implementaci bezpečnostní politiky přijímat další osobu a BP spadá do jejich kompetencí. U firem střední velikosti, které mají oddělení informačních technologií, přichází v úvahu ředitel tohoto oddělení (angl. Chief Information Officer – CIO). Jednoduše se k jeho čteným povinnostem přidá i oblast bezpečnosti. Praxe však ukazuje, že to není vždy nejšťastnější řešení. A proto ve větších firmách by za bezpečnost měl zodpovídat někdo jiný. Jednak proto, že je s tím poměrně dost práce a jednak také proto, že požadavky IT oddělení a BP mohou být v řadě případů protichůdné. Zde je nejlepší variantou zřízení samostatného oddělení bezpečnosti a pověření řádnou BP ředitele tohoto oddělení (angl. Chief Information Security Officer - CISO). Jedná se o osobu přímo podřízenou generálnímu řediteli. S ředitelem IT oddělení je služebně na stejné úrovni. Měl by být vybaven potřebnými pravomocemi pro případ krizových situací. Je samozřejmé, že u těchto firem čítajících více než 250 zaměstnanců s vlastními odděleními IT a bezpečnosti, se již nebude jednat o outsourcing jako je tomu u menších a středních organizací.

2.2 Struktura bezpečnostní politiky

Velmi důležitým faktorem při řešení BP je komplexní pohled. Je třeba dbát na to, aby se nekladl neoprávněný důraz na jednu složku řešení bezpečnosti (např. technické zabezpečení IT, útoky zvenčí) na úkor druhé (např. personální opatření, útoky zevnitř) a vzniklo tak vyvážené a celistvé řešení. Organizace si musí uvědomit, že tvorba kvalitní BP a navazující řešení bezpečnosti zasáhne více či méně do všech organizačních struktur a že se bude muset projevit ve většině stávajících psaných i nepsaných normách organizace. Zavedení a udržení požadované míry úrovně bezpečnosti vyžaduje osvětu

a pravidelné školení mezi pracovníky na všech úrovních, rovněž je nutná podpora ze strany vedení organizace. Nelze prosadit úspěšnou implementaci bezpečnostní politiky bez podpory a zainteresovanosti nejvyššího managementu organizace.

Za standardní postup při tvorbě a implementaci BP je považován tento souhrn kroků:

- předběžná studie
- zadání
- analýza rizik
- sepsání bezpečnostní politiky organizace
- realizace
- realizace a tvorba bezpečnostní dokumentace nižší úrovně
- průběžná realizace osvěty – udržování bezpečnostního povědomí zaměstnanců

2.2.1 Předběžná studie

Předběžná studie se nepovažuje za nezbytnou součást řešení, nicméně je často na místě. Z hlediska finančního jde o poměrně levnou záležitost, jež může celý projekt zkrátit a tím ve finále i zlevnit. Účelem studie je získat základní orientaci v organizaci a činnostech firmy i základní údaje o bezpečnostní situaci. Na podkladě těchto informací je možné stanovit přesněji zejména rozsah budoucích nutných prací, rozvržení a náplň jednotlivých etap a tím i rámcovou finanční náročnost.

Stanovení rozsahu by mělo být úkolem vedení organizace. Není vhodné se při zpracování studie omezovat jen na některé oblasti, protože bezpečnost je komplexní záležitost. Zužovat zájem na některé vybrané oblasti znamená, že případné problémy nemohou být ani identifikovány.

2.2.2 Zadání

V zadání stanoví organizace ve spolupráci s řešitelem své požadavky na bezpečnost. Řešitel toto zadání ve shodě se zadavatelem koriguje se smyslu zákonných předpisů, “rozumnosti” a obvyklosti požadavků zákazníka, případně navrhuje doplnění opomenutých skutečností.

2.2.3 Analýza rizik

Opravdu kvalitní BP lze sestavit pouze na základě kvalitně provedené analýzy rizik (dále AR). AR by měla rovněž předcházet jakýmkoliv finančním investicím do bezpečnosti, aby bylo zaručeno jejich maximální efektivní využití. Analýza rizik poskytne na základě relativně obecných informací ze zadání řešitelskému týmu odpovědi na otázky co chránit, proti čemu a jakým způsobem. AR se skládá z několika kroků:

- a) identifikace aktiv
- b) identifikaci hrozeb
- c) vlastní analýza rizik

Ad a) Tento krok má jediný úkol – zjistit, jaká aktiva se v systému vyskytují a jakou mají pro společnost cenu. Aktivem je cokoliv, co má pro organizaci hodnotu. Správné řízení aktiv je pro úspěch organizace životně důležité a je hlavní odpovědností všech úrovní řízení. Aktiva organizace zahrnují:

- fyzická aktiva (např. počítačový hardware, komunikační prostředky, budovy, ...)
- informace (dokumenty, databáze,...)
- software
- schopnost vytvářet určité produkty nebo poskytovat služby – know-how
- pracovní sílu, školení pracovníků, znalosti zaměstnanců, zapracování apod.
- nehmotné hodnoty (např. abstraktní hodnota firmy, image, dobré vztahy atd.)

Po vytvoření seznamu všech aktiv musíme určit jejich hodnotu. Tuto hodnotu stanovuje pokaždé někdo jiný v závislosti na tom, kdo je uživatelem ohodnocovaných aktiv. Jako příklad lze uvést, že jinou hodnotu bude mít databáze zákazníků pro obchodní oddělení, jinou pro účtárnu a zcela mizivou pro IT oddělení. Vždy je třeba brát v úvahu nejvyšší cenu. Způsob ohodnocování může být různý:

- stanovením finančních nákladů
- přiřazením empirické stupnice síly, např. 1 – 10
- použitím adjektiv z předem definovaného seznamu, např. nízký, střední, vysoký, ...

Ad b) Identifikace hrozeb, která aktivům hrozí, je o mnoho složitější krok. Hrozba má schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejích aktiv. Hrozby mohou mít přírodní nebo lidský původ a mohou náhodné nebo úmyslné. Škoda způsobená incidentem může být dočasné povahy nebo může být trvalá, jako je tomu v případě zničení, nebo nevratného poškození aktiv.

Seznam hrozeb se poměrně dynamicky vyvíjí, je tedy vysoká šance, že pokaždé na něco zapomeneme. K identifikaci hrozeb lze přistupovat několika způsoby.

- 1) *Intuitivní vyhledávání rizik* – jeho základem je důkladné přemýšlení nad všemi situacemi, které mohou nastat (Co když útočník provede to či ono? Co když do serverovny pronikne voda? ...). S největší pravděpodobností se při takovém přístupu na něco zapomene. Pak nezbyvá, než seznam hrozeb aktualizovat.
- 2) *Inspirace jinými seznamy hrozeb* – pokud zvolíme seznam, který byl vytvořen pro podobné prostředí, může být úspěšnost poměrně vysoká. I zde sice hrozí riziko omylu, není ale rozhodně tak vysoké jako v prvním případě. Nejhorší chybou je ovšem neindividualizování seznamu podle vlastního systému – každý systém i každé prostředí je lehce odlišné.
- 3) *Využití podrobných dotazníků* – pro různé prostředí jsou vytvořeny vysoce komplexní dotazníky. Při identifikaci rizik pak bezpečnostní expert prochází otázku za otázkou a zjišťuje, jak je na tom jeho systém v jeho prostředí. Výhodou tohoto přístupu je jeho vysoká kvalita – při dobře navrženém dotazníku jen stěží lze na něco zapomenout. Nevýhodou je poměrně vysoká časová náročnost a hlavně nedostupnost dotazníků.

Ad c) Nyní máme k dispozici dva seznamy - seznam aktiv, která se v systému vyskytují včetně jejich ohodnocení, a seznam hrozeb, které v daném prostředí hrozí. Úkolem analýzy je zjistit, jaká nebezpečí konkrétním aktivům hrozí. Postupně tedy procházíme jednotlivá aktiva a rozhodujeme, které hrozby se na konkrétní aktivum vztahují. Například na již zmiňovanou databázi obchodních partnerů se nevztahuje hrozba zničení velkou vodou. Tato hrozba se naopak vztahuje na nosič dat (disk), na kterém je databáze fyzicky uložena. Na nosič dat se zase nevztahuje hrozba nechtěného smazání uživatelem.

Výsledkem je seznam aktiv, kterým jsou přiřazeny jednotlivé hrozby. Každé konkrétní dvojici aktivum-hrozba lze přiřadit pravděpodobnost, s jakou ke konkrétní hrozbě u daného aktiva dojde. Můžeme tedy kvalifikovaně rozhodnout, proti jaké pravděpodobnosti hrozeb můžeme náš systém chránit.

I analýza rizik není záležitostí statickou. Prostředí, ve kterém se informační systém nachází se průběžně mění. Mění se hrozby, mění se aktiva i jejich hodnota pro firmu. Mění se pravděpodobnost výskytu hrozeb. Je tedy účelné provádět podobnou analýzu opakovaně s určitou periodou.

Výstupem AR je navržení jednotlivých ochran. Ochrana by měla být navržena pro každou dvojici aktivum-hrozba, často ale dojde k situaci, kdy jeden použitý bezpečnostní prostředek zajistí ochranu více takových dvojic. Jako ideální způsob návrhu se jeví postup shora dolů. U každé dvojice navrhujeme odpovídající ochranu a vyčíslíme náklady na její zavedení a udržování.

Posledním krokem je prosazení jednotlivých ochran (a hlavně výdajů na ně) u vedení společnosti. Vždy je možno aplikovat jednoduché pravidlo: ochrana má smysl jen tehdy, pokud náklady na její zavedení nepřevýší cenu chráněných aktiv. V této oblasti nám pomohou jednotlivá oddělení, která se přímo podílela na oceňování aktiv.

Sekundárním přínosem provedení AR a na jejím základě získaných informací může být i lepší pochopení vnitřních mechanismů organizace a zlepšení řídicích procesů firmy. Nedostatečně či špatně provedená AR může mít pro organizaci fatální následky.

2.2.4 Sepsání bezpečnostní politiky organizace

Kvalitní BP musí obsahovat minimálně tyto body:

- Stanovení účelu BP, prohlášení o závaznosti BP pro pracovníky a deklarace plné podpory ze strany vedení organizace
- Definici požadované úrovně bezpečnosti
- Definici úrovně zabezpečení a míry odolnosti proti jednotlivým typům útoků
- Definici bezpečnostního managementu organizace
- Základní (obecné) bezpečnostní opatření v oblasti administrativní, personální, fyzické a systémové (oblast IT)

- Normy chování zaměstnanců organizace
- Havarijní plány a postupy v obecné rovině
- Deklarace souladu řešení bezpečnosti s relevantní legislativou a normami

Po zpracování jednotlivých kapitol BP jsou pak tyto konzultovány a předloženy k připomínkám a akceptaci. Po odsouhlasení všech kapitol je vypracován výsledný dokument, tedy **celková BP**. Ta je poté předložena nejvyššímu managementu organizace k vyslovení souhlasu a má být uvedena v platnost. Velmi vhodné je již akceptovanou BP formou prezentace představit minimálně vyššímu a střednímu managementu organizace. Její autor by měl vysvětlit význam dokumentu a objasnit všechny používané pojmy, definice, odpovědět na dotazy atd.

2.2.5 Realizace

Realizace neboli zavedení vypracované BP do praxe se zdánlivě jeví jako snadný úkol. Ve skutečnosti však spíše opak bývá pravdou – hlavně v případech, kdy je bezpečnost v dané organizaci řešena „od nuly“. Praktické zavedení jednotlivých opatření do každodenního provozu fungující organizace vždy přináší určité restrikce vůči zaměstnancům a klade na ně požadavky, na něž dosud nebyli zvyklí. Zatímco restriktivní složka těchto opatření je patrná hned a pracovník ji pocítí s okamžitou platností, přínos daných opatření už tak snadno a jasně vidět není a obvykle se projeví až po určitém časovém úseku.

Vypracování BP představuje významný krok v nastavení bezpečnosti organizace na potřebnou úroveň, není však krokem posledním. Logickým důsledkem existence BP je potřeba vypracovat veškerou dokumentaci pro technickou i netechnickou oblast firmy.

Jak je vidno, problematika informační bezpečnosti je velmi rozsáhlá a není možné ji obsáhnout v jediné práci. Proto jsem se zaměřil na oblast počítačové a komunikační bezpečnosti - přesněji na její část, která v poslední době zaznamená největší rozmach - spyware.

3 SPYWARE

S rozmachem internetu se rozvinuly také nejrůznější metody jeho zneužití. Každá nová technologie se může stát cílem i prostředkem mnoha forem útoků. K útokům je také zneužívána řada služeb, které internet poskytuje – stále narůstající množství virů se šíří například prostřednictvím e-mailu. K nebezpečím, která jsou uživatelům již poměrně známá, a která tedy bývají i adekvátně ošetřena, se v poslední době stále více přidává velká skupina “softwarových ohrožení“, obvykle souhrnně nazývaná **spyware**. Název je složen z anglických slov spy (= sledovat nebo též špión) a software (programové vybavení počítače). Přesná definice tohoto pojmu je poněkud zamlžená. Podle některých pramenů je spyware špiónský prográmk, který se usadí ve Vašem PC a dokonale špehuje a krade Vaše hesla, historii navštívených stránek, čísla kreditních karet apod. a poté vše zasílá určitému uživateli, který dál zpracovává všechny údaje. Abych však byl co nejpřesnější, budu vycházet z definice podle COAST (Consortium of Anti-Spyware Technology Vendors), která jako spyware označuje jakýkoliv program, který napomáhá shromažďování informací o osobě či společnosti bez jejich vědomí a může tyto informace poslat neautorizované třetí osobě.

Riziko nákazy spyware záleží na několika parametrech:

- a) *Oblast zájmu uživatele na internetu*
 - nejrizikovějšími místy, kde se lze infikovat spyware jsou XXX stránky, Warez stránky a P2P síť
- b) *Používaný prohlížeč*
 - nejrozšířenější Internet Explorer patří k nejvíce rizikovým
 - dříve platilo, že přechod na jiný prohlížeč rapidně (ne-li úplně) minimalizoval možnost nákazy spyware, avšak nyní již to neplatí, jelikož i výrobci spyware si uvědomili tento trend a přizpůsobují tomu svou činnost
- c) *Operační systém*
 - ve své práci budu pracovat s operačním systémem Windows XP Professional SP2

- jelikož Windows patří k nejrozšířenějšímu operačnímu systému, mé poznatky a rady se budou vztahovat k němu, nikoli k ostatním (Linux,...)
- v dnešní době užívat Windows 98 (či dokonce starší), i když se všemi dostupnými záplatami, je vysoce riskantní (Microsoft již několikrát oznámil, že přestává pracovat na vývoji těchto svých produktů a doporučil svým uživatelům přechod na novější verze Windows)

3.1 Typy spyware

Do skupiny spyware spadá široké spektrum programů v nejrůznějších podobách. Podle účelu, ke kterému slouží, je můžeme dělit na adware, stealth networks, system monitor, dialers, backdoor trojans a cookies. Společnosti Webroot a EarthLink uskutečnily společný projekt Spy Audit, díky němuž můžete rychle zjistit množství spyware ve Vašem PC. Stačí si stáhnout malý test (asi 730 kB) a hned vidíte, kolik a jakého typu spyware máte na disku. Výsledky poté statisticky zpracovávají do tabulky (Tab.1).

Tab. 1 Výsledky projektu Spy Audit

	III/04	IV/04
System Monitors	154 878	272 211
Trojans	148 214	254 155
Adware	5 978 018	6 971 086
Adware Cookies	22 327 112	25 598 803

zdroj : www.earthlink.net

Ve výsledcích projektu uvádějí, že za rok 2004 proběhlo celkem 4 610 738 testů a bylo nalezeno 116 519 040 potenciálního spyware. Tudíž každé z testovaných PC bylo průměrně infikováno 25 spyware! Z tabulky je na první pohled patrné, že spyware rapidně přibývá a přičemž nejrozšířenějšími druhy jsou adware.

3.1.1 Adware

- advertising-supported software
- jedná se o software, který zdarma uživateli poskytuje nějakou funkci a který je financován z prodeje reklamy
- příznaky jsou vyskakující (pop-up) reklamní okna během surfování, reklamní pruhy na webových stránkách, vnucování stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem
- typickým znakem je shromažďování informací o uživatelské pohybu internetem – sleduje, které stránky uživatel navštěvuje, na které reklamní odkazy “reaguje” (klikne na ně), a na základě toho sestaví uživatelský profil, podle kterého uživateli předkládá cílenou reklamu
- shromažďování reklamy může probíhat i bez zobrazení reklamy pomocí tzv. *web bug*, což je grafický objekt umístěný na stránce, který má rozměry 1 x 1 pixel a který slouží pouze ke sledování návštěv stránek.
- samostatně běžící programy uživatele zásobují reklamou, i když není připojen k internetu, jelikož mají reklamu uloženou lokálně a při připojení ji pouze aktualizují.
- mezi nejčastější a nejznámější adware patří SaveNow šířený s aplikací Kazza, Claria (ještě nedávno známá jako Gator), Download Accelerator nebo RealPlayer
- mezi nejnepříjemnější adware patří hijacker

3.1.2 Hijacker

- neboli únosce
- jedná se o speciální druh adware, trojského koně, který unese Internet Explorer a převezme nad ním kontrolu. To se projevuje tím, že hijacker vám změní Vaši domovskou stránku, nechává zobrazovat vyskakující okna a manipuluje s vyhledávací funkcí. V některých případech jsou dokonce seznamy oblíbených stránek učiněny nepoužitelnými a nahrazeny odkazy na reklamní stránky.
- infekce probíhá pomocí bezpečnostních mezer v Internet Exploreru jako například pomocí Java skriptů nebo komponenty ActiveX (u Windows se Service Pack 2 jsou tyto mezery odstraněny)

- výhodou pro útočníky je fakt, že téměř všechna nastavení Internet Exploreru jsou zakotvena v registru a dobře dokumentována. To usnadňuje útočnickovi práci. Avšak u prosté změny nastavení většinou nezůstává – navíc ještě proběhne instalace dalších trojských koňů, které tyto záznamy hlídají a při příštím spuštění webového prohlížeče ho opět přesměrují na reklamní stránky.

- Windows nabízejí takovým trojským koním celé množství možností, jak se usadit:

- Nejpoužívanější metodou automatického startu pro hijackery jsou schopnosti zásuvných modulů Internet Exploreru. Obzvláště známé jsou Browser Helper Objects (BHO), které rozšiřují Explorer. ICQ a Adobe Reader poskytují zcela regulérní BHO. Hijackery zde naproti tomu umísťují kód k zobrazení reklamních vyskakujících oken a spyware. Až do Service Pack 2 ovšem uživatel neměl žádnou šanci zjistit, které BHO jsou aktivní. Tomu lze přijít na kloub jen přes komplikovanou rešerši v registru. Od Service Pack 2 je přinejmenším teoreticky možné různé BHO zobrazit a deaktivovat.
- “System Hooking“ je varianta, při níž trojský kůň využívá různá systémem nabízená rozhraní, jako například “ShellExecute“, a různé klíčky myši a klávesnice, aby reagoval na akce uživatele, jako je například stisk určitých kláves.
- Další metodou je “zavěšení“ trojského koně na několik procesů zároveň. Pomocí “Winsock.dll“ může například hacker vpašovat svého trojského koně do každého procesu, který přistupuje k rozhraním poskytovaným Winsockem.

- Je-li hijacker v systému ukotven, následuje zanesení reklamních stránek do seznamu důvěryhodných webových serverů. Tak jsou Java skripty a elementy ActiveX prováděny s vypnutými bezpečnostními kontrolami, aniž by si uživatel čehokoli všiml. Při nedobrovolné návštěvě webových stránek se trojské koně automaticky aktualizují a obcházejí tak antivirové kontroly, čistící nástroje a firewallly.

- Nejzákeřnější současný hijacker se nazývá CoolWebSearch podle webové stránky s vyhledávačem www.coolwebsearch.com, na kterou tento trojský kůň surfaře přesměruje. Poprvé byl identifikován v květnu 2003 a od té doby je vyvíjen a aktualizován.

Ani profesionálové z antivirových laboratoří nemohou přisoudit tento kód žádnému ze známých autorů virů. Cíl přesměrování, webová stránka CoolWebSearch, naproti tomu skrývá celé množství materiálu pro spekulace. Jsou tam k dispozici dva obchodní modely: jeden pro zákazníky, zpravidla on-line obchody a jeden pro partnery. Zákaznický model má generovat příjmy tak, že si firmy koupí své místo v seznamu výsledků vyhledávání. Jako člen partnerského modelu lze naproti tomu dokonce vydělávat peníze: CoolWebSearch zaplatí provizi (pay-per-click) za každého uživatele, kterého přimějeme k tomu, aby tuto webovou stránku otevřel. Jak se to zařídí, zůstává na každém zvlášť.

3.1.3 Stealth networks

- neboli skryté sítě
- tento typ spyware zapojí počítač bez vědomí uživatele do síťového systému, který může sloužit k nejrůznějším účelům, jako např. peer-to-peer síť na sdílení souborů, distribuovaný výpočetní systém, distribuované úložiště nebo pro útoky typu DDoS.
- pravděpodobně nejrozšířenějším zástupcem je multimediální přehrávač b3d Projector společnosti Brilliant Digital Entertainment, který je instalován zároveň s aplikací Kazaa. Společnost tak může prodávat výpočetní zdroje uživatelských počítačů (volné místo na discích, procesorové cykly) dalším podnikům, kompenzace uživatelům ovšem není nijak stanovena ani garantována.

Přestože předchozí typy (adware a stealth networks) znamenají značná bezpečnostní rizika a často nejsou zcela legální, jejich cílem nebývá poškození uživatele nebo obohacování se přímo na jeho úkor. Následující typy spyware již ale nelegální jsou a jejich účelem je zprostředkovat útok na uživatelův počítač nebo přinést zisk přímo na úkor uživatele.

3.1.4 System monitors

- neboli monitory systému
- s jejich pomocí lze sledovat veškerou aktivitu počítače včetně stisku kláves (key loggers) či snímání obsahu obrazovky
- tento typ je nyní na vzestupu a to zejména díky rozvoji nejrůznějších plateb přes internet a internetovému bankovníctví. Narůstá tedy počet krádeží identity

(uživatelských jmen a hesel nebo tajných klíčů šifer), které vedou k neoprávněnému čerpání z účtů nebo přístupu k důvěrným informacím.

- jako příklad využití lze uvést ztráty společnosti Valve, když bylo v létě 2003 pomocí spyware získáno heslo zaměstnance a prostřednictvím něho ukradena část zdrojových a datových souborů právě vyvíjené hry Half Life 2, což podle některých přispělo k odložení vydání hry o rok a mělo významné obchodní a finanční následky nejen pro společnost Valve.

3.1.5 Dialer

- neboli podvodné vytáčení

- program či skript ActiveX, který se skrývá ve webových stránkách a je schopen přesměrovat telefonické připojení na placené (zpravidla zahraniční) linky. V poslední době se však některé dialery šíří i jako spustitelná příloha emailových zpráv.

- tento problém se týká jen vytáčených připojení (dial-up)

- Existují jakési poctivé dialery a dialery, které mají za úkol nic netušícího člověka připojeného na internet nachytat. “Legální” dialery dostatečně dopředu informují o tom, že dojde k přepojení na draze tarifovanou linku a k tomuto připojení vyžadují souhlas uživatele. Informují dostatečně zřetelně a jasně také o ceně připojení. “Nelegální” dialery mají za úkol nainstalovat se a přenastavit připojení v co největší tichosti. Tedy tak, aby si toho uživatel pokud možno vůbec nevšiml. Proč takové podvodné dialery neodhalí antivirová ochrana Vašeho počítače? Jednoduše proto, že podvodný a poctivý dialer od sebe nelze takto odlišit. Jestliže totiž neprojde sítím antivirového programu “nelegální” dialer, neprojde jím ani dialer “legální”. To je důvod, proč antivirové společnosti dávají ruce pryč od obou druhů z rizika soudních žalob firem poskytujících “legální” dialery.

- Podvodných přesměrování je několikero druhů. Záleží na dialeru, který toto přepojení provádí. Podvodné přesměrování je přepojení, při kterém nebyl uživatel řádně a dostatečně viditelně a jasně upozorněn, že bude přepojen na vyšší tarif. Uživatel tedy musí dát jasný souhlas s tím, že se vědomě na drahý tarif přepojuje.

První z druhů dialerů pracuje tak, že dojde k otevření určité webové stránky (využití určité služby) a do počítače se Vám nainstaluje dialer, který volání přesměruje. Po zavření stránky se připojení zase přepojí zpátky na normální tarif. Dá se obecně konstatovat,

že u těchto druhů podvodných přepojení nedochází k takovým škodám, neboť jen málo lidí má otevřenou jednu stránku několik hodin.

Pro Vaší peněženku je mnohem nebezpečnější jiný druh přesměrování. A to je ten, který přenastaví Vaše připojení k internetu, aniž by to mělo nějakou souvislost s návštěvou nějaké konkrétní webové stránky. Tzn. že na draze tarifované číslo jste přepojen, dá se říct, kdykoliv. Nejste tedy připojen jen ve chvíli, kdy otevřete určitou webovou stránku a odsouhlasíte (ať už vědomě, či nevědomě) přepojení. Dialer, který se Vám v tomto případě do počítače dostane, Vás může připojit prakticky kdykoliv. Ať už trvale, nebo v různých intervalech (tedy ať už při každém připojení, nebo například při každém třetím připojení apod.). Některé dialery Vás dokonce můžou připojit i ve chvíli, kdy ani připojení k síti internet neinicujete. Jen například ráno pustíte počítač, odskočíte si uvařit kávu, dialer Vás během toho připojí na linku ze zvýšených tarifem, Vy přijdete s uvařenou kávou a až do večera na počítači pracujete, aniž byste tušili, že každá minuta vás stojí např. 70Kč (podle ceníku Českého Telecomu z listopadu 2004 již existují čísla s tarifací 93Kč/min!). Spojení se ukončí až teprve vynutím počítače, nebo vytrhnutím kabelu telefonní linky ze zástrčky.

Při tomto druhu dialeru ani nemusíte vytáčené připojení k síti internet na svém počítači vůbec používat a ani ho nemusíte mít nainstalované. Jen stačí, aby jste na počítači měli modem připojený kabelem k telefonní lince. Dialer už za Vás vše ostatní udělá sám (koupil jste si např. ADSL - tedy nevytáčené připojení k internetu, ale svůj starý modem jste v počítači nechal a ani jste neodpojl kabel.).

Podvedený si přepojení vůbec nevšimne, protože většina “lepších“ dialerů Vám před přepojením vypne reproduktor modemu. Když se tedy vytáčí nové číslo, nic neslyšíte (při odpojení můžete maximálně zaslechnout lehké klapnutí). Po vytočení vše probíhá stejně, jakoby jste byli připojeni klasickým způsobem. Brouzdáte po normálním, klasickém internetu.

- Je vnucována obecně mylná představa, že k podvodnému dialeru můžete přijít jen na XXX stránkách. Je pravda, že na XXX stránkách a stránkách s nelegálním softwarem je obecně pravděpodobnost napadení větší, ale podvodný dialer se Vám může do počítače dostat prakticky kdekoliv a kdykoliv. Ať už prostřednictvím emailu, či brouzdáním po obyčejných webových stránkách.

3.1.6 Backdoor trojans

- neboli trojské koně
- jedná se o aplikace, které počítač “otevírají” (většinou běž vědomí uživatele) útočníkům - ať již samotná data v něm obsažená, či jako prostředek k dalším útokům na PC
- nejnebezpečnější skupina spyware
- útočníkovi dávají plnou kontrolu nad uživatelským počítačem a útočník tak může libovolně manipulovat s jakýmkoliv informacemi v počítači se všemi důsledky, které z toho vyplývají
- mezi nejčastější a nejznámější patří zejména BackOrifice a NetBus

3.1.7 Cookies

- jedná se o malé, obvykle textové soubory, které vznikají komunikací mezi www serverem a prohlížečem. Server při komunikaci s klientem (prostřednictvím prohlížeče) vytvoří soubor s informacemi o klientovi; tyto informace pak vyšle zpět ke klientovi, který si je může (či nemusí) uložit na svém pevném disku a zpřístupnit je serveru pokaždé při dalším připojení a komunikačním toku. Vznikly jako jeden z prostředků k překonání statické podoby webových stránek.

- v překladu znamenají „koláčky“ nebo spíše „sušenky“ a ty mohou být sladké, slouží-li ke zvýšení komfortu uživatele (umožňují nejjednodušší “osobní” nastavení zobrazení webových stránek), nebo mohou být pořádně “vypečené“, jsou-li zneužity.

- jsou nejstarším a nejčastějším mechanismem, který je využíván ke sledování uživatele. Spyware je zneužije k identifikaci uživatele, ke sledování stránek, které navštívil, a k sestavení profilu jeho “prohlížečích zvyků“ pro dodávání cílené reklamy, a proto bývá někdy zahrnován přímo do skupiny adware a označován Adware Cookies.

Jednou z cest, kterou se spyware dostává do systému, je instalace se softwarem, který uživatel vědomě ze své vůle instaluje kvůli jeho užitečnosti. V takovém případě uživatel dokonce souhlasí s instalací spyware potvrzením EULA (End User Licence

Agreement, Licenční smlouva s koncovým uživatelem). Spyware může být poté v počítači v podstatě legálně, a proto se také antivirové společnosti detekci a odstraňování spyware z velké části vyhýbají. Výrobci spyware často vsázejí na to, že většina uživatelů potvrzuje souhlas s EULA bez přečtení textu. A pro ty, kteří se o to alespoň pokusí, připraví pár dlouhých chvil tím, že smlouvy napíší velmi nesrozumitelně, obsáhle a plné zavádějících a matoucích informací. Ovšem ani nesouhlas s EULA nemusí uživatele ochránit. Například instalátor peer-to-peer sítě Grokster v případě, že uživatel nesouhlasí a v instalaci aplikace nepokračuje, spyware komponenty stejně nainstaluje. Nebo jako druhý příklad mohu uvést červ FriendGreet, který se dokonce šíří nenápadně se souhlasem uživatele. Rozesílá se emailem jako pohlednice od známého. Poté, co uživatel následuje odkaz v emailu, se instaluje ActiveX komponenta, která pro zobrazení pohlednice vyžaduje souhlas s EULA. Potvrzením EULA však uživatel souhlasí s odesláním pohlednice všem kontaktům ze svého adresáře.

Spyware je nejčastěji instalován s utilitami pro stahování souborů, jako jsou peer-to-peer sítě (Kazaa,...), s multimediálními přehrávači, hrami nebo s účetními software.

3.2 Dopady spyware

Důsledky přítomnosti spyware v počítači se co do závažnosti pohybují od přímých finančních ztrát až k téměř naprosté "internetové" ztrátě soukromí. Přímé finanční škody nejčastěji pramení z krádeže identity zprostředkované nějakým druhem System monitor či Backdoor trojan. U vytáčeného připojení k internetu škody pramení z přesměrovaných připojení díky dialerům.

Spyware také často úmyslně i neúmyslně (kvůli programovým chybám) otevírá cestu hackerským útokům, virům nebo červům. Počítač tak může být zneužit k rozesílání spamu nebo pornografie, k útokům typu DDoS a dalším. Hackerským útokem může dojít k úniku či modifikaci důležitých dat, a tak nepřímé finanční ztráty způsobené spyware mohou být i řádově vyšší než případné přímé ztráty.

Tvůrci spyware své produkty neoptimalizují, a tak bývají uživatelé postiženi snížením výkonu v důsledku obsazení zdrojů spyware a nestabilitou systému způsobenou chybami spyware a jeho nekompatibilitou. Tyto jevy se zvýrazní interakcí více spyware v jednom systému (podle výsledků projektu Spy Audit (viz výše), obsahuje každé PC průměrně 25

spyware!). Snížení výkonu se znatelně projevuje prodloužením startu systému (často i několikanásobným) a zpomalením odezvy systému i při běžném provozu.

Spyware může způsobovat také ztrátu produktivity práce. Uživatel je zdržován neustálým zavíráním pop-up oken, kvůli únosům Internet Exploreru má problémy dostat se k informacím, které ho zajímají, agresivní grafické prvky reklam jej vyrušují a odpoutávají jeho pozornost.

Také sledování zdánlivě anonymních uživatelských cest internetem může být považováno za vpád do soukromí. Podle navštívených stránek lze zjistit podrobné informace o zájmech uživatele, osobních či zdravotních problémech, sociální situaci a mnoha dalších privátních informacích.

3.3 Programy k odstranění spyware

Mnoho uživatelů si stále ještě plně neuvědomuje hrozbu, kterou představuje spyware, a tak velké procento počítačů dosud není zabezpečeno žádným softwarem proti němu. Přesto by program proti spyware měl být stejně samozřejmou součástí počítače, jako je firewall či antivirový program.

Programů na odstranění spyware je celá řada. Můžeme je dělit podle toho, zda jsou placené či nikoliv. Rozhodl jsem se věnovat pouze těm produktům, které se vyskytují v freeware, shareware nebo trialware verzích. Jak zjistíte, není jich zrovna málo a jsou častokráte výkonnější v boji se spyware než jejich placená konkurence.

Nástroje proti spyware pracují velmi podobně jako antivirový software a vyčistí všechno od cookies až po trojské koně. Jejich tvůrci identifikovali tisíce spyware souborů, složek a klíčů registru a tyto programy je hledají na Vašem hardware. Když je objeví, nabídnou možnost jejich odstranění.

Rozhodl jsem se vyzkoušet a porovnat 10 programů pro odstraňování spyware. Tyto programy jsem si nevybral náhodou, ale po důkladném prostudování problematiky díky jejich vysoké výkonnosti v boji se spyware a vysoké atraktivitě u uživatelů. Jinak freeware, shareware a trialware verzí jsem na různých serverech našel přibližně kolem jednoho sta.

Testovanými programy jsou:

- 1) Microsoft Antispyware Beta

- 2) Bazooka™ Adware and Spyware Scanner
- 3) AdAware SE Personal Edition 1.05
- 4) Spybot - Search & Destroy 1.3
- 5) Webroot Spy Sweeper 3.5
- 6) SpyRemover 2.33
- 7) SpywareBlaster 3.3
- 8) Spyware Doctor 3.2
- 9) CounterSpy 1.0.29
- 10) eTrust PestPatrol Anti-Spyware 4.4

V praktické části této práce, kterou jsem prováděl ve firmě XY, provedu u každého z nich důkladný test, porovnání mezi sebou a zhodnotím jejich výhody a vytknu nedostatky.

II. PRAKTICKÁ ČÁST

Praktickou část jsem prováděl ve firmě XY. Její skutečný název se v této práci nikde neobjeví, protože to byla jedna z podmínek naší spolupráce, na kterou jsem po konzultaci s vedoucím práce přistoupil. Jelikož zkoumaná tematika je velmi citlivá pro každou firmu, bylo velmi obtížné nalézt společnost, která by byla ochotna mi tato cenná data poskytnout. Po několika nezdarech se mi podařilo najít firmu, která za cenu naprosté anonymity byla ochotna se mnou spolupracovat.

Tato společnost byla založena v 1995 a zabývá se poskytováním vysoce profesionálních realitních služeb zejména v sektoru rezidencí, rodinných domů, rekreačního bydlení a bytů. V současné době pokrývá celou oblast Moravy. Firma zaměstnává 14 pracovníků, přičemž každý z nich vlastní minimálně přenosný počítač, v některých případech i počítač stolní. V sídle firmy mi vyšel vstříc zejména majitel společnosti, který mi umožnil provádět praktickou část mé práce na místním stolním počítači.

Svou praxi ve firmě XY jsem zahájil tím, že jsem se blíže seznámil s její bezpečnostní politikou. Firma si ji nechala zhotovit u externí firmy v roce 2002, avšak bez zainteresovanosti vlastních zaměstnanců, tudíž odchod know-how spojeného s projektem proběhl současně s odchodem posledního zaměstnance externí firmy z organizace. Vynaložené prostředky tedy nebyly využity zcela efektivně, protože BP se stala statickým dokumentem. Její statickost je nejvíce patrná u počítačové a komunikační bezpečnosti. Zatímco antivirová ochrana je na velmi vysoké úrovni, když firma používá produkt české společnosti Grisoft AVG7 v jeho nejaktuálnější verzi, ochrana před hrozbou spyware zcela chybí. Při konzultacích tohoto nedostatku s majitelem firmy jsem zjistil, že o této bezpečnostní problematice slyší vůbec poprvé. Rozhodl jsem se proto, že svou práci zaměřím zejména na tuto oblast problematiky, což bylo ještě umocněno příslibem majitele firmy XY, že výsledky a doporučení mé práce budou zahrnuty do BP organizace.

Přestože jsem se rozhodl blíže se věnovat počítačové a komunikační bezpečnosti, a to zejména ochraně před spyware, nenechal jsem si utéci možnost bližšího seznámení s celou BP.

Personální bezpečnost je podle mého názoru na dostačující úrovni, jelikož BP se dosti pečlivě věnuje podmínkám přijímání nových zaměstnanců firmy. Tito nejenže musí úspěšně zvládnout přijímací pohovor, ale musí též uspět v dalších částech přijímacího řízení. Mezi ně patří čistý trestní rejstřík a reference z dřívějších zaměstnání.

Oblast administrativní bezpečnosti a organizačních opatření, která je přímo závislá na bezpečnosti personální, tedy na tom, které pracovníky do firmy vybereme, je opět na vysoké úrovni. V rámci této kategorie jsou zaměstnanci seznamováni se zásadami bezpečné práce s výpočetní technikou, nebo též sankcemi za jejich nedodržování.

S fyzickou bezpečností informačního systému je to již poněkud horší, což vyplývá zejména z daného oboru činnosti firmy a z již uvedené skutečnosti, že její pracovníci používají většinou přenosné počítače a tudíž se zde nedají aplikovat standardní doporučení, jako jsou kvalitní bezpečnostní zámky či přístupy pomocí čipových karet do místností s počítači apod. Tento nedostatek by měl být minimalizován dodržováním striktních podmínek, jako je neponechávání přenosných počítačů bez dozoru například v automobilu nebo zákaz zálohování nešifrovaných dat na nosiče, které nelze uschovat do uzamykatelných zásuvek či trezorů. Dále by slabiny této kategorie informační bezpečnosti měly být sníženy důsledným dodržováním počítačové a komunikační bezpečnosti.

V praktické části této práce jsem se tedy zaměřil na otestování, popsání a porovnání deseti programů na odstraňování spyware. Toto mi bylo umožněno na stolním počítači v sídle společnosti. Jednalo se o počítač s procesorem AMD Athlon 2200+ a operační pamětí 512 MB. Pevný disk Seagate o velikosti 160 GB s 7200 ot./min. byl zaplněn různými daty z 60 % (tedy cca 95 GB). Podle zásad bezpečnostní politiky společnosti zde byl nainstalován operační systém Windows XP Professional SP2 a také antivirový program AVG 7 společnosti Grisoft, který je pravidelně aktualizován. Podle záznamů společnosti je počítač používán nepřetržitě po dobu 9 měsíců.

Nainstaloval jsem zde tedy postupně všech deset následujících programů:

- 1) Microsoft Antispyware Beta
- 2) Bazooka™ Adware and Spyware Scanner
- 3) AdAware SE Personal Edition 1.05
- 4) Spybot - Search & Destroy 1.3
- 5) Webroot Spy Sweeper 3.5
- 6) SpyRemover 2.33
- 7) SpywareBlaster 3.3
- 8) Spyware Doctor 3.2
- 9) CounterSpy 1.0.29
- 10) eTrust PestPatrol Anti-Spyware 4.4

Poznámka:

Avšak zde je nutno zmínit skutečnost, že ne všechny produkty, které se tváří, že vám chtějí pomoci, touto pomocí skutečně jsou. Mám na mysli řadu placených programů, které při bezplatném testu PC Vám nainstalují spyware. Tudíž přestože jste přesvědčeni o naprosté “čistotě” Vašeho počítače od spyware, ony vždy něco najdou. Důvod je samozřejmě jednoduchý: takové programy se lépe prodávají, když toho najdou více než konkurence.

Aby se Vám něco podobného nestalo a nenainstalovali jste si “anti-spyware darebáka” (v anglickém originále se pro tyto programy vžil název Rogue Anti-Spyware Applications), musíte být při výběru programů opatrní. Jejich tvůrci pro ně záměrně vybírají názvy velmi podobné kvalitním a známým produktům. Jako příklad lze uvést “darebáka” SpyDoctor, který má velmi podobný název jako renomovaný program Spyware Doctor od společnosti PC Tools. Pro začátek bych proto doporučil nestahovat žádnou utilitu bez zkontrolování seznamu potenciálně nebezpečných produktů na stránce http://www.spywarewarrior.com/rogue_anti-spyware.htm . Stránku zřídil Eric L.Howes jako reakci na množství se “anti-spyware darebáky” za podpory mnoha renomovaných firem (Javacool – tvůrce SpywareBlaster, Patrick M.Kolla – tvůrce SpyBot, ...). V době psaní této práce seznam obsahuje 185 objektů!

Jedním z takových programů je SpySpotter. Na své stránce <http://www.spyspotter.com/> Vám zdarma (což nezapomene několikrát zmínit a pořádně tuto informaci zvýraznit) nabídne test, který prověří Vaši diskovou jednotku. Avšak již po prvním kliknutí to začíná být podezřelé, jelikož Vás nutí stáhnout si malý instalační soubor přímo do PC. Poté začne probíhat instalace tolik dobrosrdečného programu, jakým je SpySpotter, při které se začne něco stahovat ze složky Windows/system32, což je ještě podezřelejší. Po ukončení instalace nabídne skenování disku. Program sice našel spyware, avšak jedná se částečně o “vlastní výrobu”, o kterou má být právě “lepší” než konkurence. Tímto se Vás snaží nalákat ke koupi plné verze, která dokáže nalezený spyware i odstranit. Pokud ale zároveň spustíte i jiný program, např. Spyware Doctor 3.2, nalezne spyware přímo v programu SpySpotter (o kterém se jaksí samotný SpySpotter zapomněl zmínit).

4 TESTOVANÉ PROGRAMY

4.1 Microsoft Antispyware Beta



Obr. 1 Náhled programu Microsoft Antispyware Beta

- Microsoft se snaží dávat do svého operačního systému všechny “základní programy“, a proto rozšířil své portfolio i o program proti spyware. Nejedná se o původní produkt společnosti Microsoft. Jde o produkt firmy Giant Software, kterou Microsoft koupil. Tato verze není plnou verzí, ale jde o tzv. Beta verzi. Její platnost vyprší 31.července 2005. Z toho se dá odhadnout, že nejpozději v půli května by měla přijít finální verze, tedy MS Antispyware 1.0.
- **Podporované operační systémy:** Windows 2000 / 2003 Server / XP
- **Minimální konfigurace:** procesor 300 MHz , 64 MB operační paměti, Internet Explorer 6.0, přístup na síť Internet s přenosovou rychlostí aspoň 28.8 Kbps na používání SpyNet™
- **Velikost souboru po nainstalování:** 14 MB

- **Instalace:** přivítá Vás samotný program a varuje ohledně autorských práv → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → provede se samotná instalace → okno oznamující úspěšné ukončení instalace s možností otevření průvodce nastavením.

Po spuštění nabízeného průvodce Vám jako první krok bude nabídnuta automatická aktualizace. Druhým krokem je nastavení rezidentního štítu. Zatřetí máte možnost připojit se ke SpyNet komunitě. V posledním kroku je možnost okamžitého spuštění skenování a také nastavení jeho pravidelného spuštění ve 2 hodiny v noci (modifikace času je možná později).

- **Nastavení:** Nastavení programu lze spustit přes *Options* v horní liště a poté *Settings*. Jako první je zde možnost nastavení automatické aktualizace a též času, kdy se má tato aktualizace provádět (po startu PC atd.). Lze zde též nastavit spouštění rezidentního štítu, blokování nebezpečných akcí, připojení ke komunitě SpyNet či zobrazování výsledků po provedení skenování. Pro nastavení rozšířených nástrojů musíte kliknout na ikonu *Advanced Tools* v pravém horním rohu, kde lze donastavit systémové nástroje (*System Explorers*, *Browser Hijack Restore*) jako například blokování prvků ActiveX, probíhajících procesů či programů spuštěných po startu Windows nebo též nastavit výchozí domovskou stránku a vyhledávač v IE. Položka *Advanced Tools* obsahuje též možnost vymazání historie činností v mnoha programech počítače (*Tracks Eraser*).
- **Popis:** Úvodní okno má příjemný vzhled a umožňuje zjištění stavu a nastavení nejdůležitějších funkcí programu. Pod horním okrajem se nachází lišta s možností ovládání celého programu pomocí nabídek *File*, *Options* a *Tools*. Avšak uživatelsky příjemněji se jeví možnost používání nastavení pomocí nabídek zobrazovaných přímo v okně programu. Toto úvodní okno lze rozdělit na tři části. Na celé levé části okna jsou zobrazeny nejdůležitější informace a nastavení, která lze po kliknutí na ně přenastavit. Je zde například informace o času posledního skenování a jeho výsledky, stav rezidentního štítu nebo stáří databáze spyware. V pravém horním kvadrantu se nacházejí tři hlavní funkce: možnost spuštění okamžitého testu (**Run Quick Scan Now**), nastavení rezidentního štítu (**Real-time Protection**) a rozšířené nastavení nástrojů programu (**Advanced Tools**), které je popsáno výše. Na horní liště lze pomocí položky *Help* snadno spustit přehlednou nápovědu.

Produkt nabízí speciální funkci SpyNet™, což je dobrovolná celosvětová komunita uživatelů produktu Microsoft AntiSpyware, která hraje významnou roli při určování, které podezřelé programy je možné klasifikovat jako spyware. Členem sdružení SpyNet™ se může stát kdokoli, kdo chce společnosti Microsoft oznamovat potenciální spyware. Členové globálního sdružení SpyNet™ napomáhají rychle objevovat nová ohrožení, takže zlepšují ochranu všech uživatelů. Pro programy označené jako spyware jsou vytvářeny signatury, které jsou poté k dispozici všem uživatelům. Pokud chcete používat SpyNet™, je potřeba přístup na síť Internet s přenosovou rychlostí alespoň 28,8 Kbps.

- **Funkce:**

- skenování → možnost odstranění
- rezidentní štít (59 aktivních bodů)
- nastavení domovské stránky a vyhledávače v IE
- plánovač skenování
- automatická aktualizace

4.2 Bazooka™ Adware and Spyware Scanner



Obr. 2 Náhled programu Bazooka™ Adware and Spyware Scanner

- Produkt společnosti Kephyr je sice zdarma, ale jedná se opravdu o pouhý skener. Na druhou stranu je to skutečně výkonný rychlík: během několika sekund dokáže zkontrolovat systém a zobrazit nalezené špiony. Za špiony považuje jen skutečně nebezpečný software, který shromažďuje a posílá informace. Pokud je test kladný, ukáže Vám webovou stránku s návodem jak daný spyware odstranit, jelikož sám touto funkcí není vybaven. Na druhou stranu to nahrává zkušeným uživatelům, kteří tak mohou mít plnou kontrolu nad tím, co vlastně s daným špionem udělat.
- **Podporované operační systémy:** Windows 95 / 98 / ME / NT / 2000 / XP
- **Minimální konfigurace:** neuvedeno
- **Velikost souboru po nainstalování:** 1,4 MB
- **Instalace:** nejprve zvolíte instalační jazyk (nabídka: angličtina, němčina, francouzština, ruština nebo španělština) → poté Vás přivítá samotný program a varuje Vás ohledně autorských práv → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → výběr názvu, pod kterým ho chcete mít uložen v nabídce programů → provede se samotná instalace
- **Nastavení:** Při prvním spuštění je Vám nabídnuto, že při zadání své emailové adresy, budete informováni o nových produktech společnosti (lze samozřejmě i odmítnout). V dalším kroku Vám program ukáže, jak zastaralou databázi vlastníte a nabídne okamžitou aktualizaci.
- **Popis:** Jedná se opravdu o velmi jednoduchý prográmek, který má v levé části menu, skládající se ze sedmi položek. **Scan** – slouží k samotnému skenování, které trvá přibližně 2 sekundy. **Update** – provedení potřebné aktualizace (frekvence je častá, avšak program neumožňuje její naplánování). **Generate log** – užívá se při selhání skeneru u některého spyware. Funkce vygeneruje informaci o systému a uloží do textového souboru. Zároveň Vás požádá o jeho zaslání na emailovou adresu support@kephyr.com, kde se pokusí závadu odstranit a aktualizovat databázi. Funkce **Help** obsahuje manuál programu. **Visit us** odkáže prohlížeč na stránky výrobce a **Support us** Vás poprosí o finanční podporu tvůrce. A posledním odkazem je **About**, což samozřejmě zobrazí údaje o verzi programu. Ve spodní části jsou ještě dva odkazy na domovskou stránku a stránku s databází spyware, která v okamžiku psaní této práce zahrnovala 566 položek.
- **Funkce:**
 - skenování

4.3 AdAware SE Personal Edition 1.05



Obr. 3 Náhled programu AdAware SE Personal Edition 1.05

- Firma Lavasoft, výrobce programu, má dlouholeté zkušenosti s bojem proti spyware. Celosvětově patří tento program mezi desítku nejstahovanějších programů a nejinak je tomu i v České republice.
- Program se nachází ve třech variantách:
 - AdAware SE Personal Edition
 - AdAware SE Plus Edition
 - AdAware SE Professional Edition

Tab. 2 Rozdíl mezi jednotlivými variantami AdAware

Vlastnosti	Personal (Freeware)	Plus	Professional
Cena (v USD)	-	26,95	39,95
Rozšířená databáze	✓	✓	✓
Základní parametry příkazového řádku	✓	✓	✓
Standardní verze plug-inů a nastavení	✓	✓	✓
Automatické skenování	✓	✓	✓
Plnohodnotná podpora karantény	✓	✓	✓
Vylepšení (optické konfigurace)	limitováno	✓	✓
Vylepšená bezpečnost zálohování	✓	✓	✓
Automatické blokování	✗	✓	✓
Blokování popup oken (pouze IE)	✗	✓	✓
Blokování Active X prvků	✗	✓	✓
Blokování útoků na prohlížeč a downloadů z IE	✗	✓	✓
Zákaznické skenování	✗	✓	✓
Monitorování Ad-watch 3.0 v reálném čase	✗	✓	✓
Ochrana registrů	✗	✓	✓
Rozšířené nastavení ochrany souborů	✗	✓	✓
Vylepšená schopnost loggování	✗	✓	✓
Free podpora e-mailem	✗	✓	✓
Rozšířené filtrování	✗	✓	✓
Tiskové zprávy	✗	✓	✓
Plug-iny a nastavení verze Plus	✗	✓	✓
Plug-iny a nastavení verze Professional	✗	✗	✓
Procesový manager / prohlížeč	✗	✗	✓
Dodatečné parametry příkazového řádku	✗	✗	✓
Dodatečné možnosti menu a exportu pro reporty	✗	✗	✓
Skenování sdílené sítě a ram disku	✗	✗	✓

Zdroj: www.officeplus.cz/adaware.php

- Test jsem prováděl s AdAware SE Personal Edition, který je freeware.
- **Podporované operační systémy:** Windows 98 / ME / NT4 / 2000 / 2003 / XP
- **Minimální konfigurace:** procesor Pentium 166, RAM: operační systém + 24 MB, Internet Explorer 5.5, 25 MB volného harddisku
- **Velikost souboru po nainstalování:** 3 MB
- **Instalace:** přivítá Vás samotný program a varuje ohledně autorských práv → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → dále možnost zpřístupnění k nastavení pouze pro administrátora nebo pro všechny → provede se samotná instalace → a nakonec okno s nabídkou tří možností: skenování celého systému, možnost aktualizace a otevření souboru s nápovědou. Označil jsem první 2 kroky a po zaktualizování

a provedení skenování vypínám program, abych mohl provést doinstalování češtiny, kterou lze zdarma stáhnout na www.cestiny.cz . Po rozbalení zazipovaného souboru spustíte soubor AdAwareSE105_CZ.exe a řídíte se pokyny v češtině na obrazovce (jde pouze o to, nastavit složku, kde se AdAware nachází). Nyní opět spustíte program a kliknete na obrázek ozubeného kola vpravo nahoře. Poté na ikonu *Interface* a nabídku *Language File* změňte na *Czech*. Vše potvrdíte stiskem *Proceed*. Nyní je již program plně počestěn.

- **Nastavení:** Po kliknutí na obrázek ozubeného kola (při najetí myši na jakoukoliv ikonu se zobrazí krátký popis funkce) se dostaneme do velmi přehledného a lehce nastavitelného menu. V levé části okna je 7 podmenu: Obecné, Skenování, Rozšíření, Po startu, Defaulty, Rozhraní, Tweaky.

V *Obecném* nastavení můžete zvolit úroveň zabezpečení, obecnou platnost definičního souboru (pak Vám program bude automaticky nabízet aktualizaci) či cestu k souborům. *Skenování:* zde můžete vybrat specifické jednotky, složky, paměť, registry a oblíbené položky IE pro skenování. *Rozšíření:* lze vybrat integraci do kontextového menu, Průzkumníka či další úrovně logování. Pod ikonou *Po startu* nelze v této freewarové verzi nastavit nic. V *Defaultním* nastavení můžete zafixovat domovskou a hledací stránku v IE. *Rozhraní:* zde můžete změnit vzhled programu výběrem jiného skinu či volbou jazyka. Pod ikonkou *Tweaky* lze detailněji donastavit program (vzhled programu, zabezpečení, ...)

- **Popis:** Úvodní obrazovka, která je velmi přívětivá a přehledná, obsahuje na levé straně pět funkcí: **Stav** – je současné neboli základní rozhraní. **Skenování** – umožňuje samotné čištění počítače. Lze si vybrat buď Chytrý, Plný systémový test, nebo pouze určité složky. Funkce **Ad-Watch** je dostupná až v placených verzích a taky **Pluginy** základní verze žádné neobsahuje. Poslední funkcí je samozřejmě nezbytná **Nápověda** pro případ potíží.
- **Funkce:**
 - skenování → možnost odstranění
 - nastavení výchozí domovské stránky a vyhledávače v IE

4.4 Spybot - Search & Destroy 1.3



Obr. 4 Náhled programu Spybot - Search & Destroy 1.3

- Produkt irského nadšence Patricka M. Kolly patří mezi nejoblíbenější vůbec. Jednak proto, že je zdarma, ale také proto, že má v sobě zabudováno 45 jazyků (včetně češtiny). Počet prvků v databázi je 14 230, což ale samozřejmě není konečné číslo, protože díky pravidelnému updatu (cca 1x týdně), počet prvků stále stoupá.
- **Podporované operační systémy:** Windows 95 / 98 / ME / NT / 2000 / XP
- **Minimální konfigurace:** neuvedeno
- **Velikost souboru po nainstalování:** 11,5 MB
- **Instalace:** nejprve zvolíte instalační jazyk (nabídka: angličtina, němčina, francouzština, italština nebo holandština) → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → poté možnost instalace doplňků (skinny a další jazyky) → výběr názvu, pod kterým ho chcete mít uložen v nabídce programů → následují možnosti umístění ikony na ploše, ikony v trayi či permanentní ochrany IE nebo nastavení systému → provede se samotná instalace → a na závěr možnost spuštění programu.

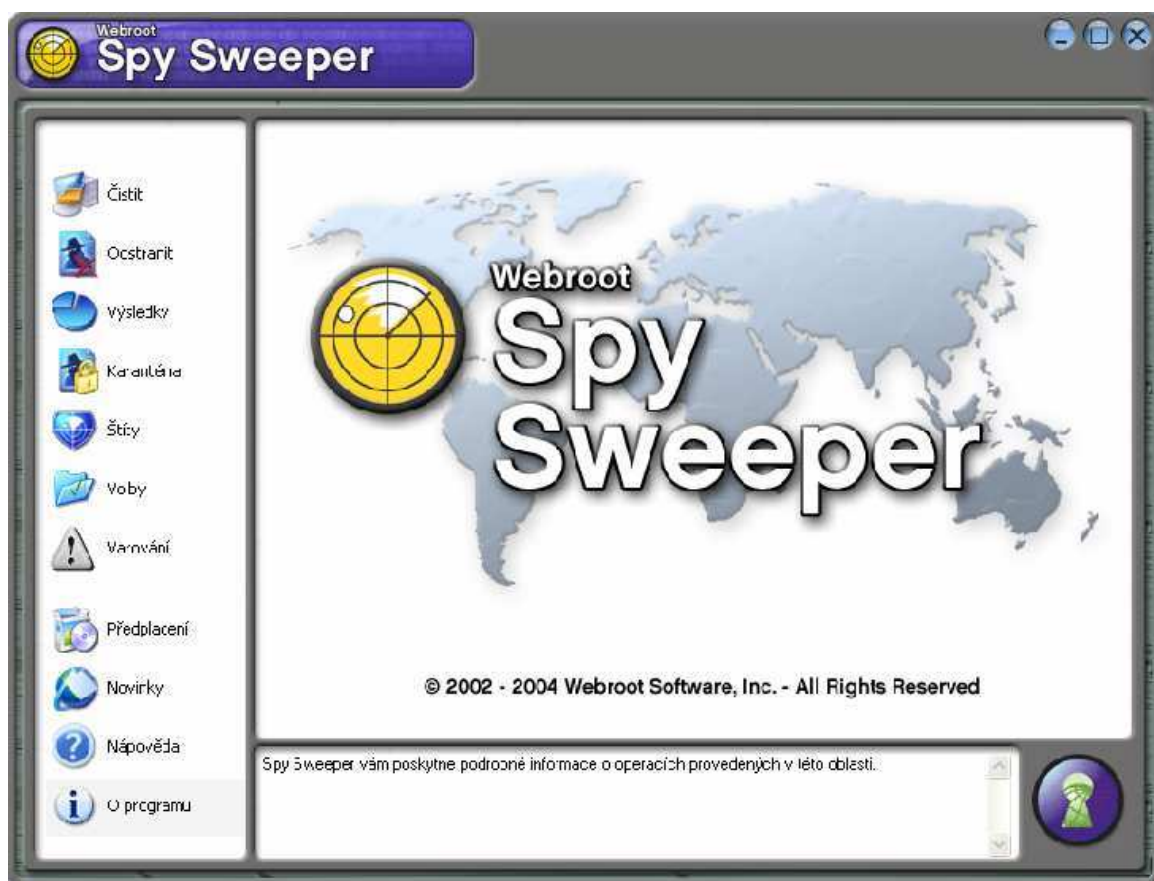
- **Nastavení:** Při prvním spuštění Vám program nabídne ve třech krocích snadné zaktualizování: V prvním kroku klepněte na tlačítko pro zálohu registru a tato operace může trvat dost dlouho, záleží na velikosti disku, takže vyčkejte, až šipka *Dále* opět zezelená a pak na ni klepněte. V druhém kroku klepněte na tlačítko pro aktualizaci programu. Ve třetím a posledním kroku, tlačítkem spustíte program. Po spuštění programu klepněte v nabídce na *Language* a vyberte Česky. Nastavovat se v programu nic nemusí. Pracovat můžete buď v prostředí základním, ze kterého provedete jednoduchý rychlý test, nebo v prostředí rozšířeném, kde si nastavíte mnoho zajímavých parametrů pro test. Například nastavením výjimek zajistíte, že pro Vás důležité programy, které mají určité agenty (u kterých jste si jisti, že jsou neškodní), se nebudou kontrolovat. Všechna tato nastavení jsou však poměrně náročná a pokud si nejste v této problematice jistí, doporučuji Vám provést kompletní test.
- **Popis:** Vše důležité je v levém menu, v němž si vybíráte podle ikoněk. V rozhraní pro pokročilé je menu rozděleno do 4 základních: SpyBot S&D, Nastavení, Nástroje, Info & Licence.

SpyBot S&D obsahuje nejdůležitější funkce *Search & Destroy* a *Aktualizace*, tudíž jsou rychle po ruce a léčení Vašeho počítače může proběhnout okamžitě. Dále je zde *Obnova*, která obsahuje seznam všech záloh, které program udělal při opravě problémů, a *Imunizace* sloužící k blokování nebezpečných webových stránek v internetovém prohlížeči, takže se může stát, že se nedostanete na některé stránky, většinou se jedná o Warez stránky a pokud na takovou stránku narazíte, SpyBot Vás na ni nepustí a prohlížeč většinou zablokuje. V **Nastavení** můžete přizpůsobit vlastní potřebě *Jazyk*, *Kategorii produktů*, *Nastavení* programu (není třeba měnit), *Adresáře*, *Skin*y, *Plánovač* (velmi cenná funkce – možnost naplánování kontroly) a také řadu výjimek. Při kliknutí na jednotlivé funkce je vše stručně a výstižně v horní části okna vysvětleno. Mezi **Nástroje** patří například *Skartovač*, *ActiveX* nebo *Domovská stránka* (zde lze snadno zrušit, pokud Váš prohlížeč napadl Hijacker). Posledním podmenu je **Info & Licence**, kde je obsažena *Licence*, *Poděkování* (zejména překladatelům do 45 jazyků), *Darování* a také *Statistika*. Tato funkce velmi přehledně ukazuje podrobnosti o nalezeném spyware (kolik a kdy nalezeno, kdy odstraněno).

- **Funkce:**
 - skenování → možnost odstranění
 - rezidentní štít

- nastavení výchozí domovské stránky a vyhledávače v IE
- plánovač skenování
- možnost obnovy
- automatická aktualizace

4.5 Webroot Spy Sweeper 3.5



Obr. 5 Náhled programu Webroot Spy Sweeper 3.5

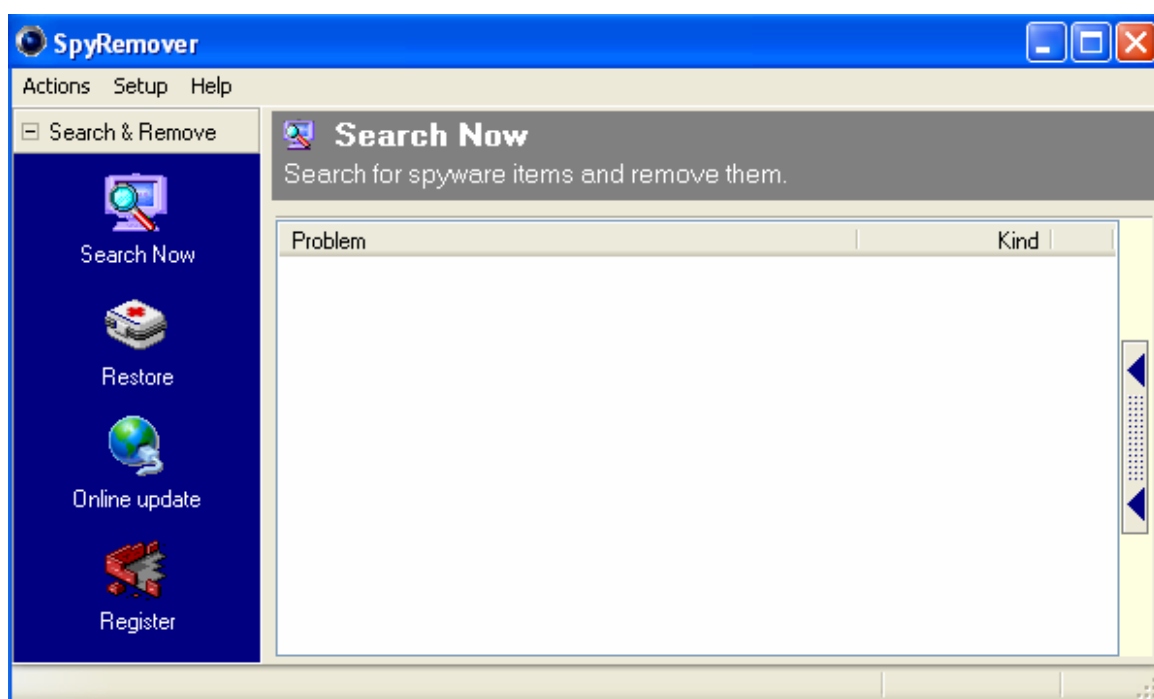
- Testovaná verze je pouze trialová na 30 dní, což znamená, po nainstalování si do 30 dnů musíme zaplatit verzi plnou (cena 29.95 USD), nebo program přestane fungovat. K tomuto kroku přistupují někteří výrobci, aby přesvědčili své potenciální zákazníky o kvalitách svého produktu. Programátoři společnosti Webroot se u současné verze naměřili zejména na rychlost a oproti předchozí 3.4 ji zvýšili o jednu třetinu.
- **Podporované operační systémy:** Windows 98 / ME / NT4 / 2000 / XP
- **Minimální konfigurace:** procesor 300 MHz , 64 MB operační paměti, 20 MB volného místa na disku
- **Velikost souboru po nainstalování:** 10 MB

- **Instalace:** přivítá Vás samotný program a oznámí, že se jedná pouze o 30-denní trialovou verzi → poté je požadován souhlas s licenčními podmínkami → následuje výběr typu instalace (ponechal jsem možnost typické) → nyní lze napsat svůj email s možností zasílání informací, tipů a triků k produktu → provede se samotná instalace → a nakonec okno s nabídkou spuštění programu a přečtení poznámek, zároveň pokud máte zapnutý internet se Vám načte stránka společnosti o úspěšné instalaci a s nabídkou koupě plné verze programu s licencí na 1 rok
- **Nastavení:** Při prvním spuštění Vám program nabídne zaktualizování databáze. Poté vypnu program, abych mohl provést doinstalování češtiny, kterou lze zdarma stáhnout na www.cestiny.cz . Po rozbalení zazipovaného souboru spustíte soubor s příponou exe a řídíte se pokyny v češtině na obrazovce (jde pouze o to, nastavit složku, kde se program nachází). Po opětovném spuštění je již program v češtině. Nastavení programu můžete provést pomocí položek **Štíty** a **Volby**. V prvně jmenované lze nastavit permanentní ochranu Internet Exploreru, programů ve Startup Windows i samotných Windows. Ve **Volbách** lze nastavit samotný program (spouštění se startem Windows, mazání položek Karantény po x dnech, provedení aktualizací, atd.), volby samotného čištění (registry, paměť, cookies, ...), plánovač čištění (možnost volby přesného dne nebo i opakování).
- **Popis:** Hlavní menu je opět na levé straně okna a skládá se z 11 položek. Při spuštění kterékoliv z nich se objeví v dolní části programu krátké vysvětlení jeho funkce. Tedy pod položkou **Čistit** nalezneme možnost spuštění testu počítače. Po nalezení spyware se pomocí tlačítka **Další** přesuneme k druhé položce **Odstranit**, ve které se můžete blíže podívat na jednotlivé druhy a umístění nalezeného spyware a také jej odstranit. Dalším krokem jsou **Výsledky**, kde se v podobě souhrnu či protokolu přehledně zobrazí závěry testu (počet nalezených, ignorovaných, smazaných položek). Čtvrtou položkou je **Karanténa**, kam můžeme některé druhy spyware vložit. Patou (**Štíty**) a šestou (**Volby**) položku jsem popsal v nastavení programu (viz výše). Další je **Varování**, kde Vás program upozorní na nepovolené změny systému. Osmou položkou je **Předplacení**, což je vlastně objednání si plné verze ze stránek výrobce. Devátou jsou **Novinky**, kde Vám radí pomocí tipů a triků jak na spyware. Předposlední je nezbytná **Nápověda** a poslední **O programu** Vám udá informace počtu dní do vypršení trialové licence a také o verzi programu a databáze.

- **Funkce:**

- skenování → možnost odstranění
- rezidentní štít
- nastavení domovské stránky a vyhledávače v IE
- plánovač skenování

4.6 SpyRemover 2.33

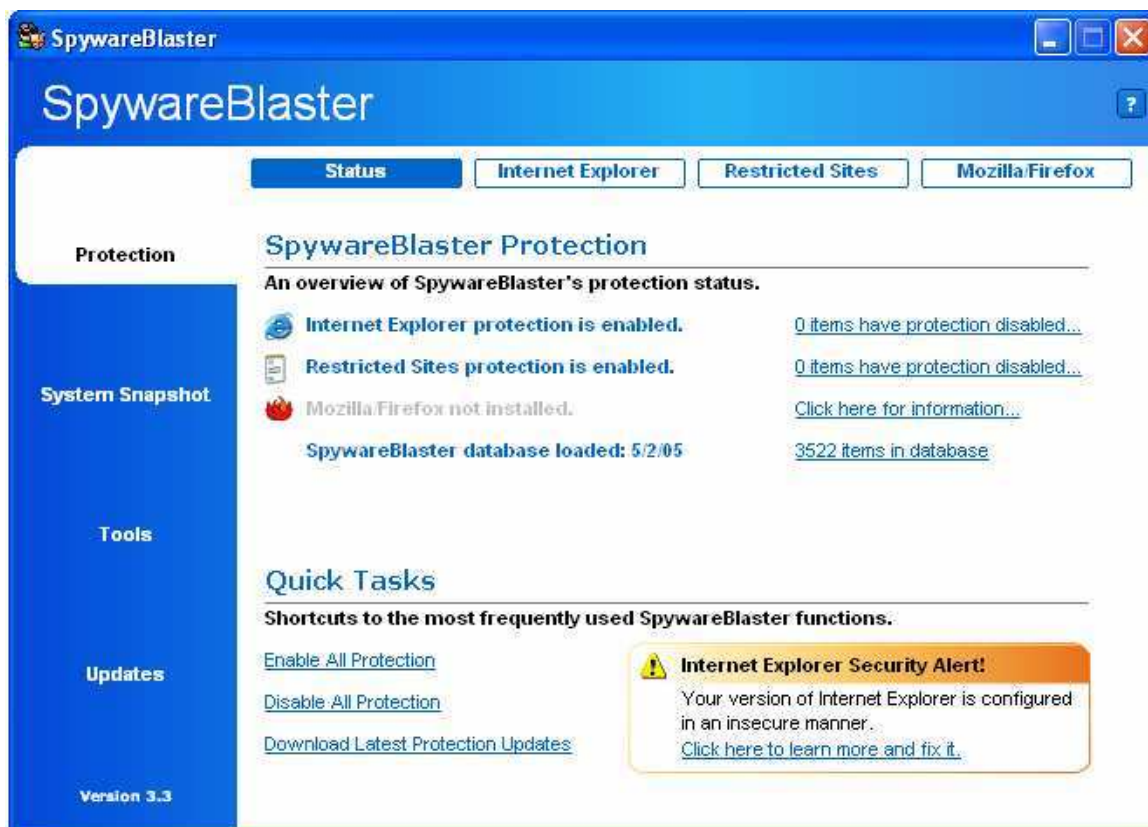


Obr. 6 Náhled programu SpyRemover 2.33

- Program, dokáže podle svého výrobce InfoWorks Technology Company detekovat a odstranit více 24 800 různých druhů spyware ve více jak 36 000 variantách. Testovaná verze je pouze shareware, který sice spyware vyhledá, avšak pro jeho smazání je potřeba plná verze, která stojí 29.95 USD.
- **Podporované operační systémy:** Windows 95 / 98 / ME / NT / 2000 / XP
- **Minimální konfigurace:** neuvedeno
- **Velikost souboru po nainstalování:** 8,3 MB
- **Instalace:** přivítá Vás samotný program → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → možnost změny názvu složky, pod kterou bude v nabídce Start → provede se samotná instalace → okno oznamující úspěšné ukončení instalace s možností otevření licenčních podmínek

- **Nastavení:** Nastavení se provádí přes Setup – Settings v horní liště. Lze zde nastavit automatické spuštění po startu PC, rezidentní ochranu, prioritu skenování či zvuky programu.
- **Popis:** Svým designem velmi připomíná Spybot - Search & Destroy, či spíše je jeho přesnou kopií. Výrobci si zřejmě ušetřili námahu s vlastním vývojem a nechali se inspirovat tímto známým freewarem. Avšak má o mnoho méně funkcí než on. K ovládání programu lze použít horní lištu či hlavní menu sestávající se ze 4 částí. První provede okamžitou kontrolu (**Scan Now**). Druhá obnoví systém (**Restore**), avšak pokud tato verze nedokáže nic smazat, není taky co obnovovat. Třetí je aktualizace programu (**Online update**). Poslední položkou je zakoupení plné verze (**Register**).
- **Funkce:**
 - skenování
 - rezidentní štít

4.7 SpywareBlaster 3.3



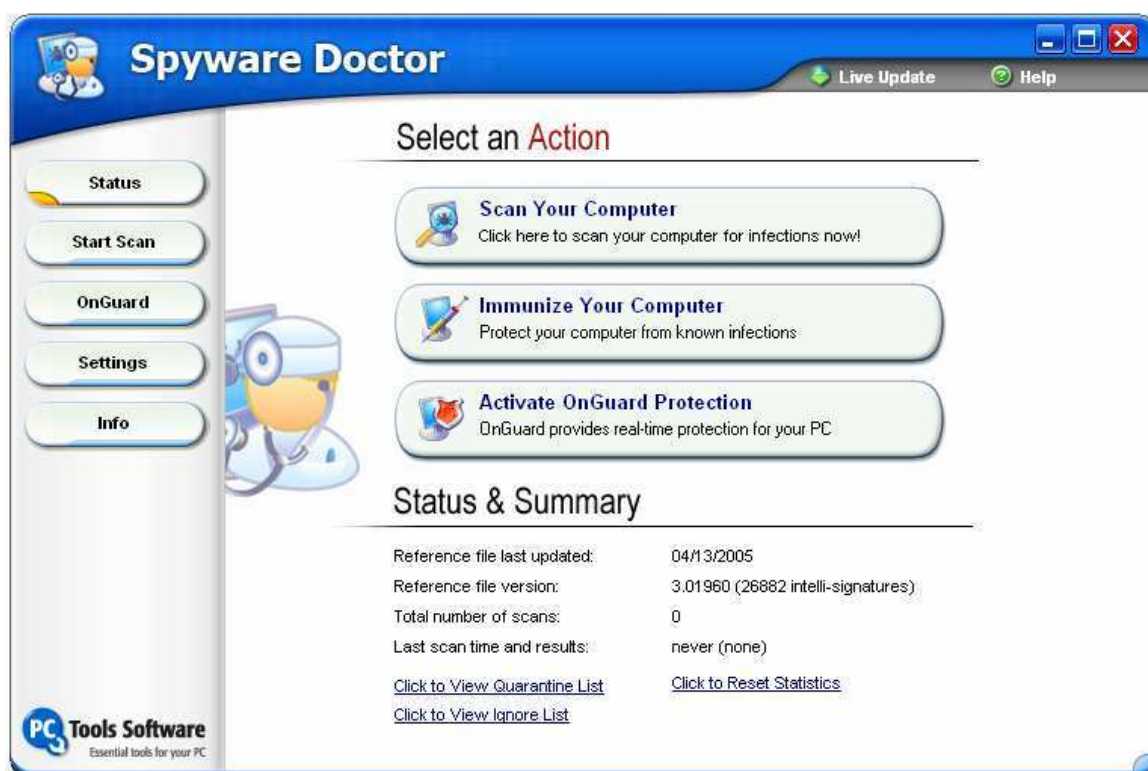
Obr. 7 Náhled programu SpywareBlaster 3.3

- Jeho hlavním úkolem je vypnout spyware ovládací prvky ActiveX. Nepracuje tedy jako většina ostatních programů, které se specializují na odstranění a odhalení škodlivých kódů v PC. Místo toho “hlídá” na vstupní bráně ze sítě (včetně internetu) a nedovolí ActiveX prvkům vstup do systému. Toho dosáhne vyřazením CLSID prvků, které používá spyware. Jde tedy o jakýsi druh prevence proti nakažení. Hlavní součástí programu je databáze známých ActiveX škůdců. Jedná se sice o freeware, ale pokud zaplatíte necelých 10 USD, získáte automatickou aktualizaci databáze.
- **Podporované operační systémy:** Windows 95 / 98 / ME / NT / 2000 / XP
- **Minimální konfigurace:** neuvedeno
- **Velikost souboru po nainstalování:** 3,4 MB
- **Instalace:** přivítá Vás samotný program → poté je požadován souhlas s licenčními podmínkami → následuje stránka s informacemi o programu → poté možnost výběru složky, kam se má program nainstalovat → možnost umístění ikony programu na plochu → provede se samotná instalace → a nakonec okno s nabídkou spuštění programu
- **Nastavení:** Při prvním spuštění se objeví okno se třemi kroky, které mají pouze informativní charakter: zaprvé popsání místa, kde je možno zapnout všechna krytí → zadruhé zdůraznění nutnosti provádění aktualizací → a zatřetí poděkování za používání SpywareBlaster a odkaz na jejich stránky pro případ problémů.
- **Popis:** Vzhledově úvodní stránka nepůsobí moc přívětivě, ale na druhou stranu poskytuje nejdůležitější funkce pohromadě. V levé části okna je 5 položek menu, přičemž nyní se nacházíme na první z nich - **Protection**. Tato položka se dělí na 2 části: v horní části můžete nastavit jednotlivé ochrany zvlášť, jedná se zaprvé o zablokování známých nebezpečných prvků ActiveX a zadruhé o zablokování cookies ze stránek obsahující spyware, nebo dole pomocí “rychlých úloh“(Quick Tasks) tyto dvě funkce můžete spustit najednou (Enable All Protection). Je zde též možnost stáhnutí nejnovější aktualizace, což také umožňuje čtvrtá položka hlavního menu – **Updates**. Druhou položkou menu je **System Snapshot**, který zálohuje a obnovuje systém. Třetí položkou hlavního menu jsou “nástroje“(Tools), kde lze nastavit výchozí domovskou stránku, výchozí vyhledávač, spouštění Macromedia Flash v IE nebo si můžete vytvořit vlastní list prvků ActiveX, které chcete blokovat. Poslední položkou je **Version 3.3**, na které lze získat informace

o výrobci, verzi nebo systému. A na závěr je zde opět možnost pomoci, která se skrývá pod ikonkou otazníku v pravém horní rohu.

- **Funkce:**
 - rezidentní štít blokování prvků ActiveX a cookies
 - možnost obnovy
 - nastavení výchozí domovské stránky a vyhledávače v IE
 - zjištění systémových informací

4.8 Spyware Doctor 3.2



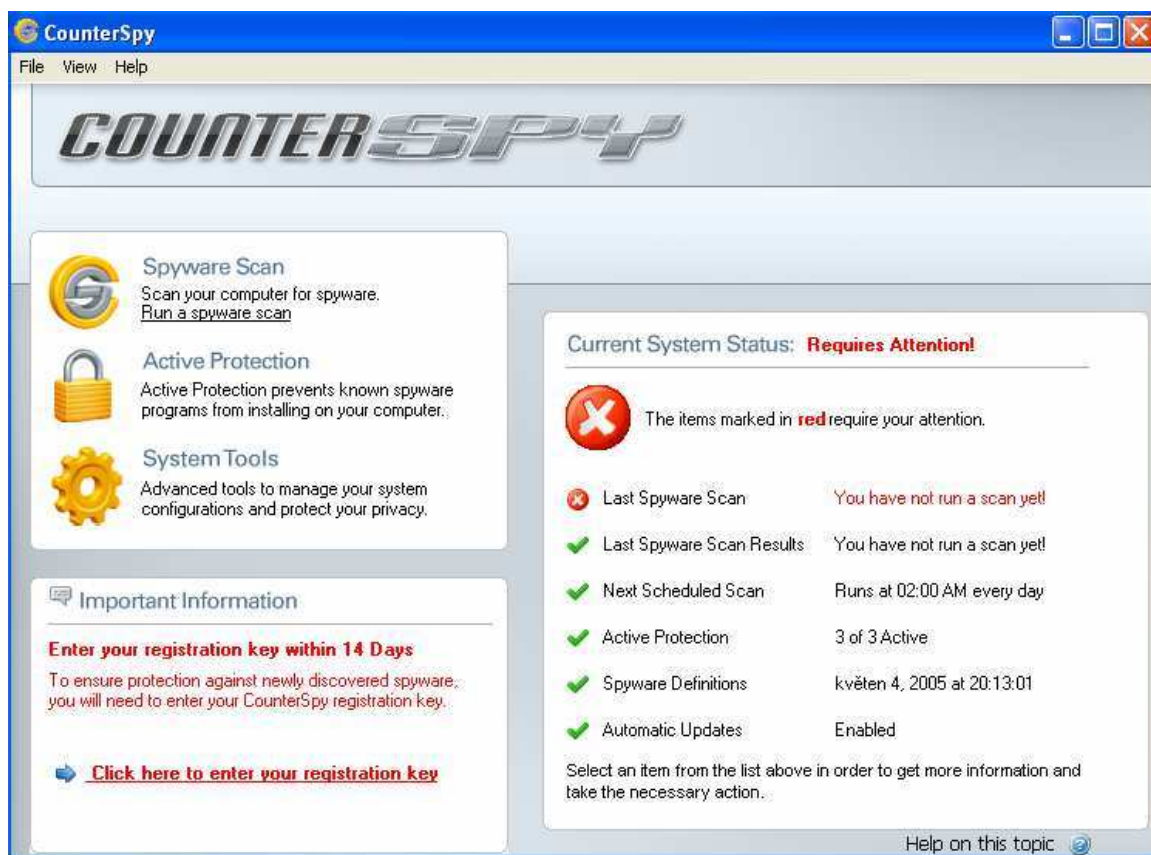
Obr. 8 Náhled programu Spyware Doctor 3.2

- Uživatelsky příjemný program, vyhledává různé druhy spyware (v databázi více než 25 000 prvků). Testovaná verze, která je časově omezena (15 dní), neumožňuje některé funkce jako rezidentní štít. Ty jsou až v registrované verzi za 39.95 USD.
- **Podporované operační systémy:** Windows 95 / 98 / ME / 2000 / XP
- **Minimální konfigurace:** procesor 486, 20 MB operační paměti, Internet Explorer 5.5, 16 MB volného místa na disku
- **Velikost souboru po nainstalování:** 11 MB

- **Instalace:** nejprve zvolíte instalační jazyk (nabídka: angličtina, němčina, španělština) → přivítá Vás samotný program → poté je požadován souhlas s licenčními podmínkami → následuje možnost výběru složky, kam se má program nainstalovat → poté je zde možnost doinstalování Registry Mechanic trial, což je prográmeček od stejného výrobce, který opravuje chyby v registrech Windows → následují možnosti umístění ikony na ploše, ikony v trayi či spuštění programu při startu Windows → provede se samotná instalace → a na závěr možnost spuštění programu a provedení testu
- **Nastavení:** Nastavení programu lze pomocí ikony Settings v hlavním menu, které se dále větví na *General* (možnost nastavení jazyka, výchozího skenování, přehrání zvuků, ...), *Log* (možnost shlédnutí výsledků předchozích testů), *Startup* (spouštění při startu Windows) a *Live Update* (automatická aktualizace – funkce nyní nedostupná).
- **Popis:** Úvodní obrazovka působí přehledně a jednoduše. Hlavní menu se opět nachází na levé straně okna, přičemž se skládá z 5 položek. Hned ta první - **Status**, na které se nyní nacházíte, umožňuje zahájit 3 nejdůležitější funkce: skenování, imunizaci a aktivaci rezidentního štítu (*OnGuard Protection*). V testované trialové verzi však funguje pouze skenování PC, které lze provádět ve třech úrovních (rychlý, kompletní a uživatelský). U placené verze imunizace plní funkci ochrany před spuštěním nechtěných prvků ActiveX při surfování Internetem a rezidentní štít neustále kontroluje Váš systém a zkoumá nezvyklé chování programů. Druhou položkou hlavního menu je **Start Scan**, který umožňuje okamžité spuštění skenování. Třetí je **OnGuard**, neboli rezidentní štít, ten je však v této verzi nedostupný. čtvrtou položkou je nastavení – **Settings** (viz výše). Poslední ikonka **Info** umožňuje on-line registraci produktu.

V pravém horním rohu programu se nacházejí ikonky pro aktualizaci (*Live Update*) a nápovědu (*Help*).
- **Funkce:**
 - skenování → možnost odstranění

4.9 CounterSpy 1.0.29



Obr. 9 Náhled programu CounterSpy 1.0.29

- U nás téměř neznámý produkt společnosti Sunbelt Software, který je sice novinkou v oboru, ale v poslední době sklízí nemalé úspěchy. V dubnu 2005 vyhrál test časopisu PCWorld o nejlepší odstraňovač spyware.
- **Podporované operační systémy:** Windows 98 SE / ME / 2000 / 2003 / XP
- **Minimální konfigurace:** procesor 300 MHz , 64 MB operační paměti, Internet Explorer 5.5, 24 MB volného místa na disku, přístup na síť Internet s přenosovou rychlostí aspoň 28.8 Kbps na používání ThreatNet
- **Velikost souboru po nainstalování:** 16,5 MB
- **Instalace:** přivítá Vás samotný program → poté je požadován souhlas s licenčními podmínkami → následuje stránka s informacemi o programu → poté možnost výběru složky, kam se má program nainstalovat → provede se samotná instalace → a nakonec okno oznamující úspěšnou instalaci s tím, že je potřeba restart počítače
- **Nastavení:** Poté se automaticky zahájí aktualizace databáze programu, který mezitím běží na pozadí a má aktivní ikonu v trayi. Po ukončení aktualizace spustíte program

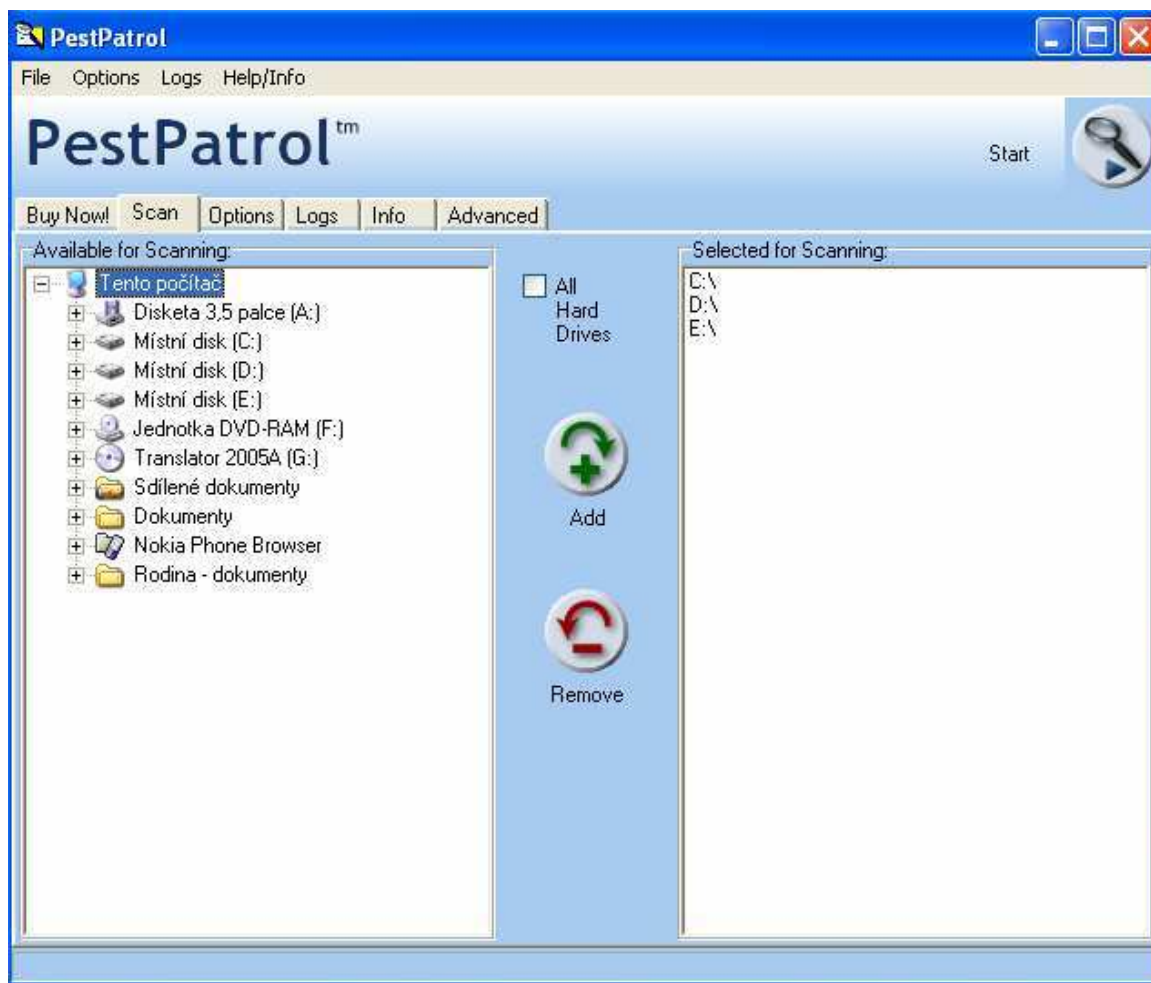
a přivítá Vás průvodní seznámení sestávající se z několika kroků: zaprvé je zde možnost zapsání registračního klíče (který si lze koupit za 19.95 USD na rok) nebo pokračujete dále, čímž se program stává trialovou verzí s omezením na 15 dní → dále zvolíte, zda chcete, aby program automaticky stahoval nejnovější aktualizace → poté máte možnost zapnout rezidentní štít a kde se bude počítač rezidentně chránit → v následujícím kroku se můžete stát členem společnosti ThreatNet, což je obdoba SpyNet™ u Microsoft AntiSpyware (viz výše) → posledním krokem je možnost spuštění skenování a nastavení každodenního testu.

Nastavení programu lze provést přes ikonu System Tools umístěnou na úvodní obrazovce. Nachází se zde 4 hlavní funkce: první z nich je *My PC Explorer*, kde lze přizpůsobit počítač svým potřebám (např. blokování prvků ActiveX, probíhajících procesů či programů spuštěných po startu Windows). Druhá funkce umožňuje zálohu celého systému (*My PC Checkup*). Poslední 2 funkce jsou pro mazání historií v systému (prohlédnutých stránek v IE, spuštěných souborů v MS Word, ...) a mazání jakékoliv souboru v počítači.

- **Popis:** Úvodní obrazovka působí příjemně a ve stylu Windows. Pod horním okrajem se nachází lišta nástrojů (*File, View, Help*), pomocí níž lze ovládat celý program, avšak uživatelsky příjemnější způsob je pomocí hlavního menu. To se nachází v levém horním kvadrantu okna a obsahuje test systému (Spyware Scan), rezidentní štít (Active Protection) a systémové nástroje (System Tools). V levém dolním kvadrantu úvodního okna se nachází informace o počtu dní do vypršení licence s možností okamžité registrace programu. Pravou část okna zabírá panel nejdůležitějších jednotlivých funkcí a informací o programu. Lze zde vyčíst, kdy byl proveden poslední test a jeho výsledky, jak je stará databáze spyware. Je tu možnost naplánovat pravidelné spuštění testu, rezidentní štít či nastavit automatické aktualizace. Díky tomu se stává program velmi jednoduše ovladatelný a přehledný. Pokud spustíme jakoukoliv položku hlavní menu, toto menu se nám neztratí, ale přesune se do horní části okna a přibudou k němu ikony umožňující návrat na úvodní obrazovku (*Home*) a ikona s možností vrácení se o krok zpět (*Back*), což také přispívá k lepší orientaci v programu.
- **Funkce:**
 - skenování → možnost odstranění
 - rezidentní štít (56 aktivních bodů)

- nastavení domovské stránky a vyhledávače v IE
- plánovač skenování
- automatické aktualizace
- možnost úplného smazání libovolného souboru

4.10 eTrust PestPatrol Anti-Spyware 4.4



Obr. 10 Náhled programu eTrust PestPatrol Anti-Spyware 4.4

- Testovaná verze je shareware, který má všechny funkce jako placená verze (39.95 USD) až na tu nejdůležitější – odstranění nalezeného spyware.
- **Podporované operační systémy:** Windows 98 / ME / NT / 2000 / 2003 / XP
- **Minimální konfigurace:** neuvedeno
- **Velikost souboru po nainstalování:** 6,3 MB
- **Instalace:** přivítá Vás samotný program a varuje ohledně autorských práv → poté je požadován souhlas s licenčními podmínkami → provede se samotná instalace →

nutnost vyplnění jména, příjmení a emailové adresy s možností zatrhnutí posílání novinek o PestPatrol → program spustí aktualizaci

- **Nastavení:** Ikona *Options* umožňuje nastavení programu. Podmenu se skládá ze sedmi položek. První nastavuje kde hledat (*Where to Search*), druhá co hledat plus krátký popis všech hledaných druhů (*What to Search for*) a třetí co vynechat při skenování (*What to Exclude*). Čtvrtá položka *Automatic Scans* umožňuje nastavení automatického skenování například při bootování PC nebo zahrnutí možnosti skenování složek kdekoliv při stisku pravého tlačítka ve Windows. Pátou položkou *Interface* upravujeme samotný vzhled programu (např. styl, velikost a barvu písma). Šestá záložka podmenu *Updates* nastavuje aktualizace a poslední *Help Wanted* poskytuje pomoc v nesnázích.
- **Popis:** Úvodní obrazovka, která je zároveň druhou položkou menu (**Scan**), umožňuje výběr a okamžité spuštění skenování. V pravém horním rohu okna je ikona dostupná z libovolného místa v programu a umožňuje okamžité skenování PC. Samotné hlavní menu se skládá z šesti položek a je nezvykle umístěno horizontálně ve formě záložek. První položkou je **Buy Now!**, která umožňuje registraci programu. Druhou a úvodní při spuštění je již zmiňovaný **Scan**. Třetí položkou je nastavení (**Options**), které již bylo popsáno výše. Čtvrtá položka označená jako **Log** umožňuje přehledný výpis výsledků jednotlivých skenování. Další položkou menu je **Info** poskytující informace nejen o verzi programu a databáze, ale též o všech hledaných prvcích databáze. Poslední položkou menu je **Advanced**, kde lze získat informace o právě spuštěných programech a registrech nebo podrobnosti o cookies. Zajímavou funkcí je možnost zanalyzování libovolného souboru v PC.
- **Funkce:**
 - skenování
 - rezidentní štít
 - zjištění systémových informací
 - plánovač skenování

Po tomto bližším seznámení s jednotlivými programy jsem přistoupil k samotnému testu jejich výkonnosti, přičemž jeho výsledky jsou v následujících tabulkách (Tab.3) a (Tab.4).

5 POROVNÁNÍ PROGRAMŮ

Tab. 3 Porovnání programů - část 1

Název	Microsoft Antispyware Beta	Bazooka™ Adware and Spyware Scanner	AdAware SE Personal Edition 1.05	Spybot Search & Destroy 1.3	SpySweeper 3.5
Výrobce	Microsoft	Kephyr	Lavasoft	Patrick M.Kolla	Webroot Software
WWW	www.microsoft.com/ cze/security/spyware	http://www.kephyr.com/s pywarescanner/	http://www.lavasoft.de/ ms/index.htm	http://www.safer- networking.org/	www.adwarereport.com/ webroot.html
Varianta	beta (zatím freeware)	freeware	freeware	freeware	trialware (30 dní)
Cena plné verze	?	-	-	-	29.95 USD
Vyhledávací engine (35%)	84	45	93	80	96
Ovládání (15%)	85	90	95	90	95
Rychlost (15%)	75	100	83	92	70
Podpora (15%)	95	85	90	85	85
Další funkce (10%)	90	0	75	90	85
Poměr cena/výkon (10%)	100	100	100	100	85
Vyhledávání					
Doba hledání (min:s)	6:02	0:02	4:50	2:43	8:06
Nalezeno spyware	93	7	145	74	161
Adware	✓	✓	✓	✓	✓
Dialery	✓	✓	✓	✓	✓
Trojské koně	✓	✓	✓	✓	✓
Cookies	✗	✗	✓	✓	✗
Funkce					
Rezidentní štít	✓	✗	✗	✓	✓
Autom. aktualizace	✓	✗	✗	✓	✗
Odstranění	✓	✗	✓	✓	✓
Různé typy testů	✓	✗	✓	✗	✓
CELKOVÉ HODNOCENÍ	87	67	90	87	88

Tab. 4 Porovnání programů - část 2

Název	SpyRemover 2.33	SpywareBlaster 3.3	Spyware Doctor 3.2	CounterSpy 1.0.29	Pest Patrol 4.4
Výrobce	InfoWorks Technology Company	Javacool Software LLC	PC Tools	Sunbelt Software	Computer Associates
WWW	http://www.itcompany.com/remover.htm	http://www.javacoolsoftware.com/	https://www.pctools.com/spyware-doctor/	http://www.sunbelt-software.com/	www.pestpatrol.com
Varianta	shareware	freeware	trialware (15 dní)	trialware (15 dní)	shareware
Cena plné verze	29.95 USD	-	39.95 USD	19.95 USD	39.95 USD
Vyhledávací engine (35%)	80	0*	89	94	81
Ovládání (15%)	70	85	90	90	85
Rychlost (15%)	95	0*	89	63	80
Podpora (15%)	55	75	90	95	85
Další funkce (10%)	50	85	40	95	85
Poměr cena/výkon (10%)	75	100	75	90	65
Vyhledávání					
Doba hledání (min:s)	1:23	0:00*	2:59	12:12	5:29
Nalezeno spyware	75	0*	111	151	82
Adware	✓	✓	✓	✓	✓
Dialery	✓	✓	✓	✓	✓
Trojské koně	✓	✓	✓	✓	✓
Cookies	✓	✓	✓	✓	✓
Funkce					
Rezidentní štít	✓	✓	✗	✓	✓
Autom. aktualizace	✗	✗	✗	✓	✗
Odstranění	✗	✗	✓	✓	✗
Různé typy testů	✗	✗	✓	✓	✓
CELKOVÉ HODNOCENÍ	74	85	83	89	81

* - program SpywareBlaster 3.3 je založen na jiném principu eliminace spyware než ostatní. Program kontroluje data přímo při vstupu do počítače, poté již nikoliv.

5.1 Způsob hodnocení

5.1.1 Vyhledávací engine

- Váha této kategorie: 35 %
- Jedná se zejména o to, kolik spyware program našel

5.1.2 Ovládání

- Váha této kategorie: 15 %
- Šlo především o přehlednost a snadnost ovládání. Kladné body získal program s lokalizací češtiny nebo s přehledným a intuitivním ovládáním. Naopak záporné pokud k samotnému spuštění testu se muselo provést několik kroků.

5.1.3 Rychlost

- Váha této kategorie: 15 %
- Jedná se o čas potřebný k prozkoumání diskové jednotky (95 GB). Pokud program umožňoval více úrovní testu, zvolil jsem tu nejpodrobnější variantu.

5.1.4 Podpora

- Váha této kategorie: 15 %
- Hodnotil jsem zejména frekvenci aktualizací. Pokud program umožňoval automatické aktualizace, získával kladné body. Ku prospěchu také bylo, když nápověda byla srozumitelná a přehledná.

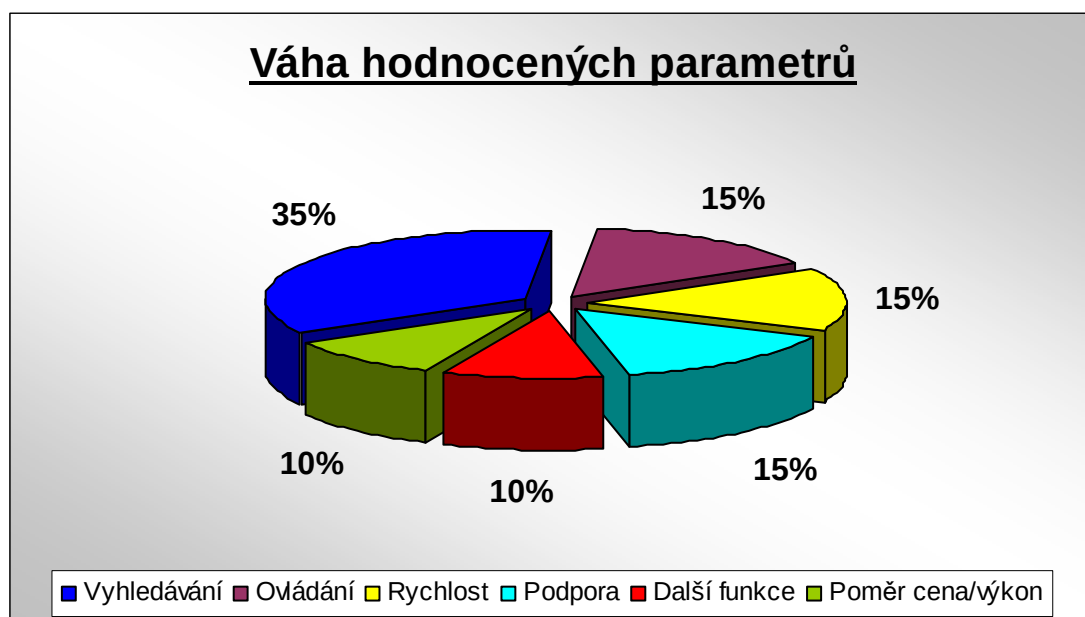
5.1.5 Další funkce

- Váha této kategorie: 10 %
- Jedná o vše, co programy obsahují navíc. Patří sem rezidentní štíty v testovaných verzích, různé přehledy a statistiky, možnost obnovy systému, přehled systémových informací, možnost nastavení domovské stránky a vyhledávače, plánovač skenování

5.1.6 Poměr cena/výkon

- Váha této kategorie: 10%
- = kolik toho za své peníze dostanete

- pokud se jedná o trialware, bere se u této kategorie v úvahu cena roční licence



Obr. 11 Procentní podíl hodnocených parametrů

6 VÝSLEDKY TESTU A ZHODNOCENÍ PROGRAMŮ

1) Microsoft Antispyware Beta

Celkové hodnocení: 87 bodů

Klady: detekce a odstranění spyware, automatická aktualizace, mnoho dalších nástrojů pro ovládání PC (mazání souborů historie, informace o spuštěných procesech počítače atd.)

Zápory: Beta verze, která se po 31.7.2005 jistě stane verzí placenou

2) Bazooka™ Adware and Spyware Scanner

Celkové hodnocení: 67 bodů

Klady: rychlost skenování

Zápory: nemožnost odstranění nalezeného spyware, žádné další funkce

3) AdAware SE Personal Edition 1.05

Celkové hodnocení: 90 bodů

Klady: možnost stáhnutí češtiny, rychlé a kvalitní skenování, intuitivní ovládání

Zápory: rezidentní štít dostupný až placených verzích

4) Spybot - Search & Destroy 1.3

Celkové hodnocení: 87 bodů

Klady: možnost nastavení češtiny, mnoho dalších funkcí

Zápory: méně časté aktualizace, nemožnost volby rozsahu testu

5) Webroot Spy Sweeper 3.5

Celkové hodnocení: 88 bodů

Klady: výborné varování před útoky v reálném čase, snadné ovládání, možnost stáhnutí češtiny

Zápory: nemožnost výběru složky při instalaci, vzhledově nepříliš přívětivý

6) SpyRemover 2.33

Celkové hodnocení: 74 bodů

Klady: rychlost testu

Zápory: nemožnost odstranění nalezeného spyware, méně časté aktualizace, téměř žádná nápověda, nemožnost volby rozsahu testu

7) SpywareBlaster 3.3

Celkové hodnocení: 85 bodů

Klady: originální systém ochrany, jednoduchá a výstižná nápověda, mnoho dalších funkcí

Zápory: nemožnost odstranění spyware již se nalézajícího v PC

8) Spyware Doctor 3.2

Celkové hodnocení: 83 bodů

Klady: velmi časté aktualizace

Zápory: žádné funkce navíc jako obnova systému, či možnost kontroly domovské stránky v IE

9) CounterSpy 1.0.29

Celkové hodnocení: 89 bodů

Klady: výkonnost vyhledávacího engine, velmi přehledné a intuitivní ovládání, stejně jako výsledky testů, mnoho vedlejších funkcí (obnova systému, rezidentní štít, plánovač skenování)

Zápory: pomalost kompletního testu vzhledem ke konkurenci, nutnost koupě licence po vypršení zkušební doby

10) eTrust PestPatrol Anti-Spyware 4.4

Celkové hodnocení: 81 bodů

Klady: častá aktualizace, důkladný test

Zápory: nemožnost odstranění nalezeného spyware, nemožnost výběru složky při instalaci

ZÁVĚR

Při bližším porovnání výsledků bylo patrné, že většina nalezeného spyware byla u testovaných programů shodná, avšak každý našel též vlastní specifické položky. Neznamená tedy, že když program SpySweeper našel největší množství spyware, že ostatní našly tytéž položky avšak ne všechny jako on. Ostatní programy jich sice objevily méně, avšak byly mezi nimi také jiné druhy než ty, které našel program SpySweeper. Každý z programů totiž využívá jiný způsob detekce a má jinou databázi spyware. Je tedy důležité, aby tato databáze byla co nejobsáhlejší. Jednak co do kvantity a také co do kvality nalezeného spyware. Důležitým kritériem při výběru vhodného programu je totiž i nebezpečnost nalezených prvků. Jako příklad lze uvést situaci, kdy mi jeden program ohlásí detekci padesáti položek a při bližším prostudování výsledků zjistím, že se ve všech případech jedná o cookies, které “pouze“ sledují mnou navštívené stránky. Druhý program, který spustím vzápětí, mi najde jen 20 položek, ale z toho 3 trojské koně, které umožňují útočníkovi získání libovolných dat z mého počítače či jejich úplné odstranění. Je samozřejmé, že je pro mne hodnotnější program druhý, který co do kvantity má výsledek testu horší, avšak po kvalitativní stránce vysoce předčí program první.

U testovaných programů se velikost databáze spyware pohybovala od 566 u Bazooka Scanneru až po 24 800 u programu SpyRemover. U tohoto programu bych ještě zmínil jednu podstatnou záležitost. Jak již jsem uvedl při podrobnějším popisu programu, vzhledová stránka programu je téměř totožná s programem SpyBot. Tato podobnost po prozkoumání výsledků testu nezůstala jen u grafické stránky, ale také ve vyhledávání mezi nimi nebyly skoro žádné rozdíly (SpyRemover našel o jednu položku cookie více než SpyBot). Při faktu, že u programu SpyBot se jedná o bezplatnou verzi, která navíc obsahuje mnoho přídavných funkcí a také dostupnost češtiny, a SpyRemover je pouze shareware, který sice spyware vyhledá, ale jeho odstranění je možné až po registraci programu za 40 USD, nevidím sebemenší důvod pro užívání programu SpyRemover, když totéž, ba dokonce o mnoho více mohu získat bezplatně.

Z uvedeného hodnocení si jednotliví uživatelé mohou vybrat ten program, který se jim bude zdát pro ně nejvhodnější. Každý z testovaných programů má své klady i zápory. Někdo dá přednost výkonu před vzhledovou přívětivostí a pro jiného je přednější design a ovladatelnost, přičemž se spokojí s nižším výkonem. Mým doporučením v boji proti spyware je kombinace dvou popřípadě tří programů. Jedná se o AdAware SE Personal

Edition 1.05 a CounterSpy 1.0.29 ve verzi placené, potažmo v kombinaci se Spybot - Search & Destroy 1.3. Jejich celkové hodnocení je na velmi vysoké úrovni. Vyhledávací engine dosahuje nejvyšších hodnot ze všech testovaných programů, což je též dáno vysokou podporou ze strany jejich výrobce. Ovládání programů je lehce srozumitelné, navíc AdAware a SpyBot jsou dostupné též v češtině. Jak již jsem řekl, u CounterSpy doporučuji nákup roční licence za necelých 20 USD, protože se domnívám, že tato investice je velmi výhodná vzhledem k úrovni získané bezpečnosti.

Na závěr bych uvedl ještě jedno doporučení: „Zničte spyware dříve, než zničí on Vás.“

SEZNAM POUŽITÉ LITERATURY

- [1] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. První vydání. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1
- [2] VANĚK, Jan. Také vás sledují?. *Chip*. 2004, roč.14, č.12, s.92 - 96. ISSN 1210 - 0684
- [3] KLEGA, Vratislav. Dopadení špióni. *Chip*. 2004, roč.14, č.12, s.97 - 100. ISSN 1210 - 0684
- [4] PŘIBYL, Tomáš. Základy informační bezpečnosti. *PC WORLD Security*. 2004, č.9, s. 2 – 4. ISSN 1214 – 794X
- [5] BUDIŠ, Petr. Jak vypracovat bezpečnostní politiku v podniku. *PC WORLD Security*. 2004, č.12, s. 44 – 46. ISSN 1214 – 794X
- [6] *Ad-aware – nástroj proti spyware* [online]. [cit. 2005-04-04]. Dostupný z WWW: <<http://www.officeplus.cz/adaware.php>>
- [7] *Microsoft Windows : Security* [online]. [cit. 2005-04-01]. Dostupný z WWW: <<http://www.microsoft.com/cze/security/spyware/software/default.mspx>>
- [8] *Kerio : slovníček pojmů* [online]. [cit. 2005-04-06]. Dostupný z WWW: <<http://www.kerio.sk/manual/kpf/cz/go01.html>>
- [9] *Trojanhelp* [online]. [cit. 2005-04-10]. Dostupný z WWW: <<http://trojanhelp.wz.cz/>>
- [10] *Earthlink Spy Audit* [online]. [cit. 2005-04-01]. Dostupný z WWW: <<http://www.earthlink.net/spyaudit/press/>>
- [11] *Security slovník* [online]. [cit. 2005-04-14]. Dostupný z WWW: <http://www.vyvial.cz/security/index_web_slovník.php>
- [12] *Podvodná přesměrování aneb desetisíce za internet* [online]. [cit. 2005-04-25]. Dostupný z WWW: <http://ada.fbi.cz/data/menu/nas_pripad.htm>
- [13] *Bezpečnostní politika (2.díl)* [online]. [cit. 2005-04-02]. Dostupný z WWW: <<http://www.isvs.cz/index.html?clanek=58>>

- [14] MAREK, R., DASTYCH, J. *Bezpečnostní politika v organizaci* [online]. [cit. 2005-04-16]. Dostupný z WWW: <<http://www.systemonline.cz/site/bezpecnost/politika4.htm>>
- [15] *Bazooka™ Adware and Spyware Scanner* [online]. [cit. 2005-04-22]. Dostupný z WWW: <<http://www.kephyr.com/spywarescanner/index.html>>
- [16] BRANDT, A. *Poor Defenders* [online]. [cit. 2005-04-10]. Dostupný z WWW: <<http://www.pcworld.com/news/article/0,aid,118362,pg,1,00.asp>>
- [17] *Legální software a základní pojmy* [online]. [cit. 2005-04-10]. Dostupný z WWW: <<http://www.pcpomocnik.cz/c/legalni-software/legalni-software.htm>>
- [18] *PestPartol 4* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.stahuj.cz/internet_a_site/bezpecnost/ostatni/pestpatrol/>
- [19] *Ad-Aware SE Personal Edition 1.05* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10319876.html?tag=lst-0-17>
- [20] *CounterSpy 1.0.29* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/CounterSpy/3000-8022_4-10375153.html>
- [21] *Bazooka Adware and Spyware Scanner 1.13.03* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/Bazooka-Adware-and-Spyware-Scanner/3000-8022_4-10377953.html?tag=lst-0-11>
- [22] *Spybot - Search & Destroy 1.3* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/Spybot-Search-Destroy/3000-8022_4-10289035.html?tag=lst-0-1>
- [23] *Microsoft Windows AntiSpyware beta* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/Microsoft-Windows-AntiSpyware/3000-8022_4-10353596.html?tag=lst-0-20>
- [24] *SpyRemover 2.33* [online]. [cit. 2005-04-27]. Dostupný z WWW: <http://www.download.com/SpyRemover/3000-8022_4-10383985.html?tag=lst-0-18>
- [25] *Spyware Doctor 3.2* [online]. [cit. 2005-04-28]. Dostupný z WWW: <http://www.download.com/Spyware-Doctor/3000-8022_4-10377263.html>

- [26] *SpywareBlaster* 3.3 [online]. [cit. 2005-04-28]. Dostupný z WWW: <http://www.download.com/SpywareBlaster/3000-8022_4-10372089.html?tag=lst-0-25>
- [27] *Webroot Spy Sweeper* 3.5 [online]. [cit. 2005-04-28]. Dostupný z WWW: <http://www.download.com/Webroot-Spy-Sweeper/3000-8022_4-10373771.html?tag=lst-0-22>
- [28] *FTC Bars Bogus Anti-Spyware Claims* [online]. [cit. 2005-04-30]. Dostupný z WWW: <<http://www.ftc.gov/opa/2005/03/maxtheater.htm>>
- [29] HOWES, E. *FTC Busts Rogue Anti-Spyware Vendor* [online]. [cit. 2005-05-01]. Dostupný z WWW: <http://www.spywarewarrior.com/rogue_anti-spyware.htm>
- [30] *Ad-Aware* 1.05 SE [online]. [cit. 2005-04-28]. Dostupný z WWW: <<http://cestiny.idnes.cz/pa/adawaregyvcz.html>>
- [31] *SpySweeper* [online]. [cit. 2005-04-29]. Dostupný z WWW: <<http://cestiny.idnes.cz/ps/spysweepercz.html>>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AR	Analýza rizik
BP	Bezpečnostní politika
IE	Internet Explorer
IT	Informační technologie
MS	Microsoft
PC	Personal computer (osobní počítač)

SEZNAM OBRÁZKŮ

Obr. 1 Náhled programu Microsoft Antispyware Beta.....	36
Obr. 2 Náhled programu Bazooka™ Adware and Spyware Scanner.....	38
Obr. 3 Náhled programu AdAware SE Personal Edition 1.05	40
Obr. 4 Náhled programu Spybot - Search & Destroy 1.3.....	43
Obr. 5 Náhled programu Webroot Spy Sweeper 3.5	45
Obr. 6 Náhled programu SpyRemover 2.33	47
Obr. 7 Náhled programu SpywareBlaster 3.3.....	48
Obr. 8 Náhled programu Spyware Doctor 3.2	50
Obr. 9 Náhled programu CounterSpy 1.0.29	52
Obr. 10 Náhled programu eTrust PestPatrol Anti-Spyware 4.4	54
Obr. 11 Procentní podíl hodnocených parametrů	59

SEZNAM TABULEK

Tab. 1 Výsledky projektu Spy Audit	22
Tab. 2 Rozdíl mezi jednotlivými variantami AdAware.....	41
Tab. 3 Porovnání programů - část 1.....	56
Tab. 4 Porovnání programů - část 2.....	57

SEZNAM PŘÍLOH

P I Slovník použitých pojmů.

PŘÍLOHA P I: SLOVNÍK POUŽITÝCH POJMŮ.

<i>Adware</i>	Typ spyware. Jedná se o software, který zdarma uživateli poskytuje nějakou funkci a který je financován z prodeje reklamy
<i>Backdoor trojans</i>	Software - jedná se o aplikace, které počítač „otevírají“ (většinou běž vědomí uživatele) útočníkům - ať již samotná data v něm obsažená, či jako prostředek k dalším útokům na PC
<i>Cookie</i>	Textové informace, které server ukládá ke klientovi (WWW prohlížeči). Slouží pro pozdější identifikaci klienta při opětovné návštěvě daného serveru/stránky
<i>DDoS (Distributed Denial of Service)</i>	Pokročilejší varianta útoku DoS, kdy k napadení serveru dochází z většího množství míst. To samozřejmě zvyšuje pravděpodobnost úspěchu
<i>Dialer</i>	Škodlivý kód, který se skrývá ve webových stránkách a je schopen přesměrovat telefonické připojení na placené (zpravidla zahraniční) linky
<i>DoS (Denial of Service)</i>	Typ počítačového útoku, kdy dochází k napadání serveru tak, že je na něj vysíláno velké množství žádosti (např. o zobrazení webových stránek). Server pak toto množství není schopen zvládnout a “spadne“.
<i>Freeware</i>	Jsou to volně šiřitelné programy. Tyto programy nepotřebují žádnou koupenou licenci. Jsou zdarma. Programy s tímto označením lze zcela libovolně šířit, kopírovat a instalovat na libovolný počet počítačů.
<i>Hijacker</i>	Speciální druh <i>adware</i> , trojského koně, který unese Internet Explorer a převezme nad ním kontrolu
<i>Outsourcing</i>	Zajišťování určitých funkcí a služeb ve firmě prostřednictvím dodavatelských firem specializovaných na danou oblast
<i>Peer-to-peer síť</i> (= P2P síť)	Programy nebo stránky sloužící ke sdílení dat (hudba, filmy, ...)

<i>Shareware</i>	Drobné i větší programy, které se často používají na jednoúčelové činnosti. Tyto programy je třeba registrovat. Nejobvyklejší zásadou ale je, že program a formu jeho distribuce nesmí nikdo bez svolení autora měnit. Shareware program lze volně kopírovat, umisťovat.
<i>Spam</i>	Nevyžádaná pošta
<i>Spyware</i>	Program, který napomáhá shromažďování informací o osobě či společnosti bez jejich vědomí a může tyto informace poslat neautorizované třetí osobě.
<i>Stealth networks</i>	Typ spyware, který zapojí počítač bez vědomí uživatele do síťového systému, jenž může sloužit k nejrůznějším účelům
<i>System monitors</i>	Typ spyware, který umožňuje útočníkovi sledovat veškerou aktivitu počítače včetně stisku kláves či snímání obsahu obrazovky
<i>Trialware</i>	Jedná se o časově omezené verze programu (nejčastěji 7, 15 nebo 30-denní), které slouží k tomu, abyste nekupovali “zajíce v pytli“. Většinou jsou bez jakéhokoliv omezení. Po určitém čase přestanou fungovat a vyžadují zlegálnění programu - koupi. Tudíž heslo, klíč - vstupenku k plnému produktu
<i>Utilita</i>	Program vykonávající jisté pomocné činnosti
<i>Warez stránky</i>	Webové stránky s nelegálním softwarem, filmy, cracky, sériovými čísly k programům apod. ke stažení
<i>Web bug</i>	Miniaturní průhledný obrázek umístěný na stránce o velikosti jednoho pixelu, takže o tom, že se na stránce vyskytuje většinou ani nevíte. Slouží ke sledování návštěv stránek
<i>XXX stránky</i>	Webové stránky s erotickou či porno tematikou