Bezpečnost na Internetu

Safety on the Internet

Petr Šimoník

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr ŠIMONÍK**
Osobní číslo:	**A09267**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost na Internetu**

Zásady pro vypracování:

1. **Sestavte literární rešerši na téma bezpečnosti na Internetu.**
2. **Formulujte nejčastější rizika současnosti.**
3. **Navrhněte postupy a rady jak se bránit popsaným rizikům.**
4. **V praktické části otestujte bezpečnost vybraného systému.**
5. **Proveďte průzkum znalostí bezpečnosti na skupině uživatelů Internetu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BITTO, Ondřej. Jak zabezpečit domácí a malou síť Windows XP : Účty, práva, firewally, antiviry a další nástroje . 1.vydání. Praha : Computer Press, 2006. 216 s. ISBN 80-251-1098-2.**
2. **LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.**
3. **SMITH, Ben; KOMAR, Brian; MICROSOFT SECURITY TEAM. Zabezpečení systému a sítě Microsoft Windows. Praha : Computer Press, 2007. 700 s. ISBN 80-251-1260-8.**
4. **VÍTEK, Miloš a Marcela VÍTKOVÁ. Sociální vědy a inženýrství. Vyd. 1. Hradec Králové: Gaudeamus, 2004, 164 s. ISBN 80-704-1474-X.**
5. **MITNICK, Kevin. Umění klamu. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.**

Vedoucí bakalářské práce: **Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Náplní mé bakalářské práce je určení největších Internetových hrozeb současnosti při používáni běžnými uživateli. Navrhnout, jak se účinně bránit popsaným hrozbám a jak snížit dopady těchto útoků. Dále otestovat různé druhy pomocných programů na systému. A provést průzkum znalostí o bezpečném používání počítače u běžných uživatelů.

Klíčová slova: Škodlivý kód, sociální inženýrství, bezpečnost, útoky

ABSTRACT

The aim of my thesis is to determine the largest Internet threats today, when used by common users. Suggest how to prevent threats and described how to reduce the impact of these attacks. Further testing of various kinds of auxiliary programs on the system. A survey done of knowledge about safe computer use at ordinary users.

Keywords: Malicious code, social engineering, security, attacks

PODĚKOVÁNÍ

Chtěl bych tímto poděkovat svému vedoucímu práce, panu ***Ing. Jiřímu Vojtěškovi, Ph. D.,*** za jeho cenné rady a připomínky, dále bych chtěl poděkovat rodině za podporu a všem účastníkům průzkumu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 URČENÍ NEJVĚTŠÍCH RIZIK **11**
2 PROGRAMY OHROŽUJÍCÍ BEZPEČNOST SYSTÉMU **13**
2.1 VIRY 13
2.1.1 Druhy virů a jejich projevy 13
2.2 TROJSKÉ KONĚ 14
2.2.1 Password- stealing trojské koně (PWS) 15
2.2.2 Destruktivní trojské koně 15
2.2.3 Downloader 15
2.2.4 Proxy trojský kůň 15
2.3 ČERVI 15
2.3.1 IM a IRC červ 16
2.3.2 Síťový červ 16
2.4 BACKDOOR 16
3 SPYWARE **17**
3.1 ADWARE 17
3.2 HIJACKER BROWSER 17
3.3 KEYSTROKE LOGGER 18
4 SPECIÁLNÍ TECHNIKY ÚTOKŮ **19**
4.1 SOCIÁLNÍ INŽENÝRSTVÍ 19
4.2 PHISHING 19
4.3 PHARMING 20
II PRAKTICKÁ ČÁST **23**
5 JAK SE BRÁNIT UVEDENÝM RIZIKŮM **24**
5.1 ANTIVIROVÁ OCHRANA 24
5.1.1 Jednoúčelové antiviry 24
5.1.2 ON-demand skenery 24
5.1.3 Antivirové systémy 24
5.2 FIREWALL 25
5.2.1 Nastavení brány firewall ve Windows 7 27
5.3 OCHRANA PROTI SPYWARE 28
5.3.1 Úroveň uživatelových znalostí 28
5.3.2 Obezřetnost a pečlivost 29
5.3.3 Vzájemná provázanost systému 29
5.4 OCHRANA PROTI PRAKTIKÁM SOCIÁLNÍHO INŽENÝRSTVÍ 30
5.4.1 Jak se chránit proti phishingu 30

5.4.2 Jak se chránit proti pharmingu 33
5.5 NASTAVENÍ SYSTÉMU WINDOWS 34
5.5.1 Řízení uživatelských účtů 34
5.5.2 Účty a práva 35
6 TESTOVÁNÍ SYSTÉMU 37
6.1 WINDOWS 7 HOME BASIC 38
6.2 AVAST! FREE ANTIVIRUS 8.0.1489 38
6.3 BITDEFENDER ANTIVIRUS 2013 PLUS 40
6.4 ESET SMART SECURITY 6 42
6.5 AD-AWARE PRO SECURITY 10.1.211.3382 43
6.6 F-SECURE INTERNET SECURITY 2011 45
6.7 OUTPOST PRO FIREWALL 46
6.8 SHRNUTÍ VÝSLEDKŮ TESTOVÁNÍ 48
7 PRŮZKUM ZNALOSTÍ BEZPEČNOSTI NA SKUPINĚ UŽIVATELŮ INTERNETU 50
7.1 ANALÝZA ODPOVĚDÍ V DOTAZNÍKU 50
7.1.1 Vlastníte osobní počítač? 50
7.1.2 Za jak zdatného se považujete při práci na PC? 51
7.1.3 Užíváte prvky uvedených sociálních sítí? 52
7.1.4 Víte co to je Sociální inženýrství? 53
7.1.5 Slyšel jste někdy jméno Kevin Mitnick 54
7.1.6 Znáte Phishing a setkali jste se s ním? 55
7.1.7 Co děláte po přijetí neznámého emailu? 56
7.1.8 Využíváte Internet banking? 57
7.1.9 Setkali jste se s tím, že vám přišel email z vašeho finančního institutu a žádal po vás přihlášení? 58
7.1.10 Jaký požíváte Antivirový systém? 59
7.1.11 Setkali jste se někdy s počítačovým virem ve svém počítači? 60
7.1.12 jaký používáte firewall ? 61
7.1.13 Používáte různá hesla pro přihlášení? 62
ZÁVĚR 64
ZÁVĚR V ANGLIČTINĚ 65
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 70
SEZNAM OBRÁZKŮ 71
SEZNAM TABULEK A GRAFŮ 72

ÚVOD

O bezpečnosti na internetu můžeme uvažovat v několika rovinách. Můžeme ji chápat jako soubor opatření, které jsou vytvořeny tak, aby znemožnily nebo maximálně ztížily převzetí kontroly nad počítačem, získání neveřejných, soukromých dat nebo obsah komunikace a v neposlední řadě útok na server s úmyslem ho vyřadit z provozu. Do další roviny patří ochrana před úniky nevhodných osobních informací, například z účtu na sociálních sítích nebo manipulace s lidmi přes sociální sítě. Ty se stávají součástí života lidí a ti tomuto masovému šílenství podléhají v čím dál útlejším věku. Nedá se říci, že starší jsou na tom lépe. Tento trend se už asi nezastaví. Pobyt u počítače a u sociální sítě je jako droga. Jak se jednou začne, tak se to s lidmi táhne až do konce života. Sociální sítě nejsou špatné, bohužel vedou ke ztrátě soukromí. Lidé se naučili rádi zveřejňovat údaje o sobě, co právě dělají nebo zobrazovat své fotky. Když toto děláte, tak musíte počítat s tím, že se objeví někdo, kdo tyto informace zneužije ve svůj prospěch.

Dále odhalíme největší a nejčastější možná rizika dnešní doby. Ty nejzásadnější si probereme blíže. Začneme od virů, které napadají své hostitele, červi šířící se elektronickou poštou, různé druhy trojských koní, spyware až po sociální inženýrství. Tyto druhy infiltrací napadají koncové stanice nebo poškozují uživatele operačních systémů Windows. Internet takzvaná „síť sítí“ obsahuje gigantické množství informací a mezi těmito informacemi se nachází hrozby, proti kterým je potřeba se bránit.

V praktické části provedu rešerši nástrojů, které zvyšují bezpečnost systému. Hlavně se budu zabývat softwarovými aplikacemi, které znesnadňují útočníkovi implementaci škodlivého programu. Také navrhnu jak se bránit různým typům útoku.

Otestuji na systému Windows 7 Home basic podpůrné programy pro zajištění bezpečnosti před možnou infiltrací pomocí škodlivého kódu, nebo útoku hrubou silou. Vše bude prováděno na virtuálním PC, aby nedošlo k narušení integrity souborů uložených na hard disku.

Na závěr analyzuji dotazník, jehož výstup bude brán jako ukazatel úrovně znalostí možných hrozeb a to u běžných uživatelů Internetu. Věkový rozestup bude dostatečně velký, abychom docílili správnosti a relevantnosti výsledků.

I. TEORETICKÁ ČÁST

1 URČENÍ NEJVĚTŠÍCH RIZIK

Na obrázku číslo 1 je vidět, jakým tempem roste počet útoků, které sesbíral národní bezpečnostní tým CSIRT za dobu svého fungování. CSIRT[1] byl zřízen ministerstvem vnitra a funguje, jako místo kam se sbíhají hlášení o útocích, u nichž není úplně jasné, kdo je způsobil, nebo se jedná o závažný incident.

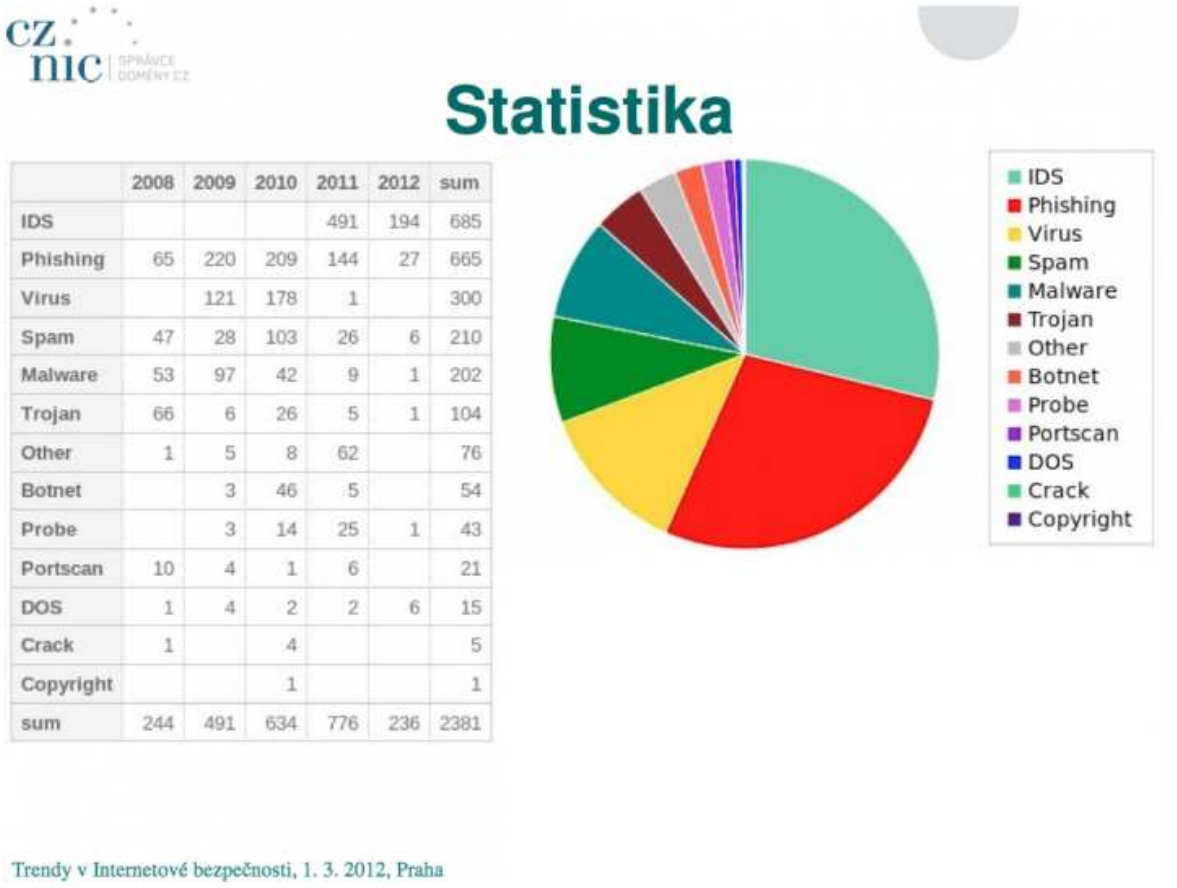
IDS[2] je zde bráno jako odhalené útoky pomocí systému na odhalování průniků, jsou to systémy monitorující síťový provoz a odhalují neobvyklé aktivity. Rozdíly mezi IDS systémy a firewallem tkví v tom, že IDS hlídá narušení i zevnitř sítě. To je dáno díky zkoumání komunikace v síti, rozpoznáváním vzorů. Po zjištění takového vzoru nebo podpisu dojde k uvědomění operátora a ukončení spojení. Tomu se také říká prevence průniku.

Dalším nejčastějším útokem je phishing ten se v České Republice objevoval už dříve, ale od roku 2008 jsou evidované záznamy, kdy bylo zaznamenáno 65 phishingových zpráv. Od roku 2008 do roku 2012 bylo zaznamenáno 665 útoků metodou phishing.

Také viry, spam, malware a trojské koně jsou častými riziky, co na nás číhají na Internetu. Proto se budu těmto rizikům věnovat, tím že je popíši, jak fungují, uvedu příklady, a jak velkou hrozbou jsou pro uživatele Internetu. [1]

[1]CSIRT- Computer Security Incident Response Team

[2] IDS - Intrusion Detection Systém, systém pro odhalení průniku



	2008	2009	2010	2011	2012	sum
IDS				491	194	685
Phishing	65	220	209	144	27	665
Virus		121	178	1		300
Spam	47	28	103	26	6	210
Malware	53	97	42	9	1	202
Trojan	66	6	26	5	1	104
Other	1	5	8	62		76
Botnet		3	46	5		54
Probe		3	14	25	1	43
Portscan	10	4	1	6		21
DOS	1	4	2	2	6	15
Crack	1		4			5
Copyright			1			1
sum	244	491	634	776	236	2381

Obrázek 1 Graf struktury útoků podle CSIRT [1]

2 PROGRAMY OHROŽUJÍCÍ BEZPEČNOST SYSTÉMU

Počítače připojené do celosvětové sítě s názvem Internet ohrožuje spousta bezpečnostních rizik a ty stále nezastavitelně rostou. Tvůrci vytvářejí stále důmyslnější metody a techniky jak získávat citlivé nebo neveřejné informace. Používají různé viry, které jsou podobné běžným programům s tím rozdílem, že je schopen se sám replikovat, šířit a provádět akce nezávisle a to bez uživatelova vědomí. Většina lidí si pod pojmem „virus“ představuje všechny typy infiltrací, aniž by rozlišili vir od trojského koně nebo červa. Různé typy infiltrací se prolínají a není možné je tedy úplně přesně zařadit.

2.1 Viry

Pojmenování počítačový virus vychází z podobnosti s biologickými viry. Zástupci jak biologického tak softwarového druhu mají schopnost množení sama sebe, ale jen když mají svého hostitele. U počítačových virů to bývají spustitelné soubory, systémové oblasti disků nebo soubory specifických aplikací (což mohou být dokumenty MS Excel, skripty Visual Basicu a mnohé další). Celé to funguje na základě spuštění hostitelského programu, tím dojde zároveň k provedení kódu viru. To má za následek další rozšiřování a replikování škodlivého kódu.

2.1.1 Druhy virů a jejich projevy

Souborové – Jejich hlavním cílem je napadnout spustitelné soubory (*.exe, *.com, *.vbs), přepisují části kódu souboru svým. Což může mít za následek změnu chování a velikost souboru.

Makroviry – cílem jsou dokumenty MS office (*.xls, *.docx, *.doc), tyto viry jsou nejčastějším druhem viru a také by mohli být v budoucnu rizikem.

Boot viry – útočí na boot sector na disku (to je jádro OS), při zavedení tohoto viru do systému se při každém použití diskety (dnešní době spíše USB flash paměti) je napadeno a slouží k šíření viru.

Rezidentní viry – nachází se v operační paměti, skenují diskové operace a zavádí se při startu PC.

Stealth – Ukrývají se před antivirovými programy, tím že při pokusech o jeho nalezení podávají mylnou zprávu.

Polymorfní – upravují svůj kód v závislosti na okolnostech, jejich odhalení je dost složité.

Projevy počítačových virů mohou být různé, já uvedu ty nejzásadnější.

Blokování místa – vir je uložen na disku, to znamená, že zabírá místo, nemusí jenom zabírat místo na pevném disku, ale i v operační paměti. Tento problém s kapacitami pamětí používaných dnes bychom mohli považovat za méně závažný.

Nestabilita systému – Virus napadá soubory, tak vzniká možnost padání aplikací kvůli její nekompatibilitě. Mimo pády muže dojít k zamrznutí celého systému. Při objevení se těchto příznaků to nemusíme dávat hned za vinu viru.

Zpomalení sytému – Aby se vir mohl šířit nebo vůbec aktivovat, potřebuje část výpočetní kapacity počítače. Počítač může být zpomalován například replikací škodlivého kódu do jiných souborů.

Různá vyskakovací okna a jiné projevy – některé viry se snaží na sebe upozorňovat různými způsoby, od vypisování textu až po audiovizuální efekty. Většinou jsou viry nastaveny tak, aby se spouštěli v určité časy.

Krádež dat – Virus může posílat osobní data přes síť kamkoliv ve světě, pokud je do ní připojen. Může je třeba šifrovat a při pokusu přístupu k nim zase rozšifrovat, aby nikdo nic nepoznal a pak je najednou zablokovat a nakonec odeslat komukoliv.

Ničení dat – Některé viry jsou uzpůsobené k modifikaci dat tak, aby byli nečitelné. Existují viry, co mažou systémové složky, celé oddíly disku nebo programovatelnou paměť FlashBIOS. [2] [3]

2.2 Trojské koně

Tento druh škodlivého kódu nemá sebe-replikační schopnost a nepotřebuje svého hostitele. Je to přímo spustitelný soubor. To znamená, že při odstraňování škodlivého kódu by mělo postačit smazání souboru. Označení trojský kůň vzniklo podle pověsti o trojském koni, který byl darován bohům. Tento kůň obsahující skupinu Řeků byl zatažen za brány Tróji a v noci, nic netušící obyvatele města přepadli. Stejným způsobem funguje i trojan

v počítači. Tváří se jako nějaký užitečný program, ale ve skutečnosti obsahuje škodlivý kód.

2.2.1 Password- stealing trojské koně (PWS)

Druh trojských koní, který je naprogramován tak, aby zjišťoval hesla. A to pomocí sledování stisků kláves u klávesnice. Stisknutá tlačítka ukládá a poté je odesílá na e-mailové adresy, které nejčastěji patří přímo tvůrcům trojského koně. U trojských koní vytvořených v cizině a umístěných na českém počítači vzniká problém s diakritickými znaménky.

2.2.2 Destruktivní trojské koně

Tento tip patří mezi klasické trojské koně. Po spuštění trojský kůň začne mazat soubory na disku nebo zformátuje celý disk. K destruktivním trojanům můžeme zařadit i BAT trojany. Je to dávkový soubor obsahující škodlivý kód, některé lze odhalit díky jednoduchému kódování obsahu.

2.2.3 Downloader

Program, po jehož spuštění dojde k vypuštění jiných škodlivých kódů. Tyto škodlivé kódy nejsou obsaženy v těle trojského koně, ale stáhne je z URL, kterou má nastavenou. Pokud by došlo k jeho spuštění, tak by mohla nastat situace, že první stáhne další software, ten spustí další vlnu stahovaní, což muže způsobit zamrznutí nebo kompletní pád systému.

2.2.4 Proxy trojský kůň

Počítač napadený tímto trojanem se stane rozesílačem spamu – tedy nevyžádané pošty. Navíc používá proxy a tím maskuje skutečného autora spamu, to znamená, že šance ho vypátrat je skoro rovná nule. [2] [4]

2.3 Červi

Červ (worm) je to druh viru, který ke své infiltraci do počítače používá elektronickou poštu. Většinou je ukryt jen v jednom souboru, obsahující jenom škodlivý kód červa. Červ bývá přiložen k emailu jako příloha. Pokud uživatel soubor spustí, uloží se červ do počítače

a navíc rozešle infikované emaily na další účty, které má uživatel uloženy v adresáři. K infiltraci do PC[3] využívá zvědavosti lidského druhu. Používají se názvy jako „Pamela Andersen“ nebo „Emma Watson“, navíc je obsah zprávy doplněn textem, například: „Nahé fotky celebrit“ a jiné nesmysly. Příjemce emailu si může myslet, že jde o obrázky, ale bohužel ve skutečnosti to může být červ, čekající na spuštění nepozorným uživatelem. Červi využívají nepozornosti osob, tím že mají dvě přípony „*.jpg.exe“. Někteří červi jsou přímo součástí zprávy, takže nepotřebují žádný soubor v příloze. Červ se spustí jen otevřením nakažené zprávy, což je způsobeno vložením škodlivého kódu přímo do HTML[4].

2.3.1 IM a IRC[5] červ

Tento typ se šíří díky technologii posílání zpráv a chatování. Infiltruje se pomocí děr v bezpečnosti konkrétního klienta.

2.3.2 Síťový červ

Druh pohybující se na lokálních sítích. Jeho vlastnosti jsou podobné ostatním červům a většinou je kombinován s IM a IRC červem. [2]

2.4 Backdoor

Typ infiltrace umožňující zdolání zabezpečovacího mechanismu, užívaného nejčastěji ke vzdálenému přístupu do systému. Když útočník získá kontrolu nad systémem, stává se z počítače tzv. „zombie“. Pokud infiltrátor kontroluje více počítačů tak celek nazýváme „botnet“. Jednou variantou backdoor trojanu je RAT (remote administration tool). Správci systému a další oprávnění uživatelé je používají pro zjednodušení práce, takže jejich původ je čistě s dobrým úmyslem, bohužel dochází k jejich zneužívání. Potom se může stát, že se nevědomky váš počítač účastní DDos útoku. [4] [2]

---

[3] PC – Personal computer, osobní počítač

[4] HTML - HyperText Markup Language, hlavní z jazyků pro vytváření webových stránek

[5] IM, IRC – Instant messaging, internet relay chat, obě slouží ke komunikaci v reálném čase

3 SPYWARE

Spyware se dá definovat jako infiltrace a nepozorovatelný provoz bez vědomí uživatele, i když je to velmi široký pojem. Tak tato definice platí pro škodlivější software. Ten méně škodlivý se snaží neustále uživatele obtěžovat a neustále na sebe upozorňovat. To bývá většinou známkou, že počítač není dostatečně chráněn. Spyware dělíme dle jeho činnosti.

3.1 Adware

Software šířený zdarma bývá vybaven adwarem pro zobrazování reklam nebo pop-up oken (vyskakovacích oken) nebo nějakým vyhledávacím nástrojem v prohlížeči, většinou o tyto doplňky systému uživatelé vůbec nestojí. Bohužel při instalaci volně šiřitelného softwaru musí souhlasit s licenčními podmínkami, což velká skupina uživatelů považuje za zbytečnost a zdržování, proto ji „odkliknou“ bez přečtení. A tím vědomky souhlasí s instalací adwaru. Existují i další možnosti jak si nainstalovat adware do počítače. Jednou z možností je při výběru částí softwaru. Tady bývá vložena jako podpůrný software, který bývá defaultně nastaven tak, aby se instaloval. Šiřitel softwaru doufá v nepozornost uživatele, který buď nedává pozor, co instaluje nebo nemá zkušenosti a netuší, co si může způsobit.

Vydavatelé jsou ovšem chytří a snaží se co nejvíce komplikovat případnou odinstalaci nechtěného softwaru, kromě složitosti může dojít i k nefunkčnosti softwaru, který jsme původně instalovali. To vede některé uživatele k tomu, že za cenu fungování programu jsou schopni akceptovat adware.[4]

3.2 Hijacker browser

Označován jako únosce prohlížeče. Má za úkol přepisovat nastavenou domovskou stránku, vyhledávací stránku vymění za svou. Jsou i případy kdy dojde ke změně v registrech a po každém restartu počítače se domovská stránka změní. K opravě je potřeba zásah do registrů.

Mezi oblíbené projevy této infiltrace je blokace různých stránek, mezi které patří hlavně stránky vývojářů antispywarerových a antivirových aplikací. Ne tak často se stává, že dokáže zablokovat samotný antivirový nebo antispywarový program. Nejčastěji

napadaným prohlížečem je Internet Explorer, protože tento prohlížeč umí spouštět ActiveX skripty přímo ze stránek. Hijacker programy se pokouší instalovat přes vyskakovací okna, kde se objevují otázky, co vypadají neškodně a při tom povolí instalaci. V nejhorším případě využijí bezpečnostní díry v prohlížeči. Tuto skutečnost uživatel nedokáže ovlivnit. Mění domovské stánky z důvodů zvýšení jejich návštěvnosti, nebo stránky s vyhledávacím programem, kde výsledky jsou sponzorované stránky.

Jako příklad si můžeme uvést CoolWebSearch (CWS). Je to standardní typ únosce, který přepisuje domovské stránky za své, na kterých je vyhledávač, kde zobrazované výsledky jsou sponzorované odkazy.[6]

3.3 Keystroke Logger

Můžeme ho rozdělit na softwarový a hardwarový. Jak už z názvu vyplývá, hardwarový je zařízení přímo namontované v počítači. My se budeme bavit o softwarových. Tyto programy dokáží sledovat stisky tlačítek na klávesnici v reálném čase. Ty se zaznamenávají a odesílají vývojáři tohoto škodlivého programu. Záznamy jsou potom používány na sbírání uživatelských jmen a hesel k dalšímu zneužití. Podobné programy jsou s námi už delší dobu, ale spywarové programy stále přibývají a tím roste i riziko infekce. [2] [4]

4 SPECIÁLNÍ TECHNIKY ÚTOKŮ

Do této skupiny patří hlavně sociální inženýrství a metody od něho odvozené. Jde převážně o přesvědčování lidí k dobrovolnému odevzdání svých citlivých dat. Můžeme je rozdělit na útoky hrubou silou anebo pouhým přinucením někoho, kdo má přístup kam potřebujeme nebo zná heslo. [8]

4.1 Sociální inženýrství

Prvním druhem speciální techniky je sociální inženýrství, což je metoda psychologického ovlivňování za pomocí cizí nebo smyšlené identity, kterou sociotechnik používá k oklamání lidí. Sociotechnik dokáže pouhým rozhovorem získat informace, tvářící se zdánlivě nevinně. Navíc si osoba, kterou takto využije ani neuvědomí, že byla okradena. Při použití této techniky může být systém vysoce zabezpečen, ale jeho slabinou bude stále uživatel. Můžeme si uvést příklad. Sice nepatří přímo do sociálního inženýrství, ale funguje stejně dobře. Metoda je založena na tom, že vir si uživatel zanese do počítače sám. Útočníkovi postačí někde na parkovišti nebo u vchodu do společnosti, z které chceme získat informace, položit například USB flash paměť nebo reklamní CD vybavené nebezpečnou „havětí“. Pokud ji uživatel zvedne a poté vloží do počítače, dojde k rozšíření škodlivého obsahu do uživatelova systému a následně i do sítě. Vraťme se zpět k pravé sociotechnice. Tuto techniku můžeme považovat za nejlevnější způsob, jak získat informace, navíc použitím komunikační techniky, jako jsou emaily, IM(instant messaging) nebo telefon. To nám dovoluje vydávat se za jiného, než skutečně jsme. Útočník se většinou snaží navázat s budoucí obětí jisté přátelství nebo důvěru tím, že se vydává za pracovníka technické podpory nebo někoho z nadřízených. V tomto případě může použít psychologický nátlak a donutit pracovníka bezmyšlenkovitě poslat informace nedůvěryhodné osobě. [5] [8]

4.2 Phishing

Je odvozeno z anglického slova fishing, neboli rybaření. Písmeno „f“ bylo nahrazeno „ph“ to pochází z internetové angličtiny. Phishing znamená získávání citlivých informací nelegálním a neetickým způsobem. Prvním zdokumentovaným phishingem je útok na emailové účty AOL z roku 1996, záznam o dřívějších útocích se nezachoval. Tzv. „phish“

(ryba u této metody spíše úlovek), mezi hackery ty to úlovky považují za platidlo, za které se dá koupit know how.

Phishing je prováděn pomocí podvodného emailu, který je posílán danému uživateli nebo skupině uživatelů s cílem získat především přihlašovací údaje k účtům, pro jejich další zneužití. V drtivé většině případů se jedná o pokus vylákat údaje k platebním kartám nebo přihlašovací údaje do internetového bankovnictví. Mimo údaje k bankovním účtům se útočníci snaží získat údaje i k jiným institucím, kde se manipuluje s penězi, jako možné cíle se jeví PayPal, Ebay,google nebo různé obchody výrobců mobilních telefonů, jako je Apple store a jiné. V phishingových emailech se používají psychologické a technické prostředky k přesvědčení adresáta k předání informací a to co nejjednodušším způsobem. Fungování phishingu je použití sociálního inženýrství, ve výsledku to znamená, že v adresátovi, po přečtení emailu, bude nabyt dojem, který ho oklame a on nepozná, jestli se jedná o důvěryhodnou osobu nebo podvodníka.

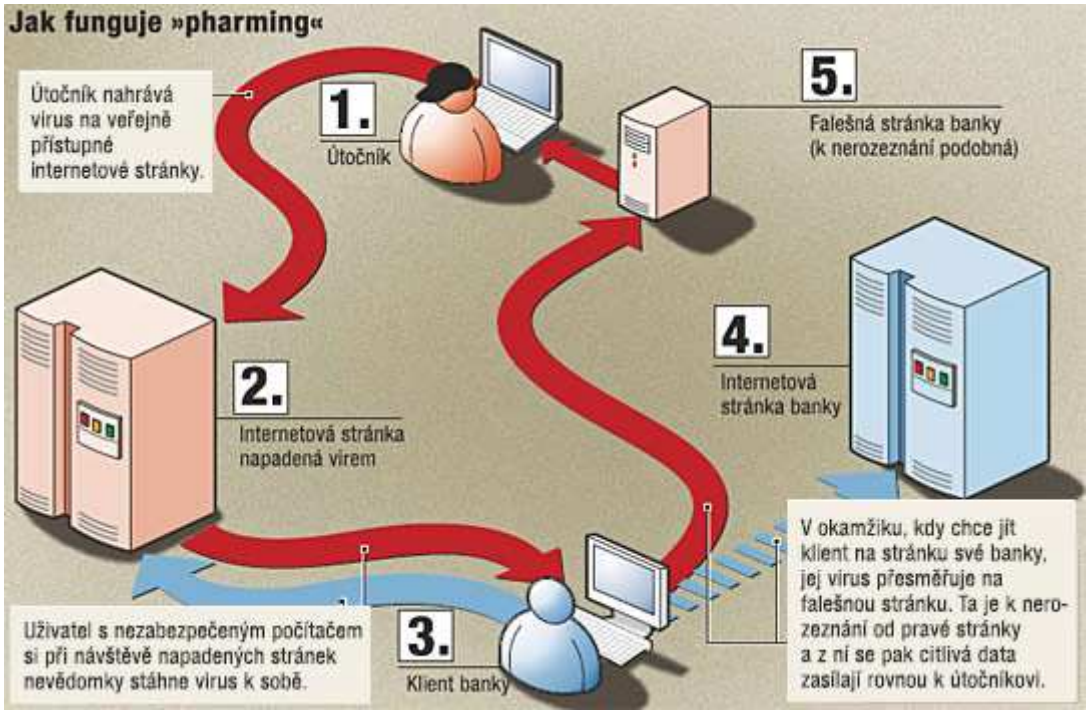
Dalšími klíčovými znaky pro udržení hodnověrnosti podvodného emailu, je zachování grafiky institutu, který se tak zvaný „phisher“ pokouší napodobit. Důležitými znaky jsou také zfalšování emailové adresy, které není nijak složité, a v neposlední řadě využívání terminologie nebo slangu pro utvrzení totožnosti. Útočníci podvodné emaily vybavují formuláři, které zjednoduší odeslání citlivých informací. Jinou možností je přidání odkazu na URL s předpřipraveným formulářem, který po vyplnění jde odeslat jednoduchým kliknutím. Ve většině případů je webová stránka přesnou kopií stránky původní. Navíc adresa je podobná originální, je zde zneužíváno záměn písmen za číslice. Pěkný případ je záměna písmena malé L „l“ za číslici jedna „1“, tohoto si všimne jen opravdový odborník nebo hodně nedůvěřivý uživatel. Phisher je omezen pouze svou fantazií, při tvorbě podvodných emailů. Jak se bránit a ukázky uvedu v praktické části. [10] [12]

4.3 Pharming

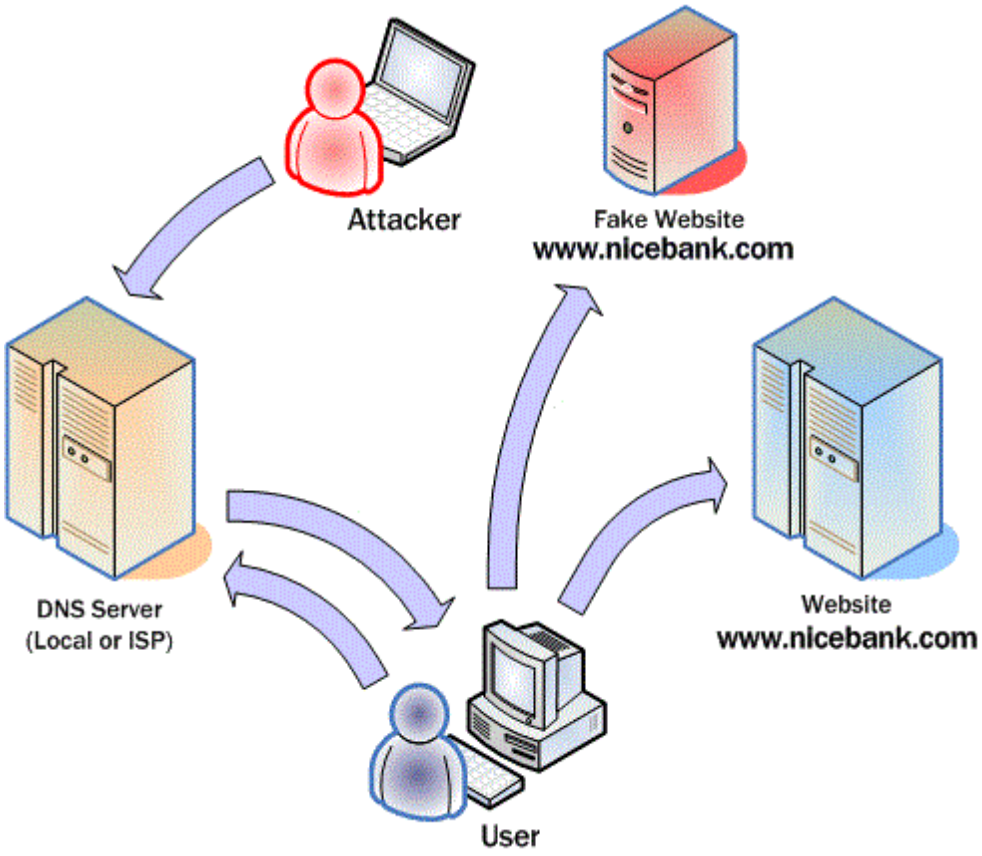
Můžeme ho považovat za nástupce phishingu nebo jako vylepšenou techniku, jak získávat citlivé údaje. Na rozdíl od phishingu, kde se vás snaží oklamat pro vstup na podvodnou stránku, u pharmingu dochází k automatickému přesměrování na podvodnou webovou stránku a to bez vašeho vědomí. Jsou dva způsoby, jak útočník může docílit tohoto podvodu. Jako první případ je infiltrace uživatelova počítače virem nebo malwarem.

Poté provádí technické úpravy na počítači. To znamená i po zadání korektní adresy dojde k automatickému přesměrování. Na obrázku 2 je vyobrazen způsob fungování této metody. Tento druh pharmingu bývá většinou identifikován antivirovými nebo antispywarovými aplikacemi.

Druhý složitější způsob, navíc je z počítače uživatele téměř nezjistitelný a je obtížné se proti němu bránit. Hacker napadne vnější DNS server a pokud se mu podaří změnit DNS záznam například u internetového bankovnictví tak veškerý přístup na stránky je přesměrovaný jinam. DNS server má za úkol překládat názvy stránek na odpovídající IP adresy. Je to z toho důvodu, že lidé si lépe pamatují slova než čísla, proto se tyto servery používají. Tento způsob je graficky vyjádřen na obrázku 3. Zde vidíme, jak napadl útočník server a při pokusu a vstoupení na požadované stánky nás přesměruje na stránky falešné. Tady si útočník pouze stáhne údaje, co mu tam vložili oběti. Stránky jsou opět podobné svým originálům, jenom mohou mít navíc nějaké nestandardní údaje. [11] [13]



Obrázek 2 Phrarming pomocí škodlivého kódu [11]



Obrázek 3 Pharming přes útok na DNS server [23]

II. PRAKTICKÁ ČÁST

5 JAK SE BRÁNIT UVEDENÝM RIZIKŮM

V této části proberu způsoby jak se chránit před různými riziky, které jsem popsal v teoretické části. Všechna rizika jsou vážná a většina z nich může zničit všechnu vaši práci nebo ji darovat někomu cizímu a ještě ke všemu přijít o svá hesla a tím se stát obětí trestného činu.

5.1 Antivirová ochrana

Antivirové programy dělíme do několika skupin. Všechny jsou naprogramované pro boj se škodlivým softwarem. Výrobců takovýchto programů je opravdu spousta, často se liší svým vybavení nebo licencí.

5.1.1 Jednoúčelové antiviry

Jsou to antivirové programy vytvořené k prohledávání a zjišťování přítomnosti viru a jeho následné odstranění, ale jen buď jistého druhu, nebo jen omezené skupinky virů. Tento druh antivirové ochrany nemůžeme použít jako plnohodnotnou ochranu. Příkladem jsou Trojan Remover, Panda Quick remover, Symantec atd.

5.1.2 ON-demand skenery

Tento skener bývá většinou součástí antivirových systémů, ale některými vývojářskými společnostmi bývá nabízen buď zdarma, nebo jako shareware. Nejčastěji jde o jednoduchou verzi OS DOS, která se ovládá pomocí příkazového řádku. Tohoto se využívá hlavně k mazání virů při nefunkčnosti os MS Windows.

Naproti tomu existují online skenery, které výrobci provozují na svých stránkách. Běžně je to skript, který s pomocí internetového prohlížeče (Mozilla Firefox, Internet Exporer, Google Chrom atd.) prohledá pevný disk.[9]

5.1.3 Antivirové systémy

Systém je složen z částí, které kontrolují hlavní vstupní a výstupní místa, jimiž bývá infiltrace často vedena. Což jsou www stránky (s nežádoucími skripty, škodlivé soubory), přenosná média a elektronická pošta. Úplně všechny antivirové programy jsou vybaveny aktualizacemi jak samotného programu, tak i virových databází. Jako nadstandardní

výbavu můžeme považovat personální firewall. Příklady produktů jsou Avast!, Kaspersky, Eset NOD32. Moderní antivirové systémy obsahují nástroje, které pomáhají odhalovat různé druhy infiltrací. Jedním takovým to nástrojem je HIPS (Host Intrusion Prevention System). Je to nástroj, který sleduje chování procesů a programů, výsledky vyhodnocuje podle pravidel zadaných v jeho databázi. Při podezření upozorní uživatele na možnou hrozbu a případně, nechá uživatele vybrat jakou akci, má vykonat. Dalším pomocným nástrojem je takzvaný sandboxing nebo taktéž virtualizace. Tento nástroj slouží k emulaci prostředí, kde spouští programy a analyzuje jejich dopad na systém a tak dokáže identifikovat nakažený soubor. Navíc vše je pouze virtuální a nemůže tak dojít k rozšíření do systému nebo ztrátě dat. [4] [2]

5.2 Firewall

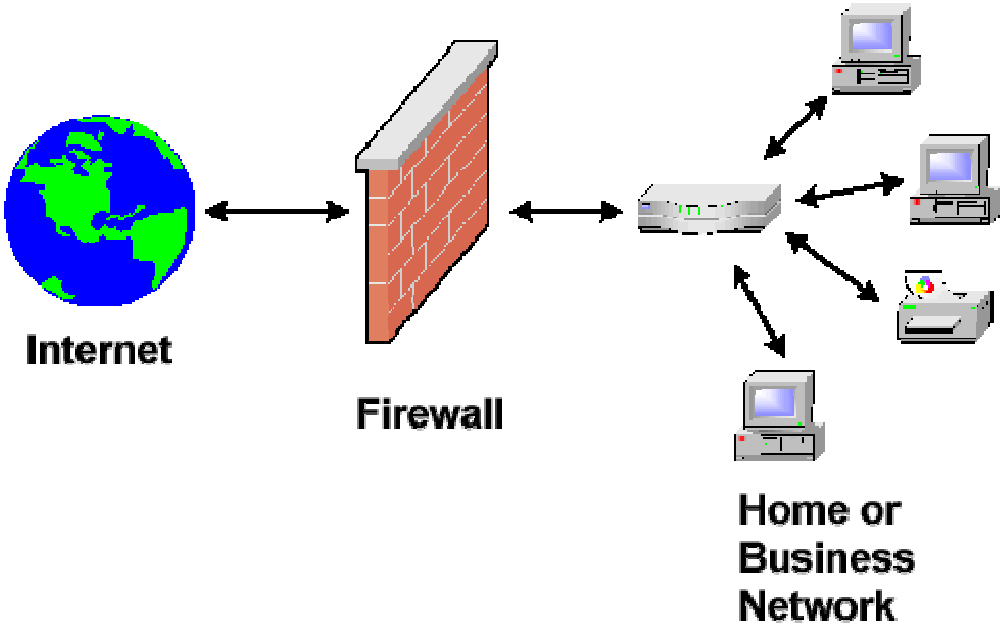
Pokud máme připojen počítač do sítě Internetu a nechceme se stát snadnou kořistí nějakého útočníka, vkládáme firewall mezi naši síť a Internet, jak je to zobrazeno na obrázku 5. Základní funkcí je bránit v navázání neautorizovaných spojení mezi internetem a sítí. Firewally jsou jak hardwarové, softwarové, anebo jejich kombinace. Hardwarový firewall je aktivní zařízení, přes které probíhá celá síťová komunikace, to znamená na jedné straně je internet, na straně druhé počítač. Firewally takového typu se používají hlavně u rozsáhlých počítačových sítí nebo u serverů. Pro domácí nebo malé sítě postačují firewally softwarové (Windows firewall, ZoneAlarm, Comodo Firewall a jiné). Tento software je nainstalován na uživatelském počítači. Ten je spuštěn zároveň s operačním systémem. Všechna data opouštějící privátní síť jsou kontrolovaná, pokud splňují podmínky pokusu o infiltraci, tak je spojení omezeno. Hlavně tedy riziko zvnějšku sítě. Kromě této hlídací funkce muže vytvářet statistiky, ze kterých se může stát zdroj pro kontrolu bezpečnosti sítě.

Známe dvě základní skupiny firewallů. Paketové filtry a aplikační brány. Router ve většině případu filtruje pakety podle zdrojové a cílové adresy a portu paketu. Omezením přístupu na i z internetu určitých protokolů nebo počítačů můžeme zabránit některým útokům. Také se používá stavová paketová filtrace. V současné době se stává základní částí firewallu, který si pamatuje stav spojení. Můžeme to popsat tak, že firewall ví, jestli bylo spojení otevřeno z vnitřní sítě a na základě toho povolí spojení navázané i opačně. Nekontroluje obsah, ale řídí jenom komunikaci. Tuto kategorii představují implementace

linuxových firewallů nebo firewall CheckPoint, u nich se tato filtrace nazývá Stateful Inspection. Rozdíl mezi filtry a aplikační bránou je v rychlosti a transparentnosti. Nevýhodou je nemožnost upozornění na neúspěšný pokus proniknout do sítě.

Aplikační proxy brány přepínají veškerou komunikaci na základě stanovených pravidel. Komunikaci nepropouštějí, ale sami realizují spojení z vnějšího světa. Toto spojení je vždy ukončeno na firewallu. Nevýhodou je podpora omezeného množství protokolů, protože přidání dalšího protokolu bývá náročné a pomalé. Na obrázku 4 je přehledně popsáno, co kontrolují jednotlivé úrovně firewallu. Paketové filtrování kontroluje pouze paketovou hlavičku, stateful paketová filtrace kontroluje paketovou hlavičku a stav spojení a aplikační úroveň filtrování jak paketovou hlavičku tak stav spojení, a navíc kontroluje aplikační data. [2]

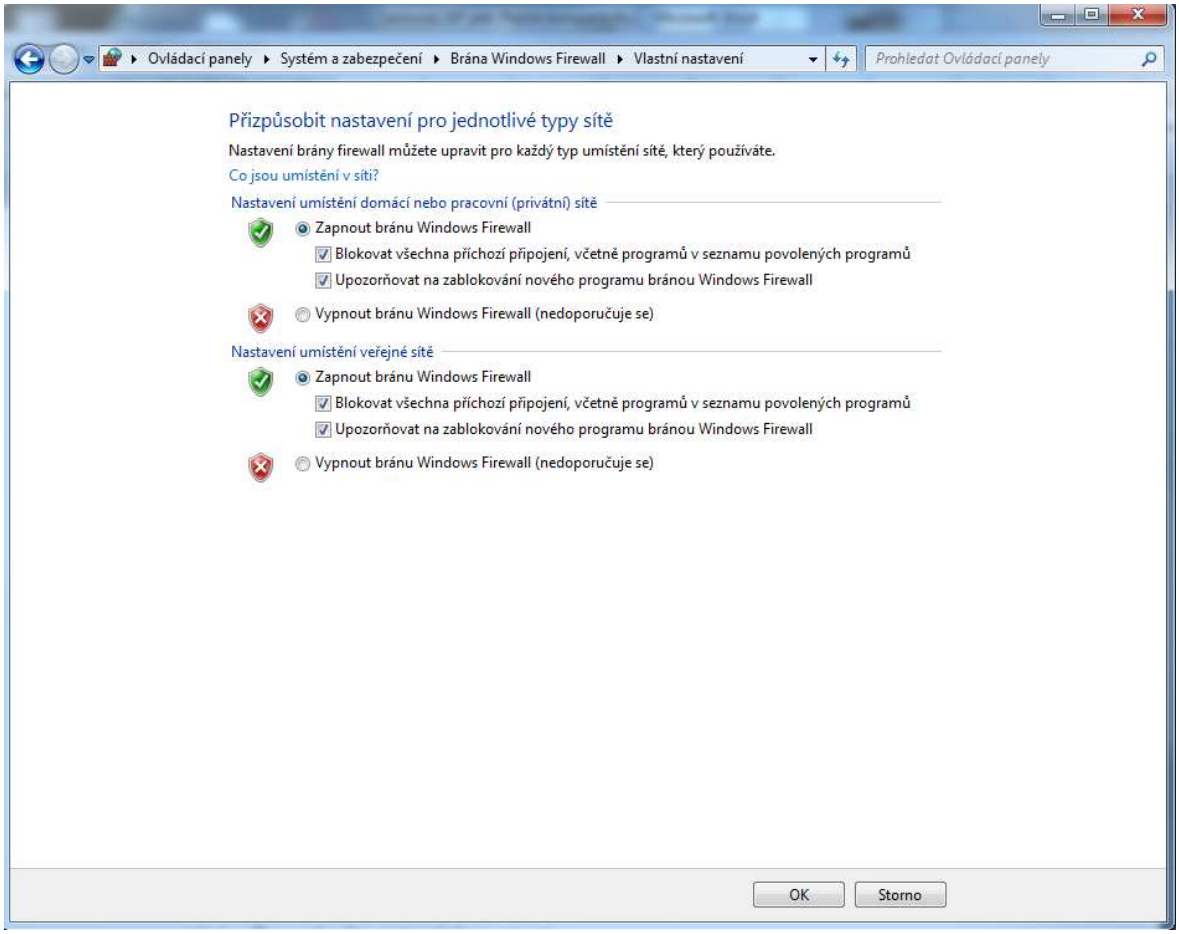
Obrázek 4 Jednotlivé úrovně filtrování komunikace[20]



Obrázek 5 Ukázka firewallu[24]

5.2.1 Nastavení brány firewall ve Windows 7

Windows 7 obsahuje bránu firewall, která brání vstupu hackerům a škodlivému softwaru. Její výchozí nastavení je zapnuto, tak že po nainstalování operačního softwaru je spuštěna. Políčko s nastavením blokovat všechna příchozí připojení, včetně programů v seznamu povolených programů je výhodné používat, pokud jste připojeni na veřejnou síť, například v knihovně nebo v restauraci. Toto nastavení zamezí nevyžádaným pokusům připojení k počítači. Výhodou tohoto nastavení je, že zajišťuje maximální ochranu na veřejné síti, všechny programy včetně programů ze seznamu povolených jsou blokovány. I když jsou všechna příchozí připojení zablokována, nebrání v zobrazení většiny webových stránek včetně posílání a přijímání emailu. Kdybychom toto nastavení používali doma nebo v práci, kde jsme připojeni na síť, mohlo by to pro nás být dost omezující. Nastavení „upozorňovat na zablokování nového programu bránou Windows Firewall“, když je políčko zaškrtnuté tak nás brána firewall upozorní na zablokovaný program a dá nám možnost ho odblokovat. Vypnutí brány Windows Firewall není doporučováno z důvodů deaktivace jakéhokoliv filtrování. To dovolí hackerům vstup do vašeho počítače. Vypnout ji můžeme, pokud jsme si nainstalovali jinou bránu firewall od některé vývojářské skupiny, a to z důvodu kolizí mezi těmito dvěma softwary.[14]



Obrázek 6 Dopručené nastavení brány Windows 7 Firewall pro veřejnou síť [7]

5.3 Ochrana proti spyware

Spyware je škodlivý software, proti kterému je potřeba se bránit a pokud dojde k infiltraci tak jej dokonale odstranit. K ochraně můžeme používat buď programy s úkolem chránit před možnou nákazou, nebo slouží k odstranění špionážní aplikace.

5.3.1 Úroveň uživatelových znalostí

Znalosti jsou jedním z nejdůležitějších kriterií, pro ochranu před tímto škodlivým softwarem. Většina uživatelů nepovažuje riziko spywaru za nějak závažné nebo o něm ani neví. Každý říká: „Mě se to stát nemůže!“. Bohužel může a taky je možné, že aplikace je už v systému a odesílá informace útočníkovi. Proto je důležité, aby se lidé v této problematice začali orientovat. Firmy by měly provádět pravidelná školení, aby si zaměstnanci udrželi jistou úroveň znalostí. U běžných uživatelů je utopie provádět nějaká školení, ale sami uživatelé by měli dělat maximum, pro zvýšení zabezpečení svých dat.

V tomto kybernetickém světě je třeba si dávat pozor na vlastní dokumenty. Tyto skutečnosti jsou způsobeny také představou vlastnictví. Lidé si stále myslí, že něco vlastnit znamená moci si to osahat, bohužel nyní duševní vlastnictví je větším lákadlem než fyzický předmět.

5.3.2 Obezřetnost a pečlivost

Pokud mám v plánu instalovat pomocnou aplikaci do vlastního počítače, tak bych si měl dávat pozor na jistá kritéria, kterých by se měl držet každý uživatel. První zní, potřebuji tento program? Je od důvěryhodného zdroje? Jak jsou s ním spokojeni ostatní uživatelé? A jedna velmi zásadní, neobsahuje nějaký adware nebo spyware? Pokud je tento program nutný a neobejdete se bez něj, pokud program pochází od nějaké známé programátorské skupiny, tak bychom se nemuseli bát, adware bude pouze volitelný a měl by jít instalovat i bez tohoto doplňku. Před instalací je dobré se podívat po různých recenzích toho softwaru, raději projít více zdrojů, u některých by mohlo jít o úmyslné klamání. V dnešní době je máloco zdarma. Při samotné instalaci je potřeba si přečíst licenční dohodu, jestli je ve smlouvě zmínka o tom, že data budou posílána nějaké třetí osobě, tak silně doporučuji zrušit instalaci a zkusit najít jiný software a svá data nechat v bezpečí.

Lidé jednají bezmyšlenkovitě, nečtou licenční dohodu. Je to dáno buď částečnou leností, nebo snad šetřením času, jenomže tito lidé si neuvědomují závažnost situace. Nejde jen o zpomalení systému, nebo nedej bože ztrátu dat, ale ušetřením deseti nebo patnácti minut při instalaci, může dezinfekce počítače zabrat i hodiny a navíc pokud na to člověk potřebuje profesionála, tak musí počítat i s finančními výdaji. Tvůrci spywaru spoléhají na to, že se uživatel nechce zabývat čtením nebo kontrolou toho co instaluje, ale čekají od uživatele odkliknutí všeho, co požadují. Proto doporučuji nikam nespěchat, vše si důkladně přečíst, a pokud něčemu nerozumím, tak se zeptat někoho, kdo se v tomto oboru orientuje, nebo se podívat na Internet, protože ten je nevyčerpatelná studnice moudrosti.

5.3.3 Vzájemná provázanost systému

Představme si ji jako budovu, u té zabezpečujeme na několika úrovních. Je to ochrana perimetru, plášťová ochrana a nakonec předmětová ochrana. Začneme ochranou perimetru, to je zeď nebo plot s bránou v informační technice je to firewall. Průchod ven i dovnitř je hlídán strážným a ten rozhoduje, kdo může projít. U firewallu jsou to vstupní a

výstupní pakety. Po areálu se pohybuje hlídka (antivirový program a antispywarový program), ta má na starosti hledat ukrytý spyware a nezvyklé chování aplikací. Další úrovní je budova, tu můžeme považovat za zabezpečení vlastního operačního systému, brání před převzetím kontroly nad počítačem. Předmětová ochrana je v tomto virtuálním objektu, zaměřena na soubory. K jejich ochraně můžeme využít kryptografii a soubory zašifrovat nějakou složitější šifrou. Pokud bude celý systém pracovat a uživatel bude obezřetný, tak je pouze malé riziko nákazy.

5.4 Ochrana proti praktikám sociálního inženýrství

Jak jsem uvedl již v teoretické části, jedná se o oklamání lidské důvěřivosti. Hlavním představitelem sociálního inženýrství je světově známý hacker Kevin Mitnick. Ten byl za své činy několikrát odsouzen. Jako zásadní praktiky jsem vybral rybaření, jak se říká česky phishingu a pharming. Útoku přímo sociotechnik y je obtížné se bránit, ale jde to. Ukážeme si to na příkladu. Pracuji ve firmě s víc jak 20 zaměstnanci, přijde za mnou nebo mi zavolá člověk, který se představí jako někdo mě nadřízený, chce nějaké dokumenty a čím dřív tím líp nebo ať mu dám přihlašovací údaje a on si dokument stáhne sám. Jsou tři možnosti. Budu mu věřit a pošlu dokument nebo mu dám heslo, v opačném případě zkontroluji, zda někdo takový opravdu existuje a jestli ten dokument potřebuje. Jeto trochu obtížné na psychiku odporovat nadřízenému, ale může to společnosti ušetřit spoustu peněz a starostí. [5]

5.4.1 Jak se chránit proti phishingu

Mezi hlavní prvky ochrany patří zaručeně obezřetnost. Počítač je nástroj a člověk ho ovládá, je logický stroj a podle toho funguje. Pokud s ním uživatel špatně pracuje, tak počítač to sám nezachrání.

Co dělat když se v příchozích zprávách objeví email z banky, u které mám otevřený účet. V předmětu zprávy je napsáno naléhavé. To by ve vás mělo vzbudit podezření, bohužel to většinou způsobí zrychlení přemýšlení a to vede k tomu, že se z vás stane „phish“.

Věc, kterou opravdu nedoporučuji dělat, je přecházet na weby v těle emailu. Příklad známého phishingu na Českou Spořitelnu (obrázek 7). Dodržování tohoto pravidla je dobré i při spamu. Když se stane, že by nějaký institut chtěl vyplnit dotazník, kde by se

objevovaly jisté citlivé informace, tak zcela jistě by použili zašifrovaný přístup „https[6]“. Vůbec není na škodu kontrolovat adresu, na které se nacházíte a u ní i platnost a důvěryhodnost certifikátů, pokud tam tedy nějaké jsou. U prohlížečů se to pozná podle zeleného pole s visacím zámkem v poloze zamčeno. Obrázek 8 znázorňuje podvodnou stránku, kde není jak šifrování, tak URL je jiná a certifikát úplně chybí. Můžeme si vypomoci různými doplňky prohlížeče (Netcraft Toolbar), ty by nás v případě phishingu měli upozornit na možné riziko. Česká republika není tolik v hledáčku phisherů, je to dáno složitostí jazyka, v tom máme jistou výhodu. Proto si musíme dávat pozor na emaily se špatnou diakritikou, v cizím jazyce nebo jiným fontem. Musíme čekat, že banka bude používat formální vzor a bude dodržovat jisté standardy. [12] [10]

[6] HTTPS - Hypertext Transfer Protocol Secure, nástavba síťového protokolu http a ta umožňuje zabezpečit komunikaci s webovým prohlížečem a webovým serverem

[SPAM] VISA Karty 4XXX-XXXX-XXXX-XXXX

Ceska - Verified by Visa [vsbv@csas.cz]

To: undisclosed-recipients:

VERIFIED by VISA

ČESKÁ SPOŘITELNA

Varování pred novou verzí podvodných e-mailu

Vázení klienti,

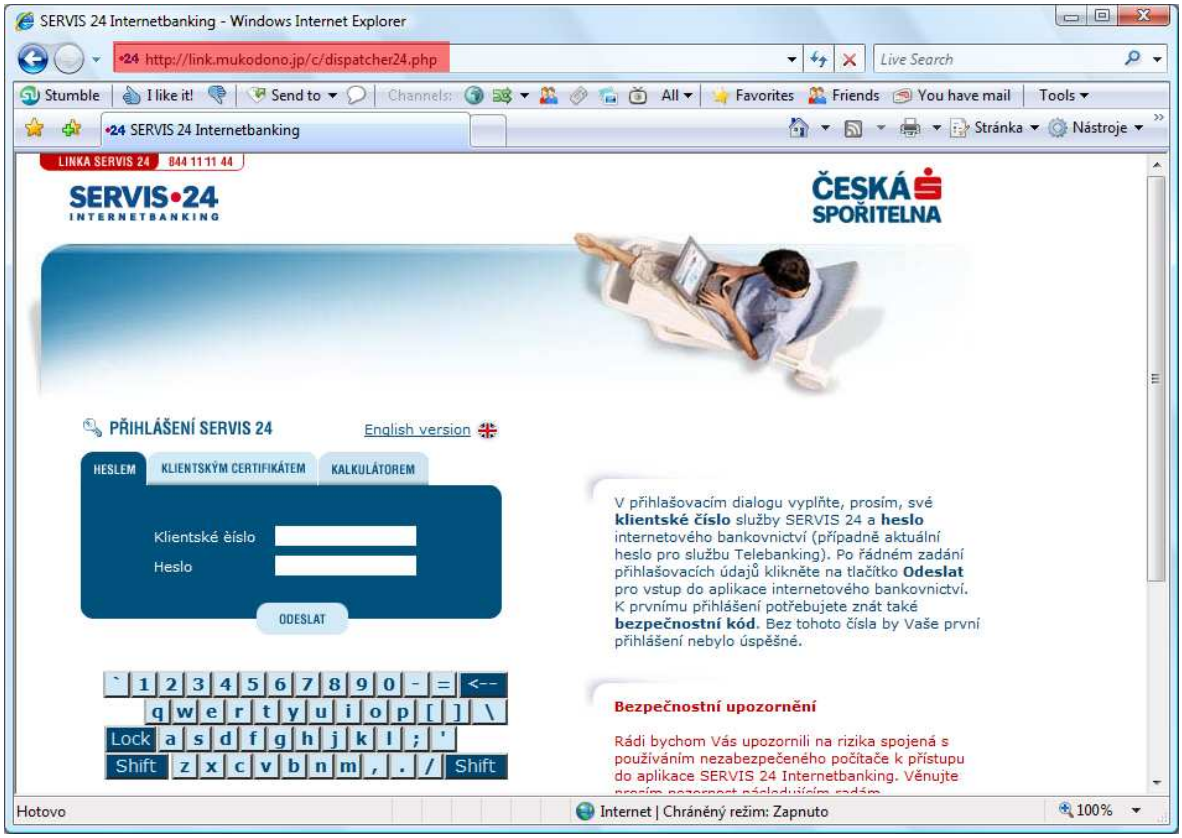
rádi bychom Vás upozornili na novou verzi podvodného e-mailu (tzv. phishingu). Nová verze e-mailu má jako ty predeslé vzbudit dojem, ze byla odeslána z e-mailové adresy Ceské sporitelny, tentokrát však z oficiální e-mailové adresy banky csas@csas.cz. Obsahuje odkaz v tele na údajné webové stránky internetového bankovnictví banky a uzivatel je vyzván k prihlášení, tedy zadání osobních bankovních údaju.

Prosím, verifikujte tuto emailovou adresu kliknutím na spojení níze:

https://www.servis24.cz/ebanking-s24/app/register.pl?code=2E1E-EBB6-EA1N-D1EC&step=vrf_email_actions

Verifikovací spojení je platné do 24 hodin.

Obrázek 7 ukázka podvodného emailu [21]



Obrázek 8 Ukázka podvodné stánky [21]

5.4.2 Jak se chránit proti pharmingu

Pharming je mnohem nebezpečnější než phishing, to je dáno jeho zákeřností. Tato metoda je tak účinná, že dokáže oklamat i zkušeného uživatele. Prohlížeče jsou vybavovány nástroji na odhalování podvodných webů a i ty občas nejsou schopny takovou stránku odhalit včas. Možnosti jak odhalit pharming založený na útoku na DNS server jsou rovny téměř nule. Naštěstí tyto útoky jsou hůře proveditelné a tak jejich četnost není nějak velká.

Naproti tomu ochrana proti lokální formě útoku závisí na funkčním, aktualizovaném a dobře nastaveném antivirovém systému. Program prochází soubory a hlídá všechny soubory posílané emailem a i stahovaný obsah webů. Útočníci důmyslně šifrují a vkládají do archivů, a proto antiviry kontrolují obsah archivu v době jeho rozbalení. Další možností jak se bránit, je používání nástrojů, co zobrazují informace o načítané webové stránce. Toto je však určeno hlavně pro pokročilejší uživatele počítačů. Pokud spoléháme na ochranu před podvodnými weby, tak musíme doufat, že stránku někdo již označil. Protože na tomto principu pracují nástroje na odhalování podvodných webů.

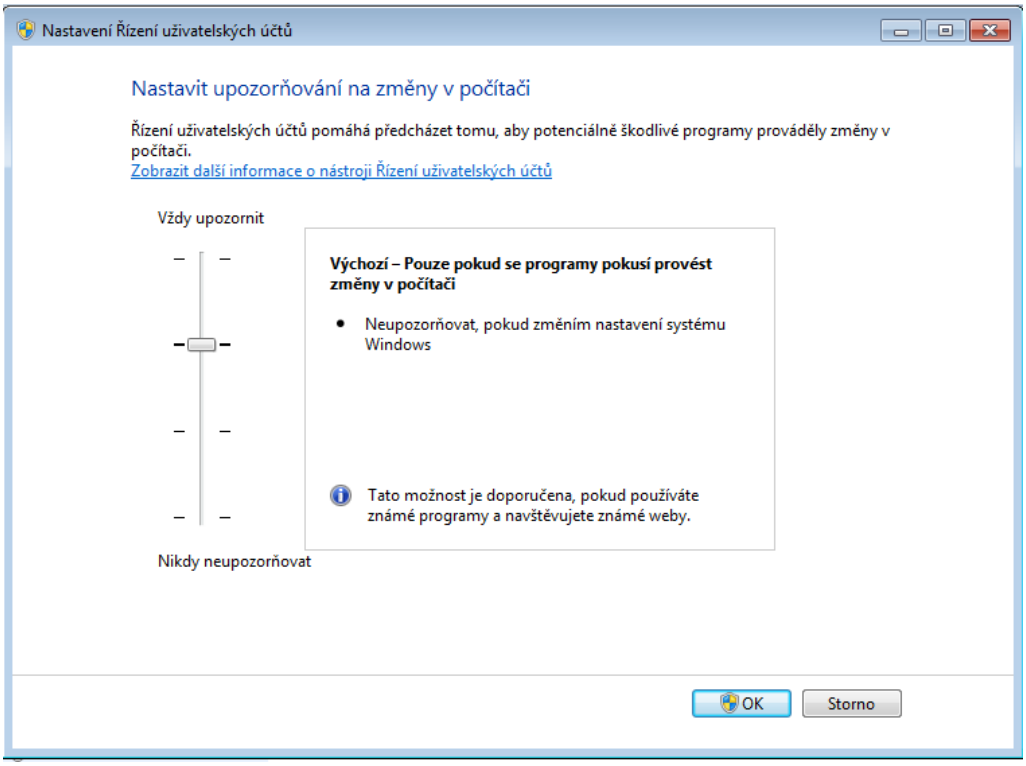
Rychlost odhalení podvodného webu nebývá vždy dostatečná, pokud jsou útoky zaměřeny na malé území (například česká spořitelna).

Obecná ochrana je důležitá pro snížení jakéhokoliv rizika útoku. A informovanost a nepodceňování rizika jsou důležité faktory, co vedou ke zvýšení bezpečnosti.[11] [13]

5.5 Nastavení systému Windows

5.5.1 Řízení uživatelských účtů

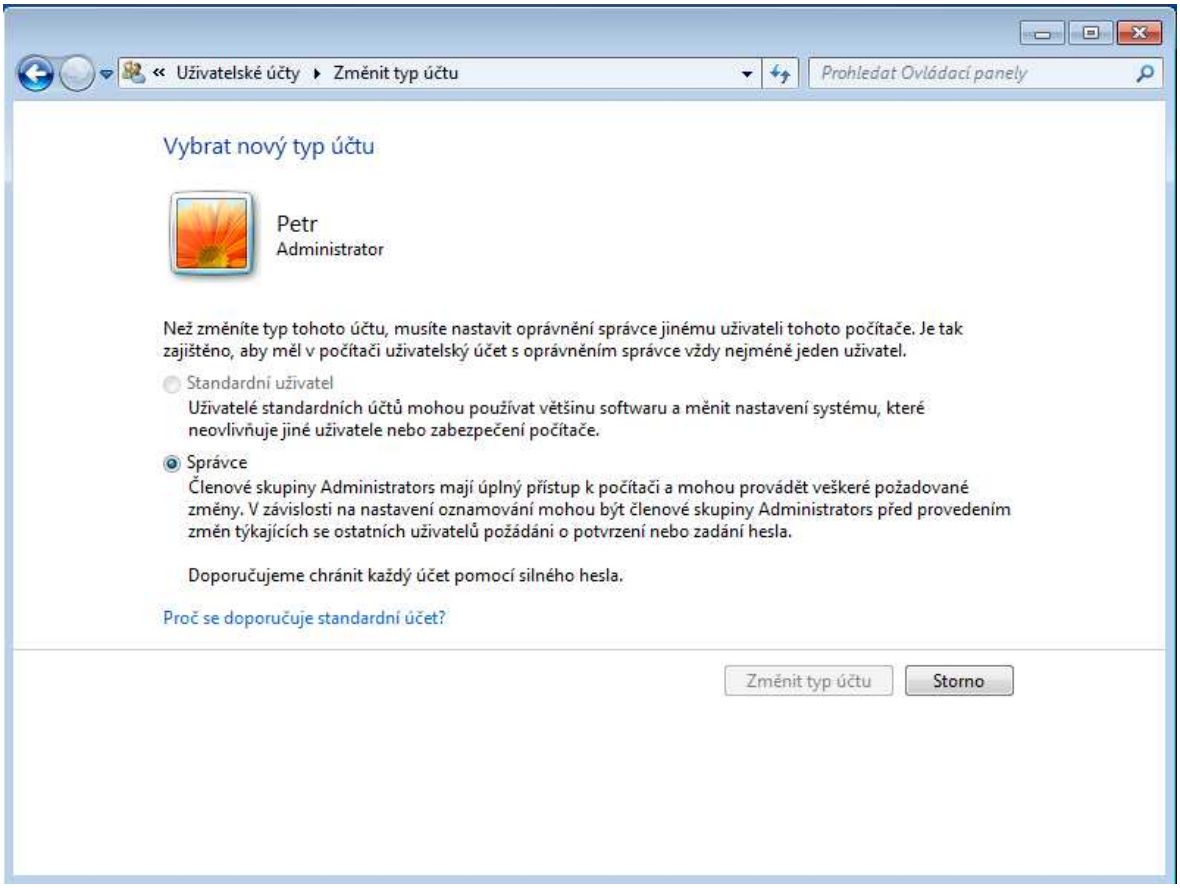
Nástroj ke zvýšení ochrany před hackery a škodlivým kódem. Toto se uplatňuje při pokusech o provedení větší změny na počítači. Na tuto akci upozorní a požádá o povolení. Uživatel si může vybrat ze čtyř různých nastavení. První a také nejhorší nastavení je „nikdy neupozorňovat“, nastavení, které rozhodně nedoporučuji. Neposkytuje dostatečnou úroveň zabezpečení, počítač je vystaven potenciálnímu riziku, všechny programy mají povoleno provádět změny v počítači. Dalším nastavením je „Upozorňovat pouze v případě, pokud se programy pokusí provést změny v počítači (nestmívat plochu)“, také po uživateli žádá o povolení programu na provedení změny, které vyžadují povolení správce. Rozdíl mezi tímto a nastavením o úroveň víš je. Dialogové okno se nezobrazuje na zabezpečené ploše, takže program může manipulovat podobou tohoto okna. Doporučeným nastavením na obrázku 9, je označeno jako výchozí „Upozorňovat pouze v případě, pokud se programy pokusí provést změny v počítači“ upozorňuje, pokud program potřebuje povolení správce, k provedení změny v počítači nebo systému Windows. Nejvyšším stupněm ochrany je „upozornit vždy“, dialogové okno se zobrazuje na zabezpečené ploše, to znamená, že plocha je ztmavená a není možné spuštění jiného programu. Toto nastavení je dobré používat při častých návštěvách neznámých stránek a instalaci programů od neznámých vydavatelů. Důležité je také číst si dialogová okna, abychom věděli, co povolujeme.[25]



Obrázek 9 Doporučené nastavení Řízení uživatelských účtů[7]

5.5.2 Účty a práva

Dobrým bezpečnostním opatřením je nepoužívání správcovského účtu. Účet správce dovoluje instalovat jakýkoliv software, proto je výhodné použít standardní uživatelský účet, hned po dokončení nastavení celého systému. Ten dovoluje používat nainstalované programy, nemůžeme instalovat a odinstalovat software ani hardware, mazat soubory potřebné k provozu počítače a měnit nastavení počítače ovlivňující bezpečnost uživatelů. Některé programy mohou vyžadovat před provedení určitých procesů, zadání hesla správce. Vytvoření účtu se provádí po přihlášení jako správce, v nabídce start vybereme ovládací panely, zde uživatelské účty a provedeme vytvoření uživatelského účtu. Zde vybereme nastavení „standardní uživatel“ vzhled okna vidíme na obrázku 10. [26]



Obrázek 10 Nastavení typu účtu [7]

6 TESTOVÁNÍ SYSTÉMU

Probíhalo na systému Windows 7 Home basic. Tato verze bývá nejčastěji dodávaným operačním softwarem u běžných počítačů určených pro domácí použití. Operační systém jsem nainstaloval do virtuálního počítače vytvořeného pomocí programu VMware Player. Virtuální počítač bude mít dvoujádrový procesor 2.0 GHz a velikost paměti RAM[7] bude 1.3 GB. Samotný test jsem prováděl programem PC Security test 2013. Během jednotlivých testů, budu měřit zatížení procesoru a paměti RAM. Pomocí programu PC Brother Memory Optimization, z kterého bude výstupem graf zátěže. Po dokončení instalace jsem provedl zálohu, kterou jsem používal jako základ při každém dalším testu. Samozřejmě jsem u Windows 7 stáhl a nainstaloval všechny aktualizace a použil jsem doporučená nastavení. Webový prohlížeč byl aktualizován na verzi 10.

Program PC Security test 2013 obsahuje tři úrovně testu:

Antivirus protection test – testuje reakci antivirového programu. První částí je zabezpečení registru při startu Windows. Další část simuluje infikaci testovacím známým virem od EICAR. Následující prvek simuluje infikaci neznámým virem. Poslední test simuluje napadení paměti virem.

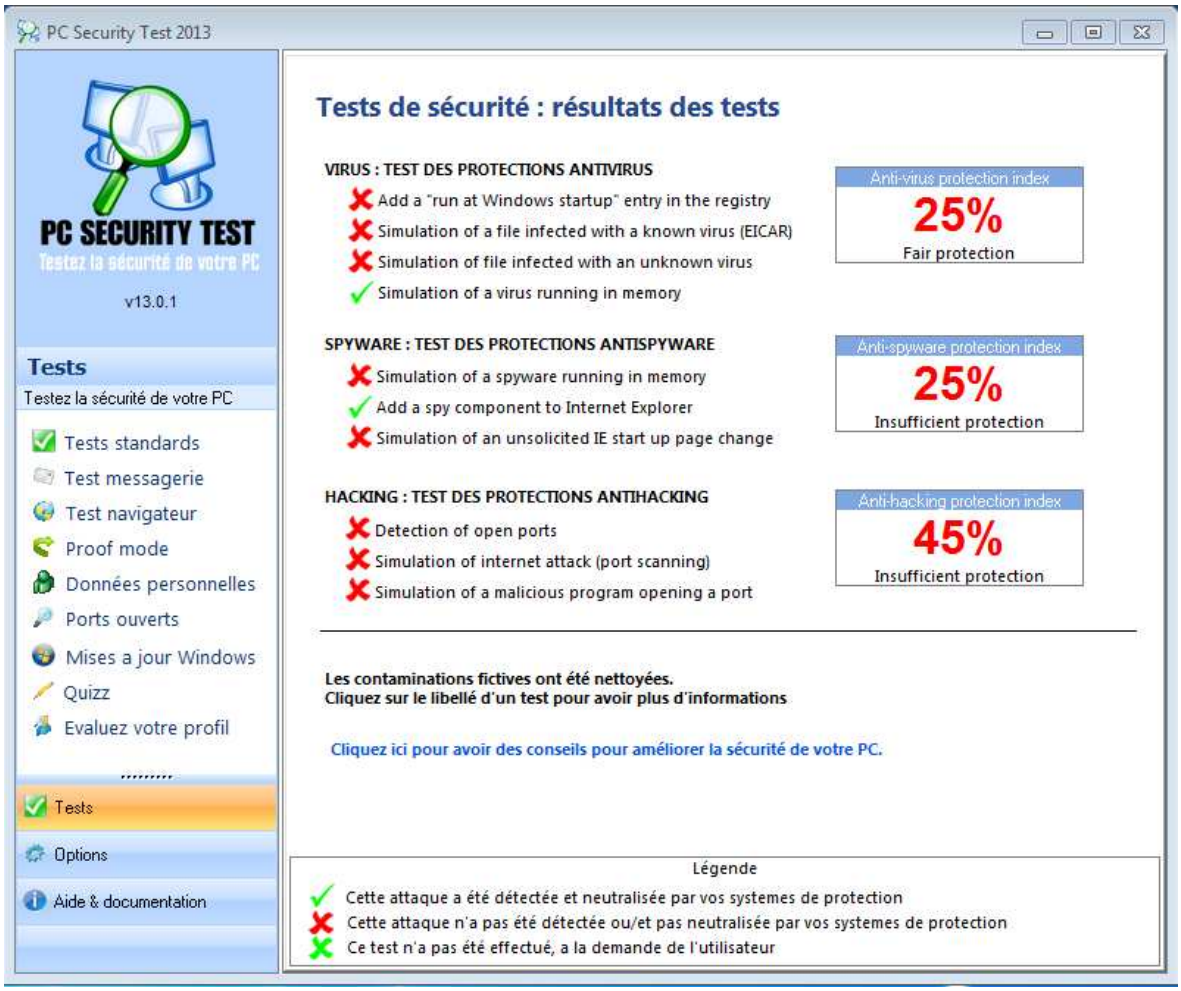
Antihacking protection test – Tato úroveň testuje firewall. Zabezpečení otevřených portů. Simulace útoku hackera pomocí skenování portů. Simulace škodlivého programu otevírajícího porty.

Antispyware protection test – jak už z názvu vyplývá, jedná se o test s několika úrovněmi spywarové ochrany. Simuluje infikaci paměti spywarem, útoku spyware přes webový prohlížeč a zabezpečení před nevyžádanou změnou start-up stránky prohlížeče Internet Explorer

[7] RAM – Random-access memory, je to paměť s libovolným přístupem, tato paměť je součástí každého počítače

6.1 Windows 7 Home basic

Po nainstalování programu na testování jsem provedl test nezabezpečeného systému Windows pouze s aktivním Firewallem. Jelikož systém Windows 7 obsahuje pouze základní prvky, což zaručeně znamená, že bychom ho neměli používat, dokud nenainstalujeme antivirový a antispywarový program. Brána firewall taky není dostatečně bezpečná. Neobstála při detekci otevřených portů ani simulovanému útoku z internetu a simulace otevření portu.

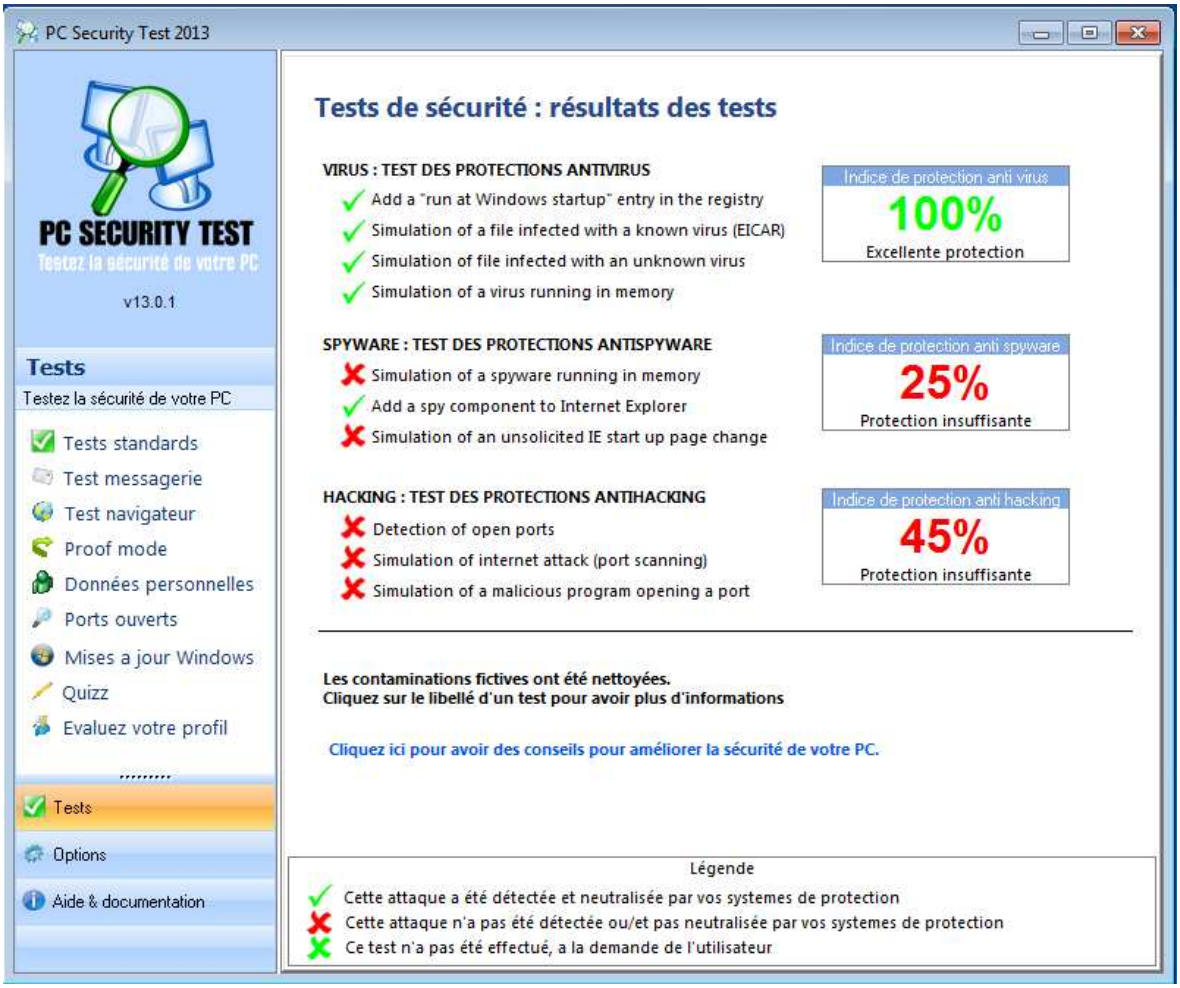


Obrázek 11 Test systému bez antivirového programu[7]

6.2 Avast! Free Antivirus 8.0.1489

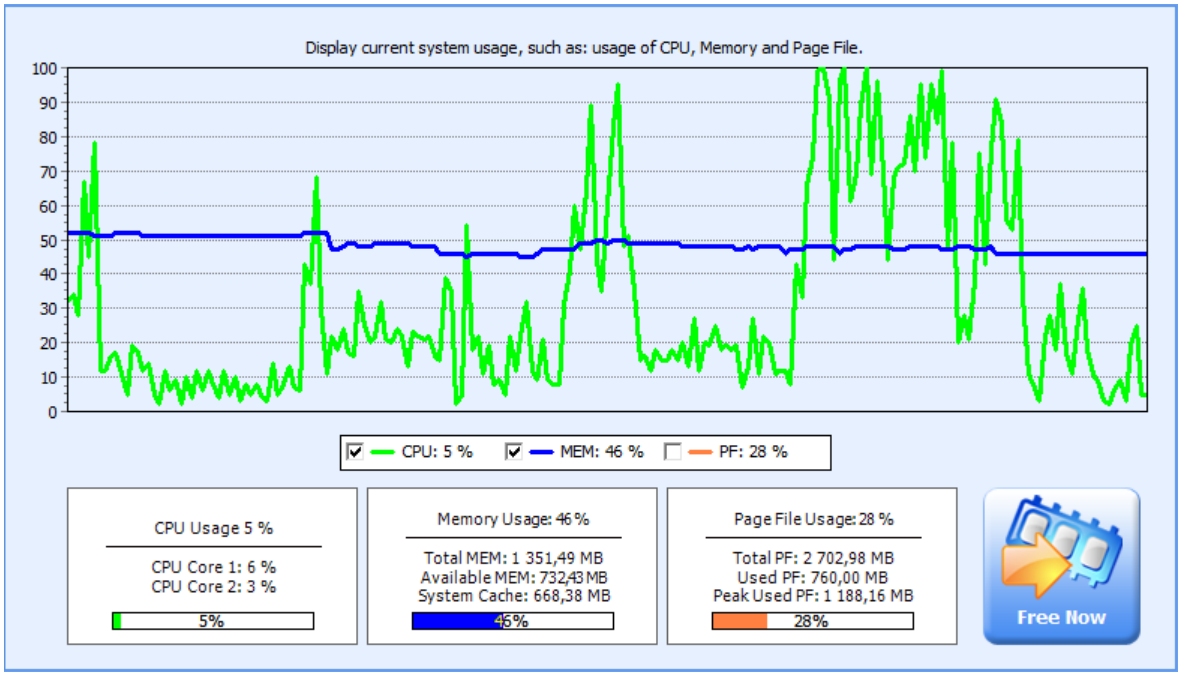
Je to freewarový software, jednoduchý na ovládání. Samotná instalace není nijak složitá, je kompletně český. Vybral jsem ho z důvodu rozšířeného používání mezi uživateli. Dalším důvodem byl dobrý výsledek na stránkách AV-comparatives.org, kde získal v testu výkonu z března a května 2013, ocenění advanced+, v detekci souborů

advanced. U posledního testu antiphishingu ze srpna 2012, kde zablokoval 82,2% phishingu. Obsahuje antivirové jádro, rezidentní ochranu před rootkity, detekci potenciálně nežádoucích programů, behaviorální štít, štít souborového systému, mailový štít, webový štít, štít peer-to-peer (P2P), štít IM, síťový štít, technologii WebRep, která poskytuje hodnocení spolehlivosti stránek. [16] [19]



Obrázek 12 Test systému s antivirovým programem Avast! [7]

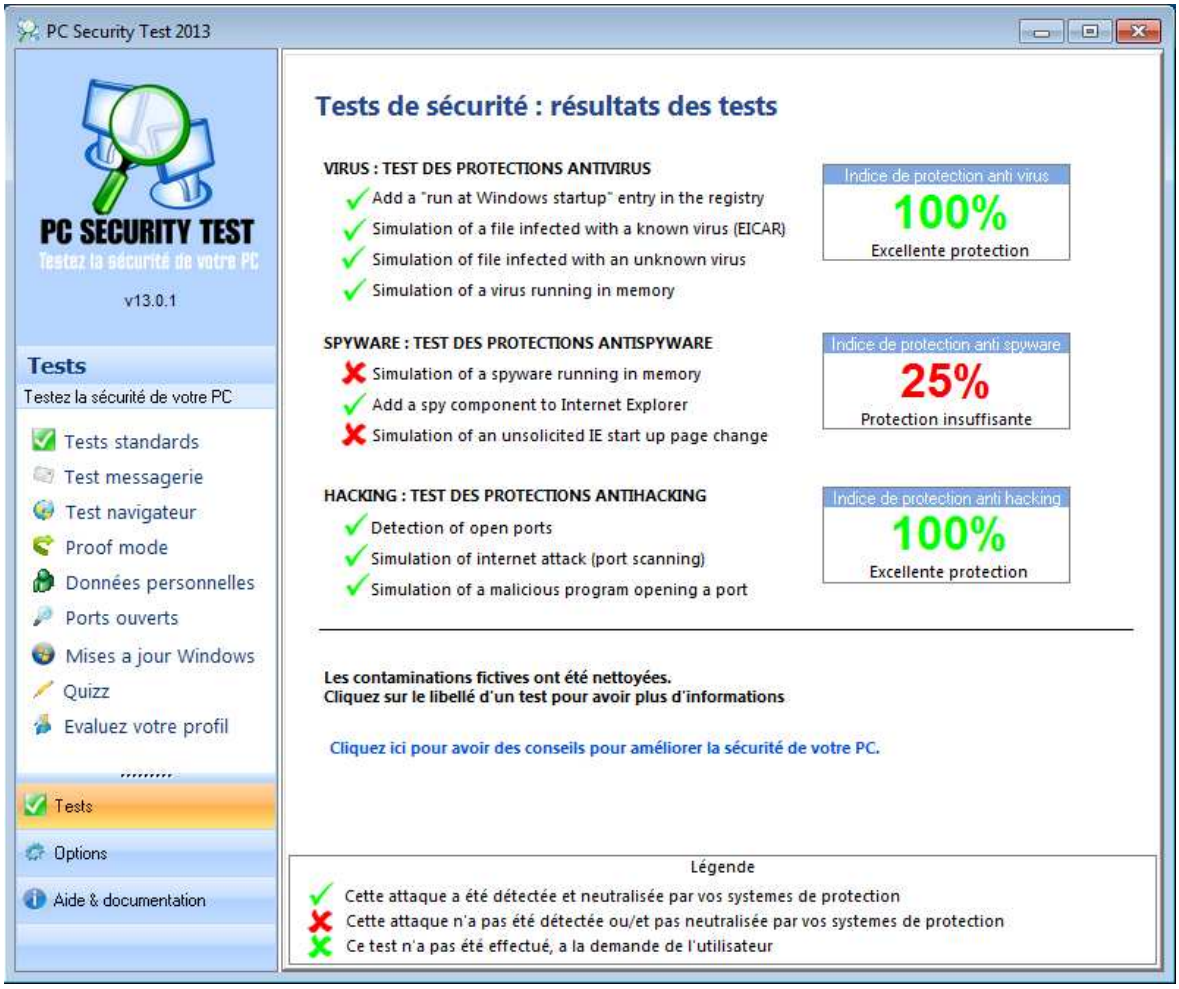
Test antivirového programu dopadl úspěšně, program odhalil všechny virové pokusy o infiltraci, bohužel neobsahuje antispywarový program, proto je výsledek stejný jako u nezabezpečeného systému. Firewall také není součástí balíku, ale dá se stáhnout jako samostatný program. Zatížení procesoru je dost proměnlivé. Na začátku testu se zvyšuje na 80%, poté opět klesá. Špičky zatížení dosahují i 100%, jak je vidět na obrázku 13. Paměť RAM je využívaná téměř konstantně kolem 50%.



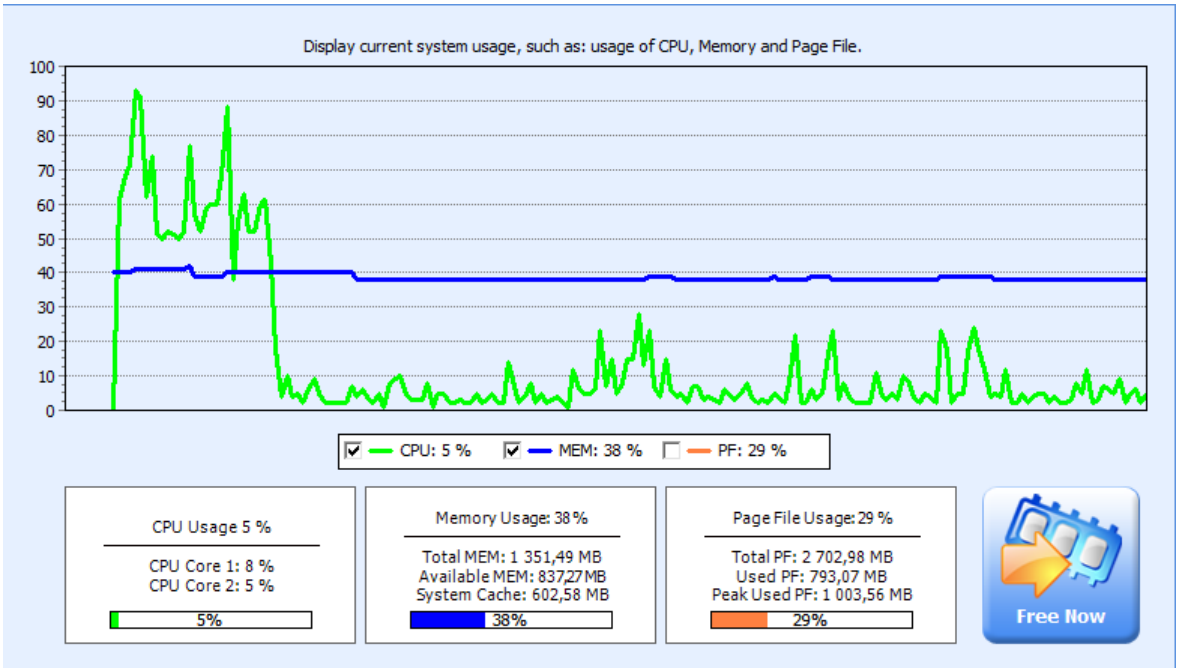
Obrázek 13 Zatížení procesoru a paměti RAM při testu [7]

6.3 Bitdefender Antivirus 2013 Plus

Instalace tohoto softwaru byla proti Avastu! delší, protože při instalaci provádí skenování systému. To vede k odhalení škodlivého kódu ještě před nainstalováním a nemělo by dojít k napadení souborů antivirového programu. Také obsahoval firewall, který úplně zablokoval všechny pokusy o průnik. Takže je to plus tohoto softwaru. Práci antivirového programu můžeme považovat za plně vyhovující. Bohužel balík neobsahoval proti spywarovou ochranu. Tento software je dodáván jako zkušební verze s omezením na 30 dní. Za celou dobu testu zatížení procesoru nedosáhlo 100%, pouze na počátku se pohybovalo v rozmezí 50 až 90%. Zatížení RAM se pohybovalo kolem 40%. To svědčí o dobré odladěnosti tohoto programu. [17]



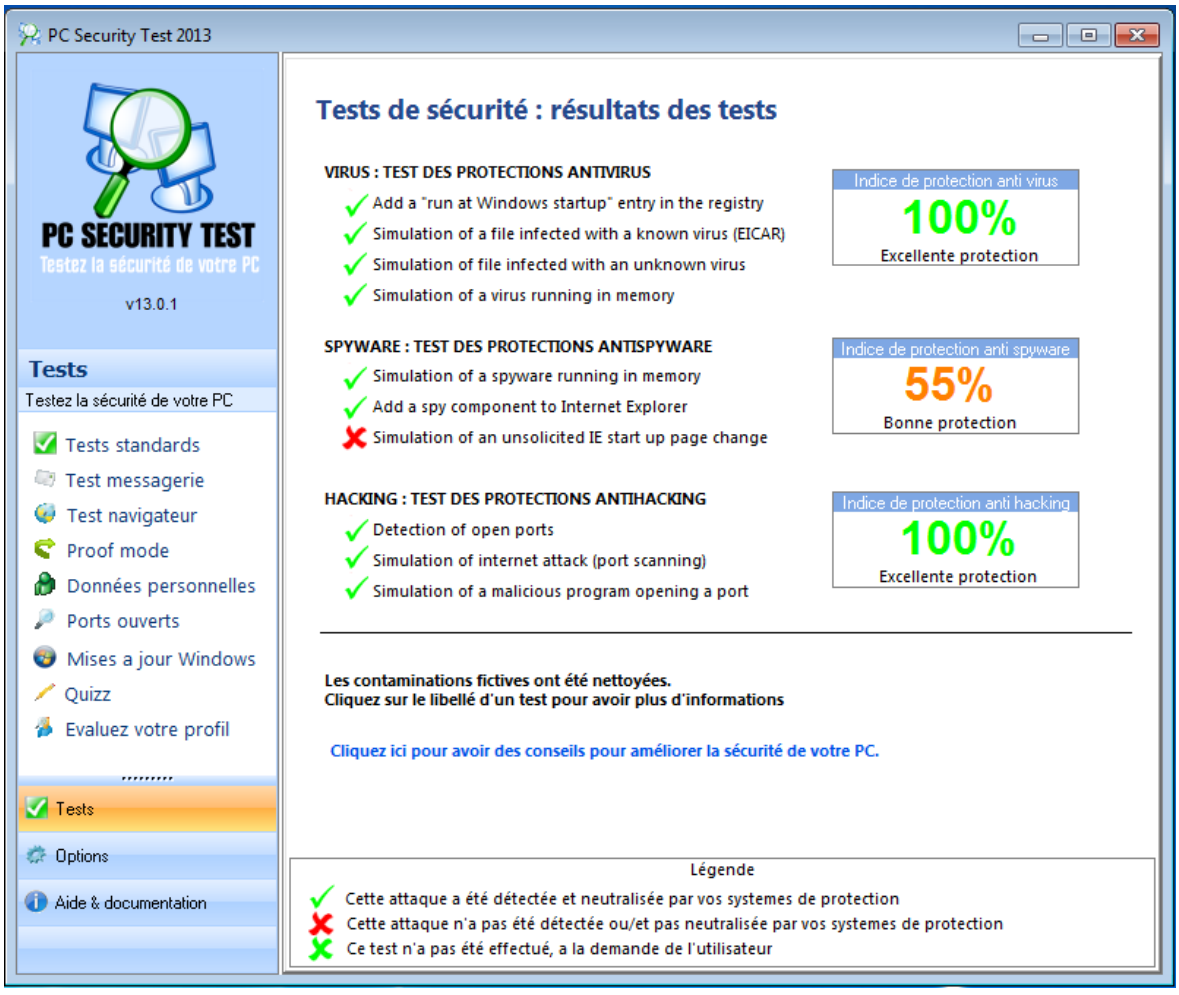
Obrázek 14 Výsledek testu systému s BitDefendrem [7]



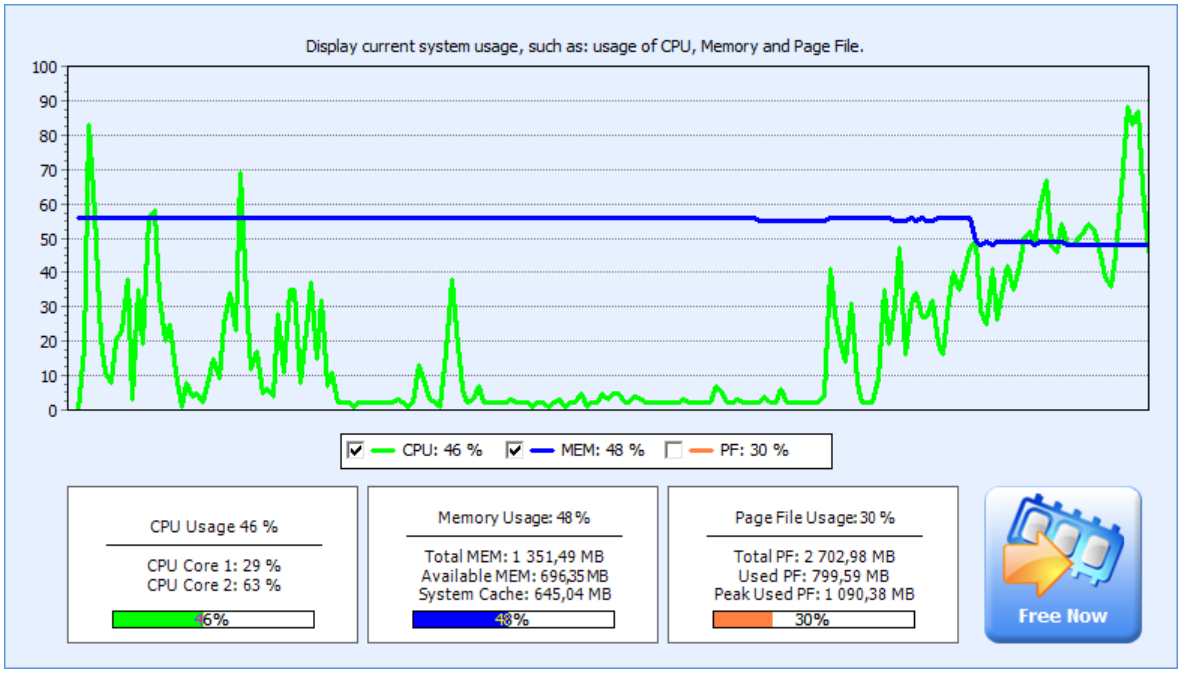
Obrázek 15 Průběh zatížení procesoru a RAM při testu [7]

6.4 ESET Smart Security 6

Oblíbený dobře hodnocený antivirový program, bohužel má pouze omezenou licenci na 30 dní. Při testu antivirového systému uspěl dobře ze 100 % úspěšností. Rozpoznal pokus o vložení testovacího viru, jak známého tak i neznámého. Antispywarová ochrana odhalila simulaci spywaru v paměti, tak i pokus o vložení komponentů do programu Internet Explorer. Ziskem 55% ukázala, že je dostačující. Integrovaná brána firewall zachytila pokusy o průnik do systému pomocí tří nejčastějších metod. Proto brána firewall získala 100%. Tento program je plně dostačující a může se použít jako kompletní ochrana počítače. Během testu se využití procesoru pohybovalo maximálně do 90% a to pouze na začátku a na konci. Zaplnění paměti RAM bylo 55% a ke konci testu kleslo na 50%. Pokud bychom chtěli investovat do ochrany svého počítače, tak tento program je komplexní řešení. [18]



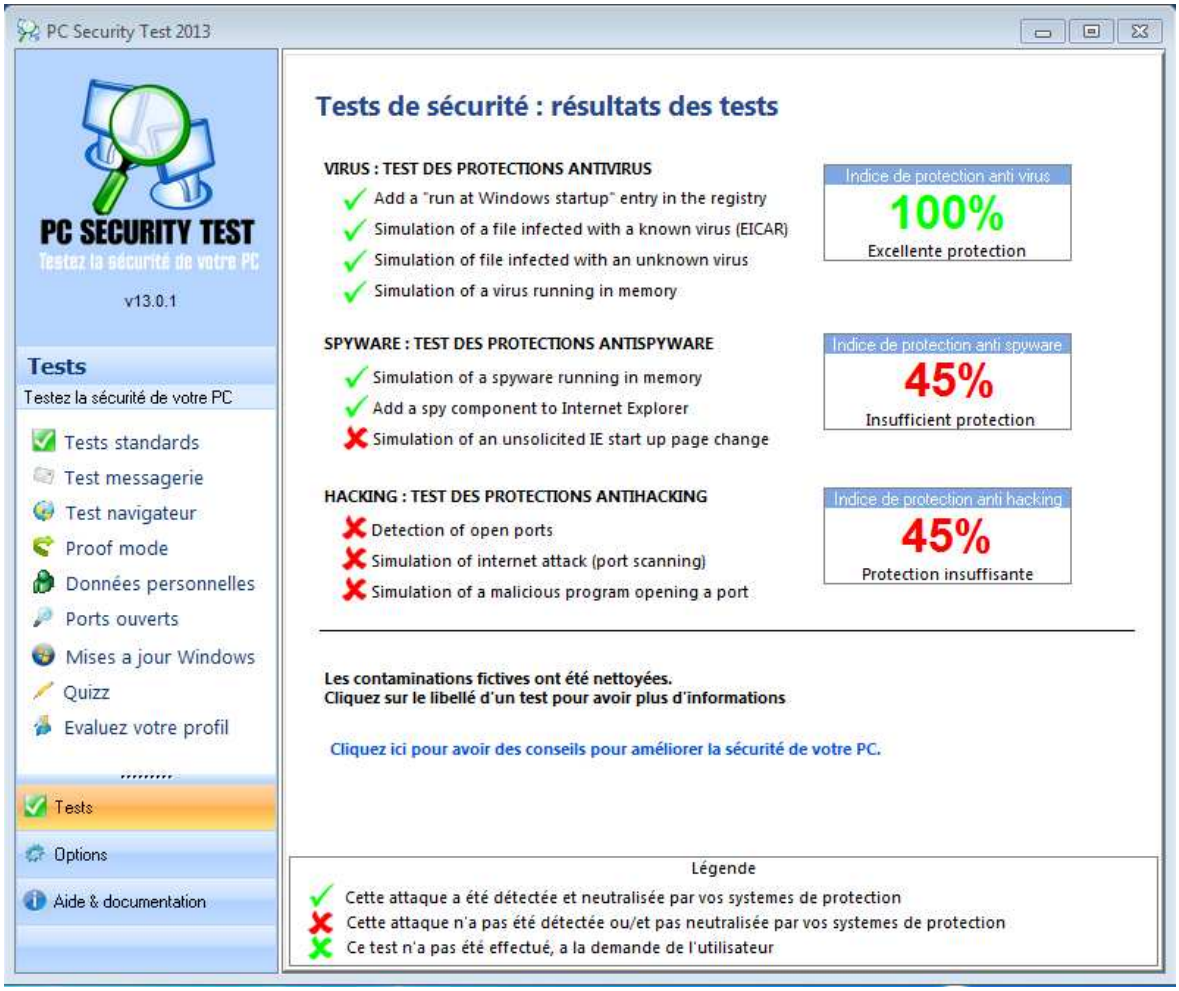
Obrázek 16 Výsledek testu systému s antivirem ESET [7]



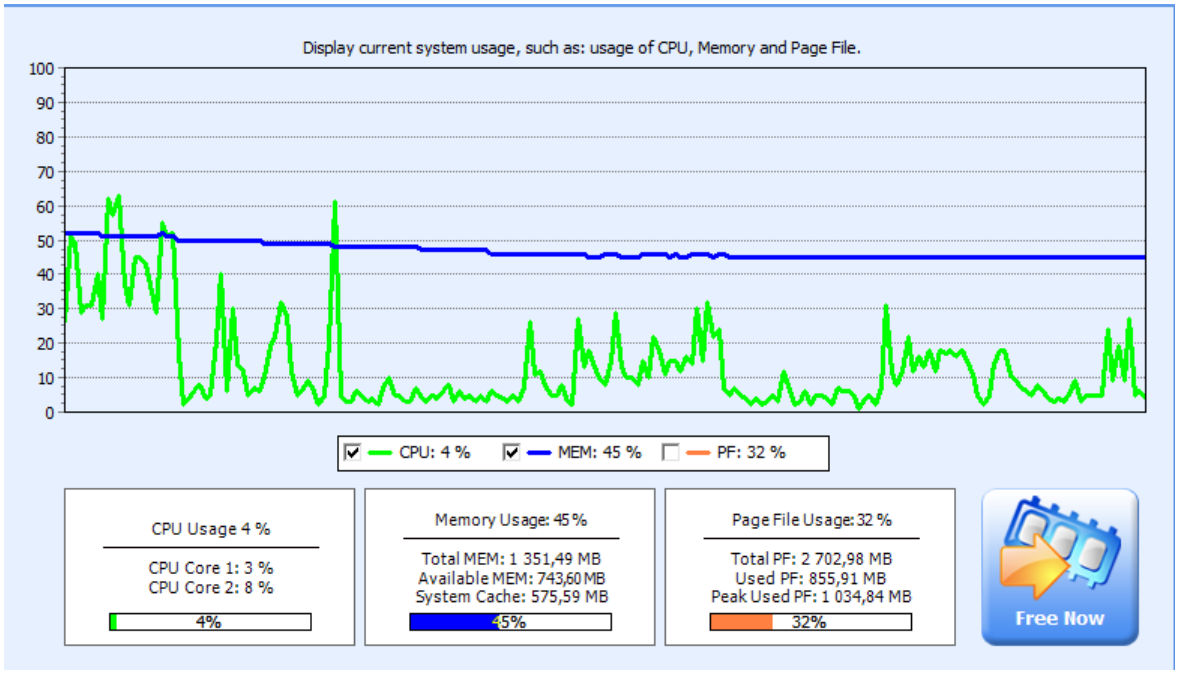
Obrázek 17 Zatížení procesoru a paměti RAM při testu [7]

6.5 Ad-Aware Pro Security 10.1.211.3382

Tento software je nabízen jako shareware, to znamená, že funguje po omezenou dobu. Program se chová jako antivirový a antispywarový. V testu antivirového programu uspěl na 100 %, zamezil všem pokusům o infiltraci, naproti tomu spywarová ochrana v tomto testu neobstála z důvodu, že se bere v potaz i rychlost odezvy na infiltraci. To ji řadí do kategorie nedostatečný. Tento program neobsahoval bránu firewall, takže při testu se testovala pouze Brána Windows Firewall. Zatížení procesoru bylo podstatně nižší než u předchozích, které nepřesáhlo 60%. U paměti RAM to bylo využití klesajícího charakteru. [22]



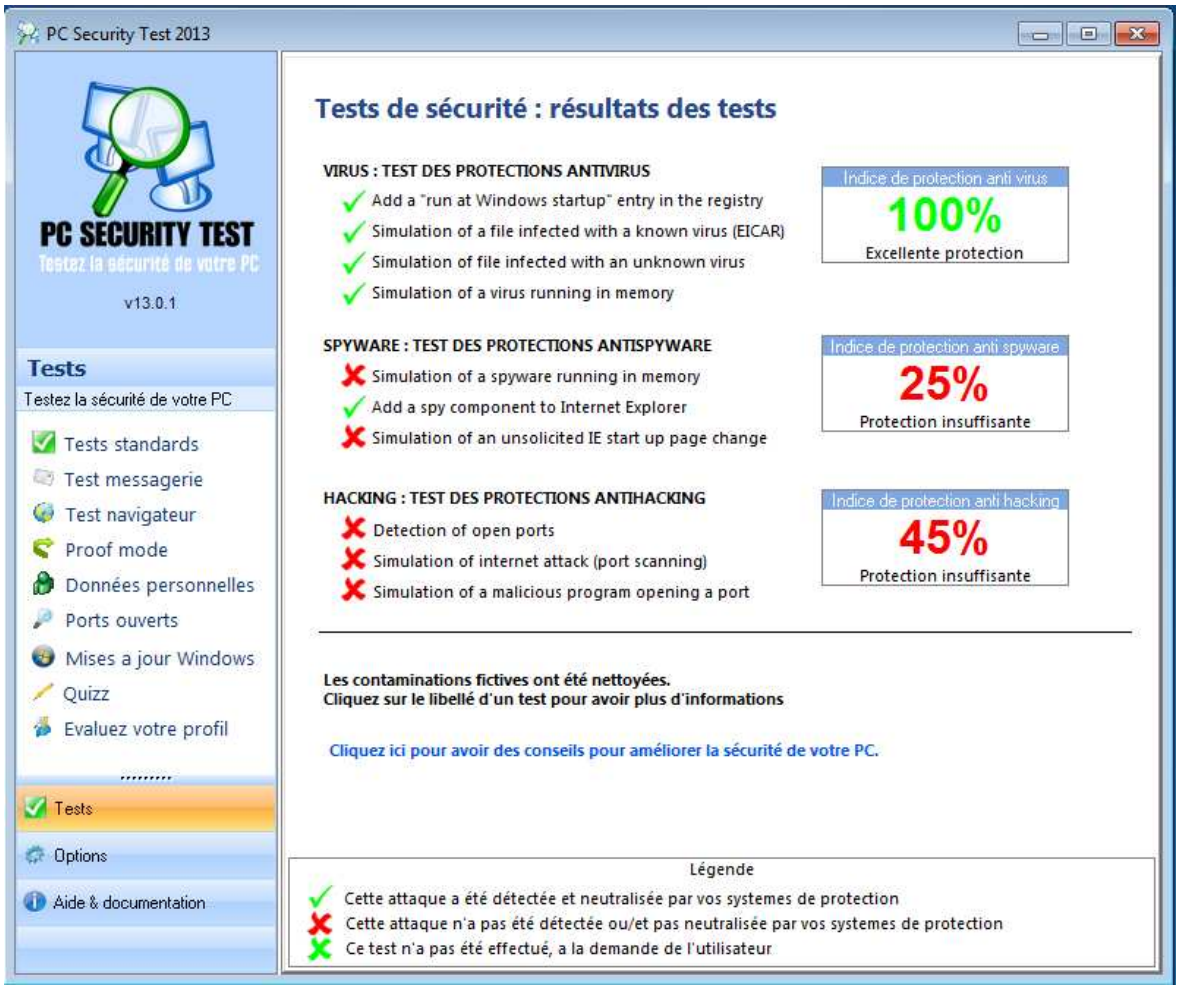
Obrázek 18 Výsledek testu systému s AD-Adware [7]



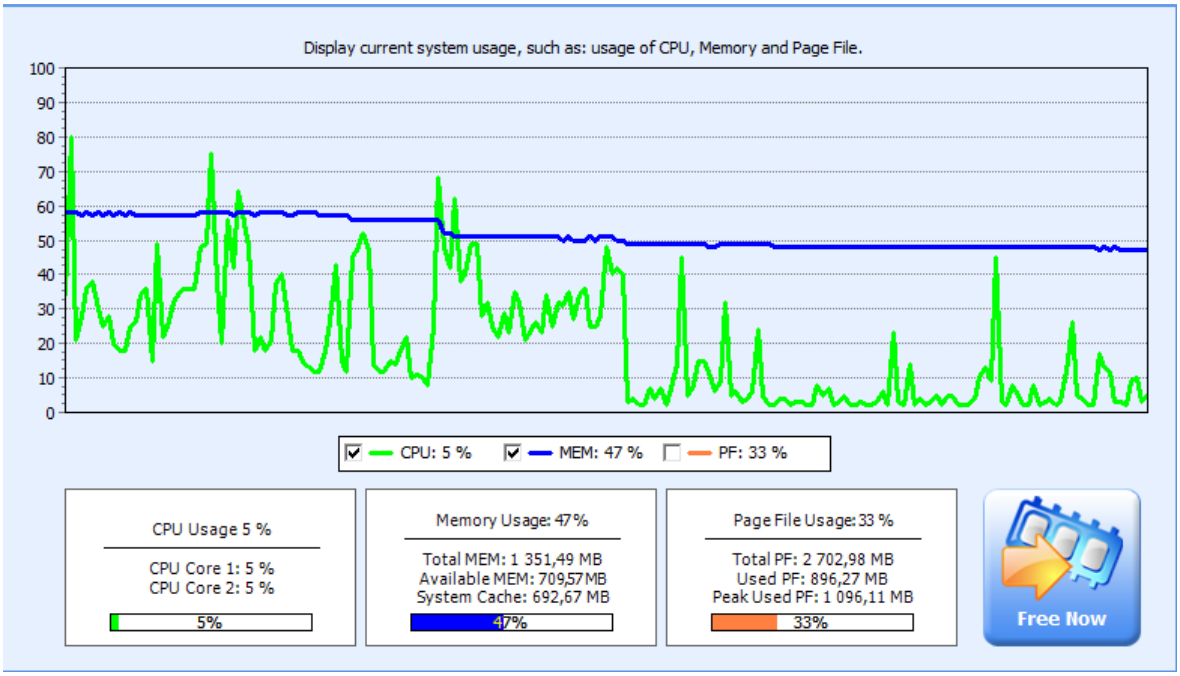
Obrázek 19 Průběh zátěže procesoru a RAM při testu[7]

6.6 F-Secure Internet Security 2011

Tento známý antivirový program v roce 2013 v testu real-world protection test zablokoval 100% možných hrozeb. A celkově byl hodnocen advanced+. Při testování pokusu o infiltraci dokázal antivirový program zabránit všem útokům. Tím potvrdil své kvality. Je škoda, že neobsahuje antispywarovou ochranu ani firewall. Procesor byl zatěžován na začátku testu 80% a dále zátěž klesala, paměť RAM byla zaplňována v rozmezí 50-60%. Výhodou je také kompletní čeština, pro uživatele co neumí dostatečně anglicky.[15] [19]



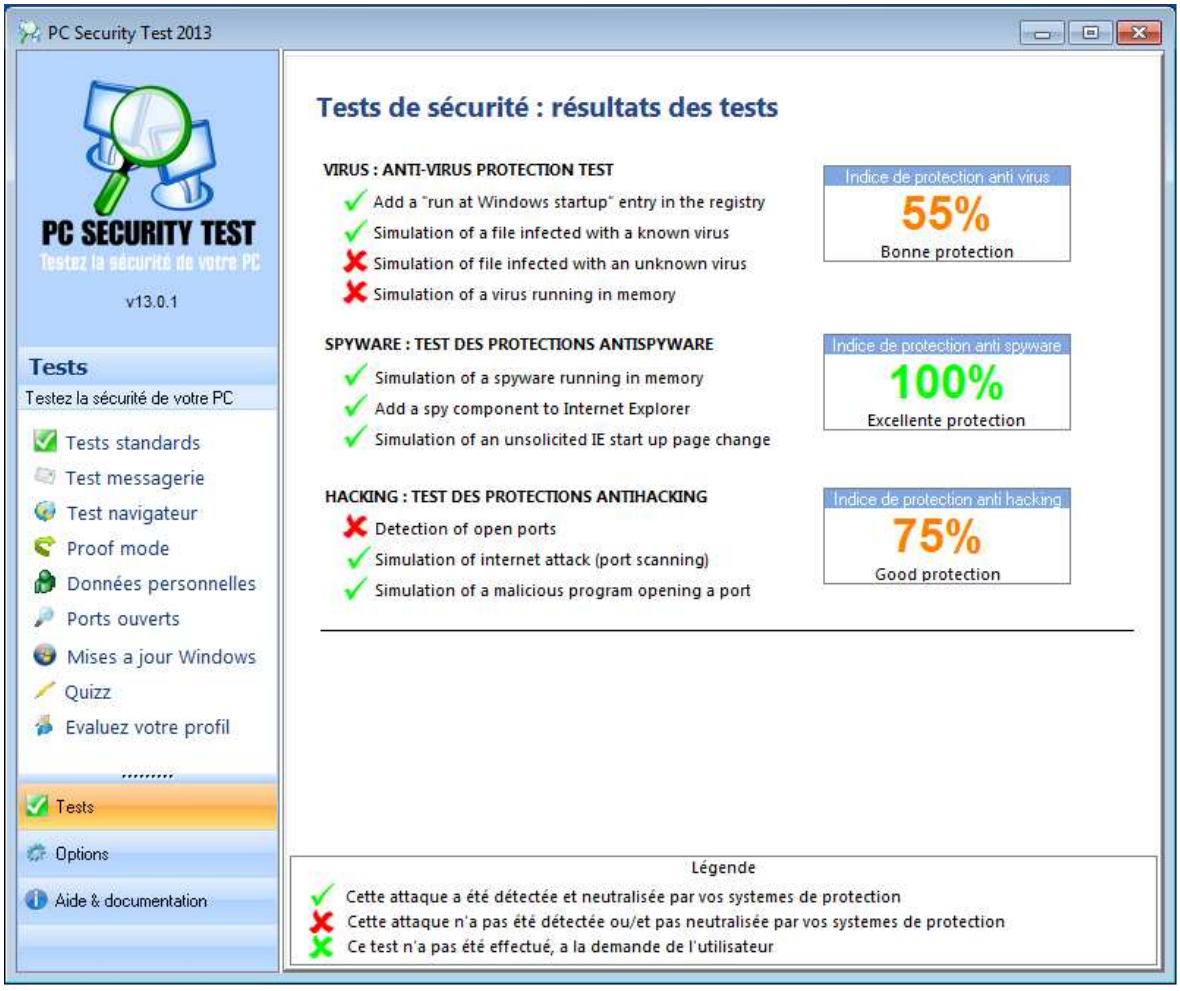
Obrázek 20 Výsledek testu systému s aplikaci F-Secure [7]



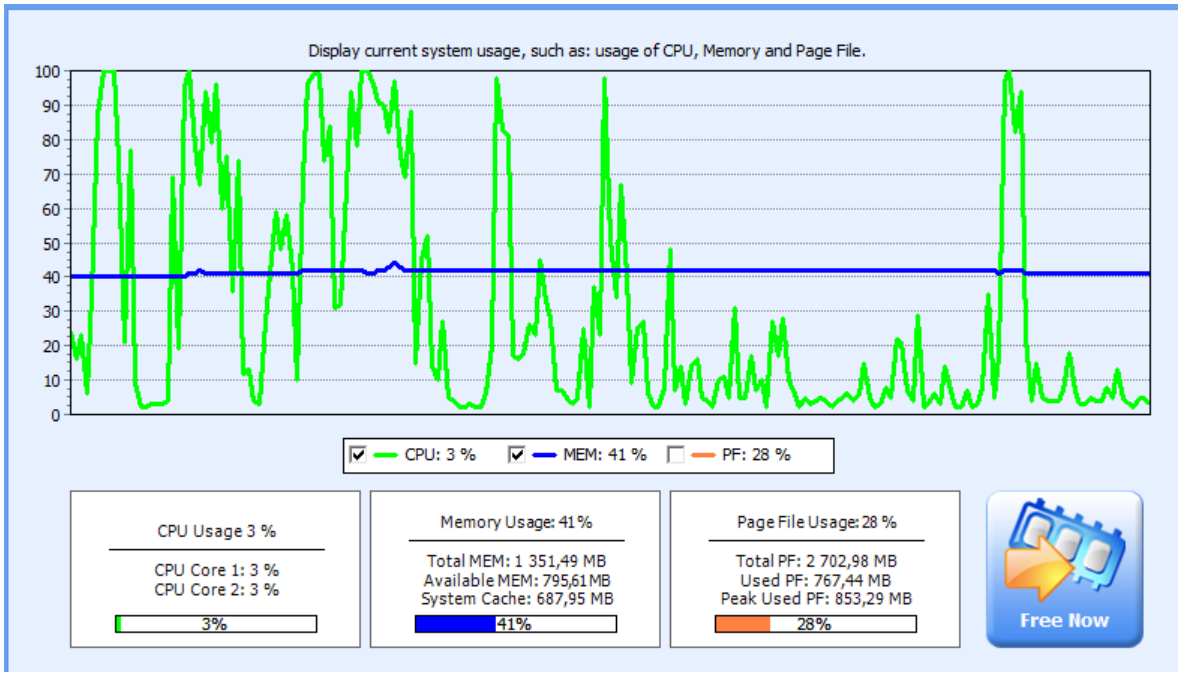
Obrázek 21 Zátěž procesoru a RAM v průběhu testu [7]

6.7 Outpost Pro Firewall

Tento program slouží jako brána firewall, také obsahuje antispywarovou ochranu, při testování na systému Windows 7 se brána firewall ukázala jako dostačující, plně nahrazuje originální bránu firewall. Navíc spywarová ochrana zachytila 100 % hrozeb. Na obrázku 22 je vidět, že tento program dokázal zachytit pokus o přidání programu po spuštění a také simulaci známého viru. Outpost Pro Firewall je zkušební verze na 30 dní. Lehkou nevýhodou je dost vysoká zátěž procesoru, která se dost často dosahuje 100%. Paměť RAM je po celou dobu testu zaplněna ze 40%.[27]



Obrázek 22 Systém s nainstalovaným firewallem Outpost firewall [7]



Obrázek 23 Zatížení Procesoru a RAM při testu [7]

6.8 Shrnutí výsledků testování

Avast! Free Antivirus se zdá asi jako dobrá volba z důvodu jeho jednoduchosti, navíc je zdarma. V kombinaci se spywarovým skenerem a programem firewall by byl systém opravdu bezpečný. Pokud bychom chtěli, je možnost koupit si placenou verzi a ta obsahuje i tyto zmíněné nástroje.

Bitdefender Antivirus 2013 Plus ten to program při testu antiviru obstál se 100% navíc má integrovanou bránu firewall, která pracuje na 100 %. Obsahuje i nástroj na bezpečné přihlášení na internetové bankovnictví a speciální aplikaci na plochu, která zobrazuje aktuální prováděné operace. Také je zde možnost přepínání z uživatelského módu na takzvaného „autopilota“, ten se chová podle zjištěných informací o používání. Bohužel jde o verzi trial na 30 dní.

ESET Smart Security 6 jsem testoval z důvodu jeho oblíbenosti. Neplacená verze funguje pouze 30 dní. Obsahuje antispyware a firewall. Výhodou tohoto je zabezpečení celého systému jedním programem.

Ad-Aware Pro Security je zase omezená verze, ale při test antiviru dokázal své kvality 100% výsledkem a ochrana spyware se také zvýšila z 25 % na 45 % úspěšnost. To není plně dostačující, alespoň se ochrana zvýšila.

F-Secure Internet Security 2011 při tomto testu antivirový program dokázal zachytit 100% infiltrací. Výhodou je jeho česká lokalizace.

Outpost Pro Firewall je program určený pro ochranu proti průniku do PC z vnějšku sítě. Ukázal, že vlastní i dobrou ochranu před spywarem. Kdybychom ho použily v kombinaci s antivirovým programem dosáhl by kvalitního výsledku, je tedy vhodný pro zabezpečení systému.

Testovaný program	Test firewallu	Test spywaru	Test antiviru	Plusy a mínusy
Avast!	Nevyhověl	Nevyhověl	Vyhověl	+ Zdarma
Bitdefender Antivirus	Vyhověl	Nevyhověl	Vyhověl	- Nepřítomnost spywaroné ochrany
ESET Smart Security 6	Vyhověl	Dostatečný	Vyhověl	+ Kompletnost
Ad-Aware Pro Security	Nevyhověl	Nevyhověl	Vyhověl	- Spywarová ochrana
F-Secure Internet Security 2011	Vyhověl	Nevyhověl	Nevyhověl	+ Nízká zátěž CPU
Outpost Pro Firewall	Vyhověl	Vyhověl	Dostatečný	+Spywarová ochrana

Tabulka 1 Vyhodnocení testovaných softwaru na systému

7 PRŮZKUM ZNALOSTÍ BEZPEČNOSTI NA SKUPINĚ UŽIVATELŮ INTERNETU

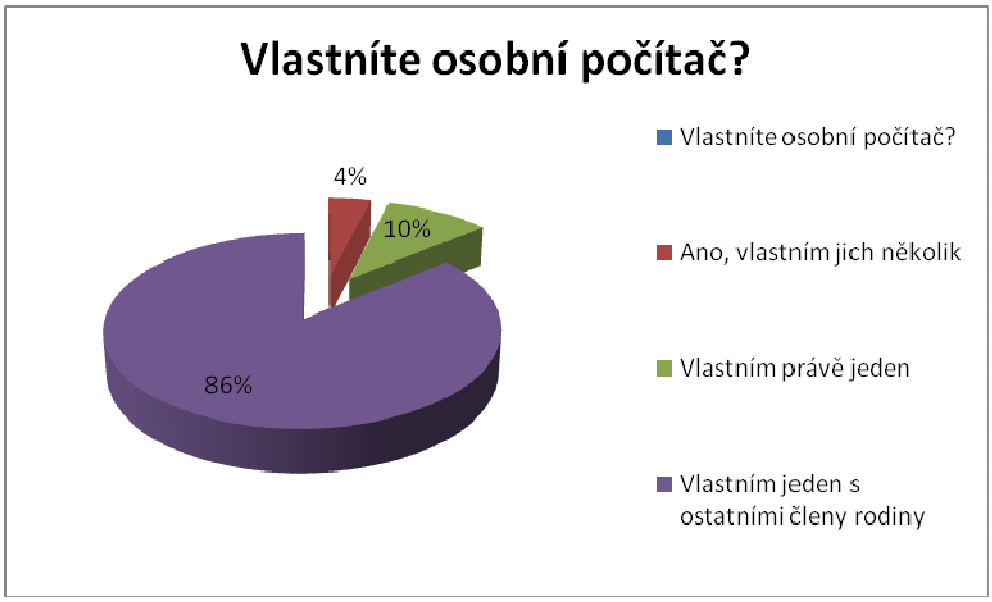
Pokud chceme získat přehled o tom, jak jsou lidé znalí v různých problematikách, použijeme k tomu různé formy dotazníků nebo anket. Já jsem zvolil papírovou formu dotazníku, který jsem rozdával v okolí svého bydliště. Dotazník byl anonymní a sbírání údajů trvalo 14 dní.

7.1 Analýza odpovědí v dotazníku

Dotazník jsem sestavil tak, abych zjistil nejen znalosti bezpečného používání počítače, ale i obecné údaje o používání počítače. Průzkum jsem prováděl s cílem získat přehled o znalostech, kterými disponují uživatelé internetu. Průzkumu se účastnilo 200 respondentů a jejich věkové rozpětí bylo 15 - 61 let s uživatelskou úrovní od začátečníků až po profesionály.

7.1.1 Vlastníte osobní počítač?

- Ano, vlastním jich několik
- Vlastním právě jeden
- Vlastním jeden s ostatními členy rodiny
- Nevlastním, ale využívám jej u přátel
- Nevlastním, ale využívám jej na veřejných místech (knihovny, kavárny...atd.)
- Nevlastním a nevyužívám jej vůbec

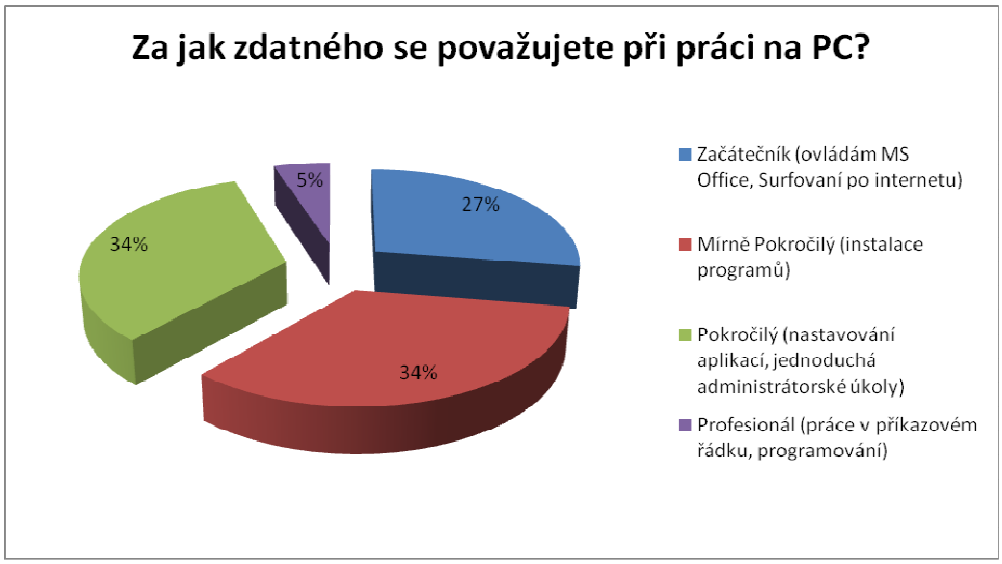


Graf 1 Vlastníte osobní počítač? [7]

Hned u první otázky je zajímavé to, že většina dotázaných sdílí počítač s ostatními členy rodiny, bohužel zde není specifikováno, zda používají každý vlastní účet nebo mají jeden společný. Pokud mají jeden společný a navíc administrátorský, může dojít zanesení některého z druhu infiltrací a to nedbalým používáním.

7.1.2 Za jak zdatného se považujete při práci na PC?

- Začátečník (ovládám MS Office, Surfovaní po internetu)
- Mírně Pokročilý (instalace programů)
- Pokročilý (nastavování aplikací, jednoduchá administrátorské úkoly)
- Profesionál (práce v příkazovém řádku, programování)

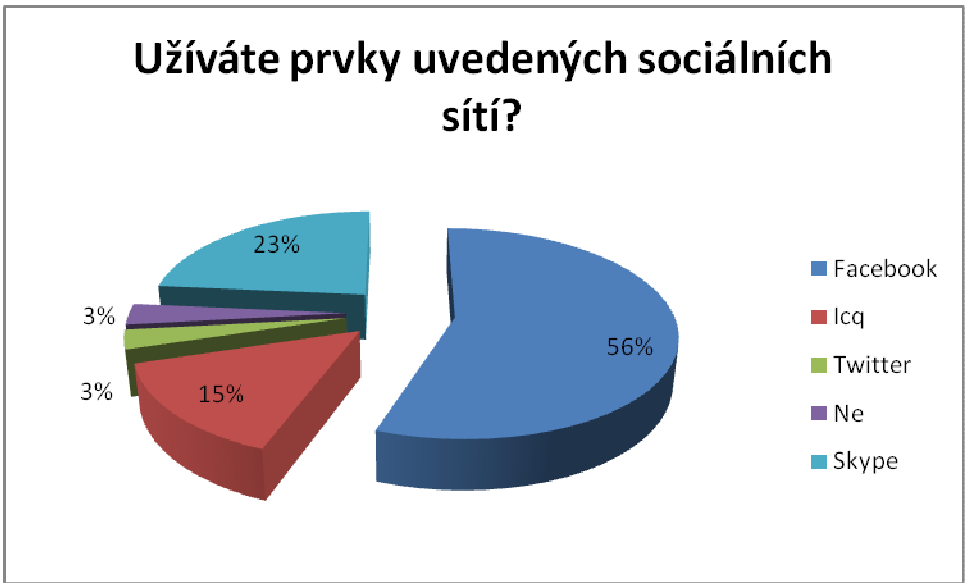


Graf 2 Za jak zdatného se považujete při práci na PC? [7]

U tohoto dotazu mne zajímaly uživatelské dovednosti. Pouze 5% se považuje za profesionály, jinak ostatní se rozdělují téměř rovnoměrně do zbylých skupin. Takže v průzkumu se účastnila široká škála uživatelů s rozdílnou zkušeností.

7.1.3 Užíváte prvky uvedených sociálních sítí?

- Facebook
- Icq
- Twitter
- Ne
- Skype



Graf 3 Užíváte prvky uvedených sociálních sítí? [7]

Dnes je Internet náhradou ranních novin, v některých případech i snídaně. Jeto způsobeno hlavně rozmachem sociálních sítí a to převážně Facebookem, který používá 56% dotazovaných. Sociální sítě jsou fenoménem dnešní doby. U této otázky jsem zvlolil sociální sítě, které jsou nejvyužívanější v České republice.

7.1.4 Víte co to je Sociální inženýrství?

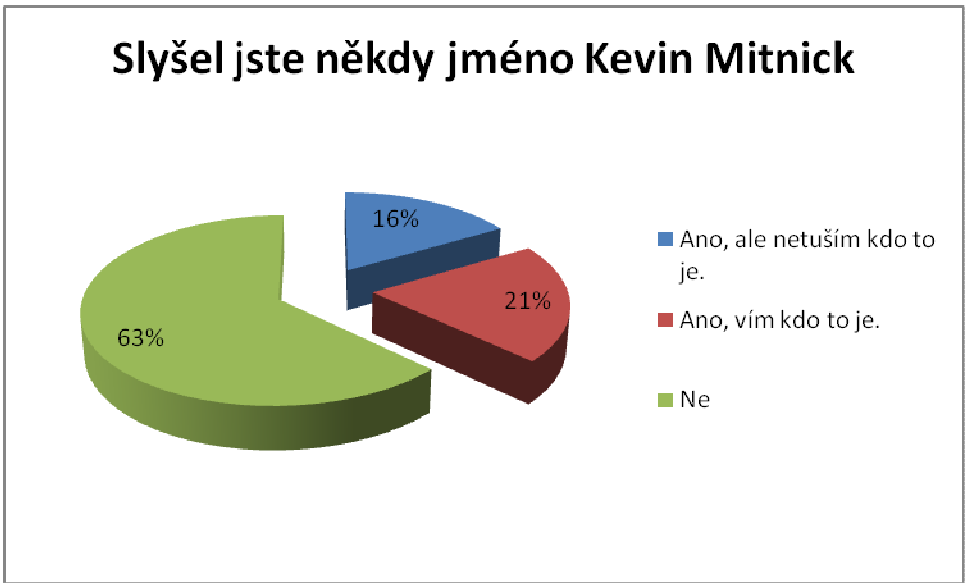
- Ano, ale nevím, co to znamená
- Ano a vím co, to znamená
- Nevím

Graf 4 Víte co to je Sociální inženýrství? [7]

Touto otázkou žačalo získávání dat pro představu o informovanosti okolí. Celá polovina dotázaných vůbec neví, co to je sociální inženýrství. 28% tento pojem slyšelo, ale neví, co to znamená. To svědčí o malé informovanosti.

7.1.5 Slyšel jste někdy jméno Kevin Mitnick

- Ano, ale netuším kdo to je.
- Ano, vím kdo to je.
- Ne

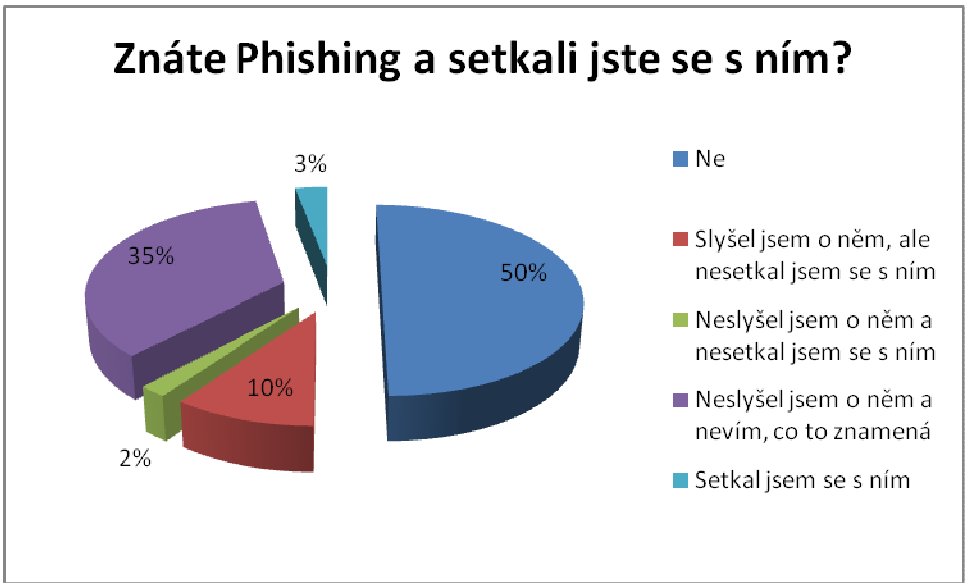


Graf 5 Slyšel jste někdy jméno Kevin Mitnick? [7]

Kevin Mitnick známý používáním sociálního inženýrství. Výsledek je dán, tím že lidé neznají sociální inženýrství, tak nemou znát i tohoto muže. Důvodem je také medializovanost. Pokud by tento dotaz byl vznesen v Americe, určitě by dopadl úplně opačně.

7.1.6 Znáte Phishing a setkali jste se s ním?

- Ne
- Slyšel jsem o něm, ale nesetkal jsem se s ním
- Neslyšel jsem o něm a nesetkal jsem se s ním
- Neslyšel jsem o něm a nevím, co to znamená
- Setkal jsem se s ním

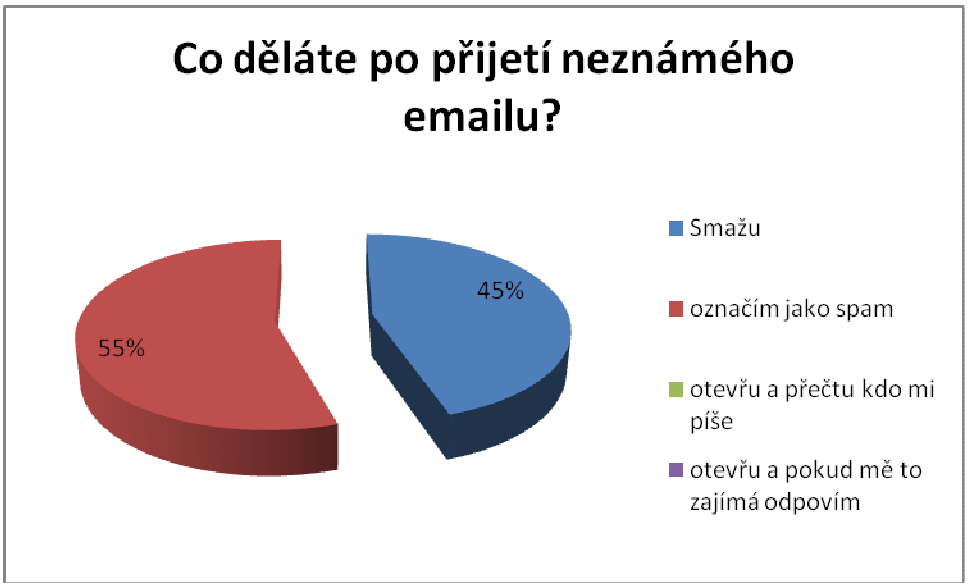


Graf 6 Znáte Phishing a setkali jste se s ním? [7]

Tato otázka mě zajímala. Zajímalo mě, kolik lidí tuto metodu útoku zná nebo se s ní setkalo. Očekával jsem trochu optimistický výsledek. Opak je pravdou. Takovou katastrofální neznalost jsem nečekal. Lidé by se měli začít vzdělávat v oblasti bezpečnosti používání počítačů. Pokud byt tento trend pokračoval tímto tempem, tak se z našich počítačů stanou veřejně přístupné vitríny.

7.1.7 Co děláte po přijetí neznámého emailu?

- Smažu
- označím jako spam
- otevřu a přečtu, kdo mi píše
- otevřu, a pokud mě to zajímá, odpovím

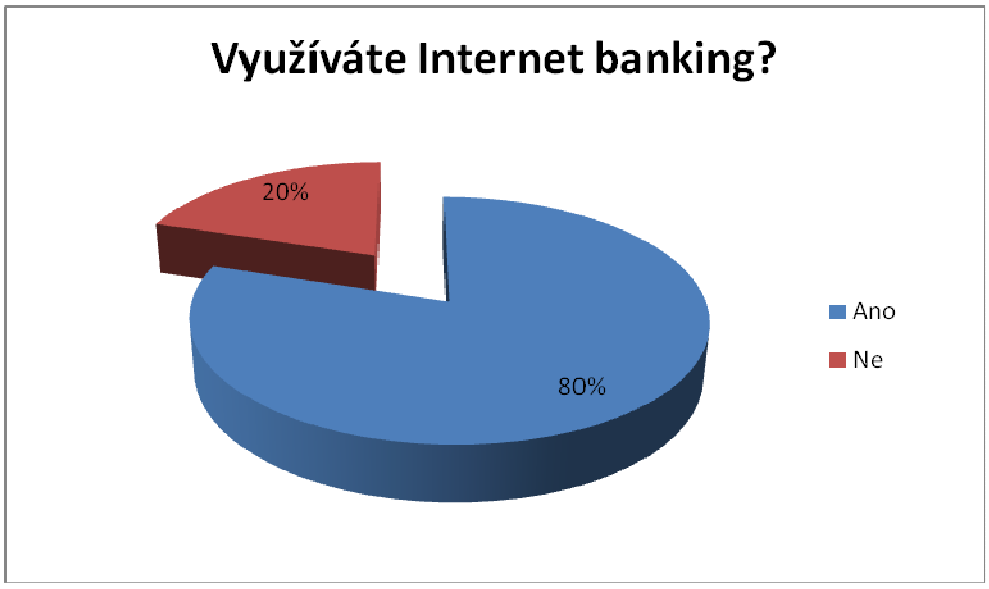


Graf 7 Co děláte po přijetí neznámého emailu? [7]

55% lidí označuje tyto přijaté zprávy jako spam a 45% je rovnou maže. Toto je skutečně dobrý výsledek. To znamená, že spam se dostal do povědomí společnosti a tím se riziko zásadně snižuje.

7.1.8 Využíváte Internet banking?

- Ano
- Ne



Graf 8 využíváte Internet banking?

Tuto službu banky nabízejí bezplatně svým klientům, protože jim usnadňuje práci s financemi, platby přímo z domu bez nutnosti jít do banky. Pouze 20% respondetů stále této vymoženosti nevyužívá, což uživatele chrání před hrozbou těchto rizik.

7.1.9 Setkali jste se s tím, že vám přišel email z vašeho finančního institutu a žádal po vás přihlášení?

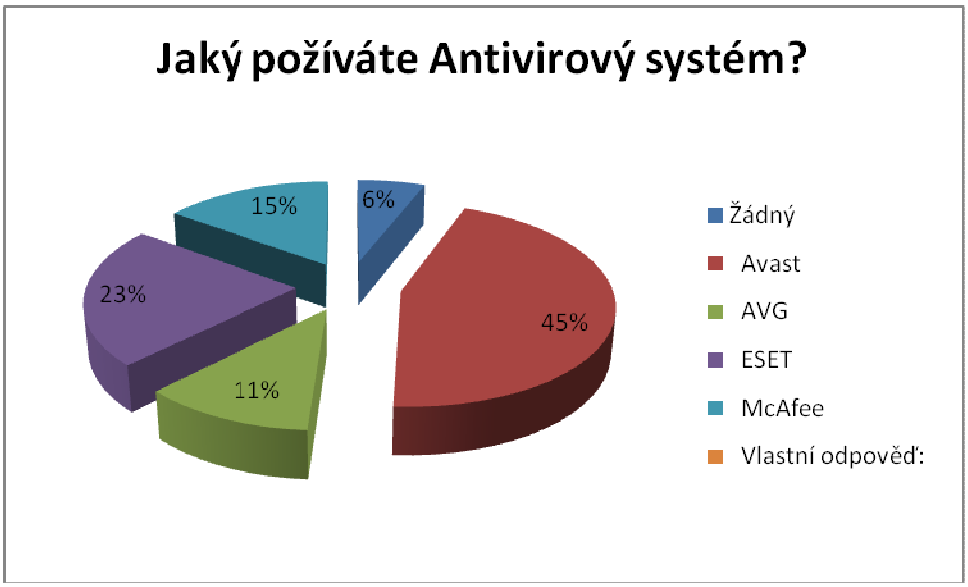
- Ano
- Ne

Graf 9 Setkali jste se s tím , že vám přišel email z vašeho finančního institutu a žádal po vás přihlášení? [7]

Pouze 11% tázaných se tedy setkali s phishingem. Zbylých 89% dotázaných si myslí, že se s ním nesetkali nebo o tom ani nevědeli, v lepším případě nepoužívají internet banking, nebo to považovali za spam.

7.1.10 Jaký požíváte Antivirový systém?

- Žádný
- Avast
- AVG
- ESET
- McAfee
- Vlastní odpověď:



Graf 10 Jaký požíváte Antivirový systém? [7]

Použití antiviru zavisí na rozhodnutí uživatele. U této skupiny dotazovaných převládá Avast! Je to spolehlivý a kvalitní antivir a navíc je zadarmo. Hned za ním skončil ESET s 23% . V kapitole testování jsem provedl test nejnovějších verzí obou programů.

7.1.11 Setkali jste se někdy s počítačovým virem ve svém počítači?

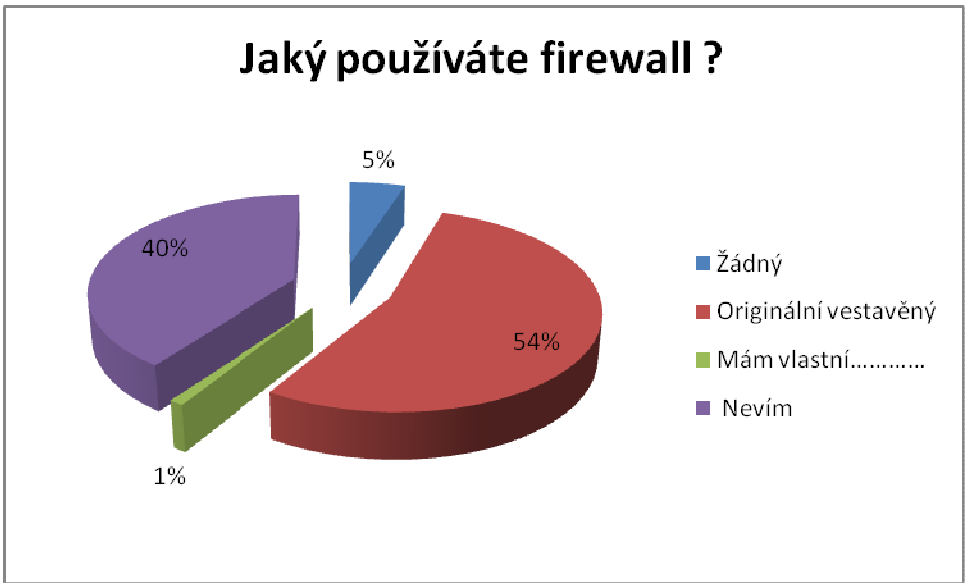
- Ne, nikdy
- Ano, už se mi to jednou stalo
- Ano a nejednou
- Nevím, nepoznám to

Graf 11 Setkali jste se někdy s počítačovým virem ve svém počítači? [7]

Alarmujícím výsledky je, že 11% lidí nepozná infiltraci. U těchto uživatelů je předpoklad, že nepoužívají antivirový program. Jak graf ukazuje lidé se s viry setkávají, dle mého usouzení na viry je upozorní jejich antivirová ochrana.

7.1.12 jaký používáte firewall ?

- Žádný
- Originální vestavěný
- Mám vlastní……
- Nevím



Graf 12 jaký používáte firewall? [7]

Nadpoloviční většina používá firewall, který je implementován do operačního systému. Bohužel tento firewall není úplně dostačující, pouze jedno procento (to jsou dva lidé) nevěří originálnímu firewallu a používají ZoneAlarm.

7.1.13 Používáte různá hesla pro přihlášení?

- Ano
- Ne

Graf 13 Používáte různá hesla pro přihlášení? [7]

Toto je nešvar lidí, dalo by se to považovat za zlozvyk. Nebaví nebo nechce se jim pamatovat více hesel nebo nějaká složitá hesla s různými speciálními znaky. Tak používají jednoslovné hesla, třeba jméno psa, nebo číselnou kombinaci „1234“, nebo složitější „4321“. Navíc používají stejná hesla k bankovnímu účtu, tak jako heslo k emailové schránce nebo různým fórům. Dotazovaná skupina lidí se zde chová pečlivě a 81% má různá hesla k více účtům.

ZÁVĚR

Tato bakalářská práce vznikla z důvodu přesvědčení o všeobecné neznalosti možných hrozeb napadení počítače útočníkem nebo škodlivým softwarem mezi běžnými uživateli Internetu. Proto jsem se snažil shrnout všechny možné útoky a pokusy o infiltraci do jedné práce, která bude sjednocovat všechny důležité informace o těchto hrozbách.

V úvodní části při posuzování rizik jsem určil ty nejčetnější. Podle jejich počtu jsem vybral nejpoužívanější typy škodlivých kódů, k nim jsem přidal jejich bližší popis. Také jsem uvedl jak se šíří, v čem tkví jejich nebezpečnost a způsoby prezentování jejich přítomnosti. Popis jsem se snažil koncipovat tak, aby i nepříliš zkušený uživatel pochopil princip fungování popisovaných nákaz nebo metod útoků.

Důležitou částí je návrh, jak se jednotlivým útokům bránit. V této kapitole popisuji jak se bránit s pomocí různých programů pro prevenci nebo následnou dezinfekci systému. Také navrhuji, jak by se měl uživatel chovat. Kterým věcem se vyvarovat, jak poznat, že se jedná o podvodnou stránku nebo email. Doporučuji zde uživatelům začít se vzdělávat právě v oblasti bezpečného pohybu po Internetu. Dále uvádím jakým způsobem nastavit operační systém Windows 7 Home Basic s přehledným popisem, co každá funkce systému dělá a proti kterým rizikům nám pomáhá se bránit.

V části testování systému jsem zkoušel jednotlivé programy na ochranu před infiltrací. Celý test byl prováděn na virtuálním počítači pomocí softwaru VM-ware player, kde jsem instaloval postupně uvedené antivirové programy a testoval je pomocí programu PC Security 2013, navíc jsem měřil zátěž procesoru a paměti RAM. Výsledky testů jsem ukládal jako fotografie, které jsem vložil do své práce. Výstupem měření zátěže byly grafy pro jednotlivá měření. Na konec kapitoly jsem provedl závěrečné zhodnocení všech testovaných antivirových softwarů.

V závěrečné části mé práce se nachází průzkum znalostí lidí, používajících Internet. Jeho výsledek se blíží tomu, co jsem si myslel. Lidé jsou lhostejní k bezpečnosti při používání Internetu. Neznají hlavní rizika, co na ně číhají někde v síti. Jediné o čem ví, je existence virů. Ten si představují jako něco, co jim může zničit i hardware. Uživatelé si neuvědomují hrozbu špionáže jejich počítače nebo útoky pomocí sociálního inženýrství.

Přínosem této práce je ucelení informací o bezpečnosti práce s Internetem a také snaha upozornit na neznalost skupiny uživatelů využívající služby Internetu.

ZÁVĚR V ANGLIČTINĚ

This work was because of the general belief in the ignorance of potential threats infecting your computer attacker or malicious software among ordinary Internet users. That's why I tried to summarize all possible attacks and attempts to infiltrate into a job that will unite all the relevant information about these threats.

In the introductory part of the risk assessment, I identified the most frequent. According to their numbers, I chose the most common types of malware, they've added their detailed description. I also said how it spreads a great deal about the hazards and ways of presenting their presence. Description I have tried to conceive so that even less experienced users understand the operating principle described diseases or methods of attack.

An important part of the proposal, as did the individual attacks. This chapter describes how to defend themselves using various programs to prevent or subsequent disinfection system. It also suggests how the user should behave. Which things to avoid, how to know that this is a phishing site or email. I recommend users start here to learn just in the safe browsing. Further mention how to set the operating system Windows 7 Home Basic with a clear description of what each function does and the risks against which helps us to resist.

In the test system I have tried various programs to protect against infiltration. The entire test was performed on a virtual machine using VM-ware software player, where I installed progressively antivirus programs and tested them using PC Security 2013 plus I measured the load on the processor and RAM. The results of my tests, I saved a picture that I put into my work. The output of the load measuring charts for individual measurements.

At the end of the chapter, I made the final evaluation of all tested anti-virus software.

In the final part of my work is a survey of knowledge of people using the Internet. The result is close to what I thought. People are indifferent to safety while using the Internet. They do not know the risks of what they are lurking somewhere in the network. Only what he knows is the existence of viruses. He imagines as something that they can destroy the hardware. The users do not realize the threat to their computer espionage or attacks using social engineering.

The contribution of this work is a comprehensive information security work with the Internet and also an effort to highlight the ignorance of users through Internet.

SEZNAM POUŽITÉ LITERATURY

[1] Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť. In: . www.lupa.cz [online]. 2. 3. 2012 [cit. 2013-05-16]. Dostupné z: http://www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/?labelsBox-labelId=859&do=labelsBox-switch

[2] HÁK, Igor. *Moderní počítačové viry* [online]. třetí vydání. [s.l.] : [s.n.], 2005 [cit. 2013-04-24]. Dostupné z WWW: <http://viry.cz/viry.cz/kniha/kniha.pdf>

[3] MIKLAS, Michal a Jaromír SVĚTLÍK. Počítačové viry. In: *Počítačové viry* [online]. 2012 [cit. 2013-05-21]. Dostupné z: http://www.gjszlin.cz/ivt/esf/ostatni-sin/pocitacove-viry.php

[4] BITTO, Ondřej. *Jak zabezpečit domácí malou síť Windows XP: účty, práva, firewally, antiviry a další nástroje*. Vyd. 1. Brno: Computer Press, 2006, 216 s. ISBN 80-251-1098-2

[5] MITNICK, Kevin. *Umění klamu*. Vyd. 1. Gliwice: Helion, 2003. ISBN 83-7361-210-6

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

[6] Browser hijacking. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001, 19.5. 2013 [cit. 2013-05-21]. Dostupné z: http://en.wikipedia.org/wiki/Browser_hijacking

[7] Vlastní galerie obrázků

[8] VÍTEK, Miloš a Marcela VÍTKOVÁ. *Sociální vědy a inženýrství*. Vyd. 1. Hradec Králové: Gaudeamus, 2004, 164 s. ISBN 80-704-1474-X.

[9] Antivírusový softvér. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 18.5.2013 [cit. 2013-05-22]. Dostupné z: http://sk.wikipedia.org/wiki/Antiv%C3%ADrusov%C3%BD_softv%C3%A9r

[10] PŘIBYL, Tomáš. Nebezpečí jménem phishing. [online]. [cit. 2013-04-05]. Dostupné z: http://m.cw.cz/securityworld/nebezpeci-jmenem-phishing-46139

[11] MITTELBACH, Jan. Pharming může ošálit i zkušenějšího uživatele internetu. [online]. 2008 [cit. 2013-04-05]. Dostupné z: http://tech.ihned.cz/c1-23480750-pharming-muze-osalit-i-zkusenejsiho-uzivatele-internetu

[12] DŽUBÁK, Josef. Co je to phishing. [online]. 2011 [cit. 2013-04-05]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[13] 'Pharming' scams. [online]. 2011 [cit. 2013-04-05]. Dostupné z: http://www.scamwatch.gov.au/content/index.phtml/itemId/829456

[14] *Principy nastavení brány Windows Firewall* [online]. 2013 [cit. 2013-05-21]. Dostupné z: http://windows.microsoft.com/cs-cz/windows7/understanding-windows-firewall-settings

[15] F-SECURE. *F-Secure* [online]. [cit. 2013-05-16]. Dostupné z: http://www.f-secure.com/en/web/home_global/home

[16] AVAST!. *Avast!* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.avast.com/cs-cz/index

[17] *Bitdefender* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.bitdefender.com/solutions/free.html

[18] *ESET* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.eset.cz/cz/domacnosti/produkty/smart-security/

[19] *AV-comparatives* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://chart.av-comparatives.org/awards.php?year=2013

[20] Bezpečnost firewallů - zabezpečení firemních sítí. In: *Lupa.cz* [online]. 21. 10. 2003 [cit. 2013-05-16]. Dostupné z: http://www.lupa.cz/pr-clanky/bezpecnost-firewallu-zabezpeceni-firemnich-siti/

[21] Google Chrome zablokoval vstup na jediný článek na Lupě pro phishing. In: DOČEKAL, Daniel. *Pooh.cz* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.pooh.cz/tag.asp?tag=Phishing

[22] Lavasoft.com/. *Lavasoft.com* [online]. 2013 [cit. 2013-05-16]. Dostupné z: http://www.lavasoft.com/

[23] Pharming on the Net. *Palizine* [online]. 2006 [cit. 2013-05-22]. Dostupné z: http://palizine.plynt.com/issues/2006Mar/pharming/

[24] Firewalls - what they are, what they do and why you need one!. *Www.pc-help-online.co.uk* [online]. 2007 [cit. 2013-05-22]. Dostupné z: http://www.pc-help-online.co.uk/libdoc.php?doc=45

[25] Nástroj Řízení uživatelských účtů. *Windows* [online]. 2013 [cit. 2013-05-22]. Dostupné z:http://windows.microsoft.com/cs-cz/windows7/products/features/user-account-control

[26] Změna typu uživatelského účtu. *Windows* [online]. 2013 [cit. 2013-05-22]. Dostupné z: http://windows.microsoft.com/cs-cz/windows-vista/change-a-users-account-type

[27] OutPostProFirewall. *Agnitum* [online]. 2013 [cit. 2013-05-22]. Dostupné z: http://www.agnitum.com/products/outpost/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

URL Uniform Resource Locator.

DNS Domain Name System.

PC Personal Computer.

CISRT Computer Security Incident Response Team

IDS Intrusion Detection System

HTML HyperText Markup Language

IM Instant massaging

IRC Internet Relay Chat

DDoS Distributed Denial of Service

AOL America On Line

IP Internet Protocol

RAM Random Access Memory

SEZNAM OBRÁZKŮ

Obrázek 1 Graf struktury útoků podle CSIRT [1] 12
Obrázek 2 Phrarming pomocí škodlivého kódu [11] 21
Obrázek 3 Pharming přes útok na DNS server [23] 22
Obrázek 4 Jednotlivé úrovně filtrování komunikace[20] 26
Obrázek 5 Ukázka firewallu[24] 27
Obrázek 6 Dopručené nastavení brány Windows 7 Firewall pro veřejnou síť [7] 28
Obrázek 7 ukázka podvodného emailu [21] 32
Obrázek 8 Ukázka podvodné stánky [21] 33
Obrázek 9 Doporučené nastavení Řízení uživatelských účtů[7] 35
Obrázek 10 Nastavení typu účtu [7] 36
Obrázek 11 Test systému bez antivirového programu[7] 38
Obrázek 12 Test systému s antivirovým programem Avast! [7] 39
Obrázek 13 Zatížení procesoru a paměti RAM při testu [7] 40
Obrázek 14 Výsledek testu systému s BitDefendrem [7] 41
Obrázek 15 Průběh zatížení procesoru a RAM při testu [7] 41
Obrázek 16 Výsledek testu systému s antivirem ESET [7] 42
Obrázek 17 Zatížení procesoru a paměti RAM při testu [7] 43
Obrázek 18 Výsledek testu systému s AD-Adware [7] 44
Obrázek 19 Průběh zátěže procesoru a RAM při testu[7] 44
Obrázek 20 Výsledek testu systému s aplikaci F-Secure [7] 45
Obrázek 21 Zátěž procesoru a RAM v průběhu testu [7] 46
Obrázek 22 Systém s nainstalovaným firewallem Outpost firewall [7] 47
Obrázek 23 Zatížení Procesoru a RAM při testu [7] 47

SEZNAM TABULEK A GRAFŮ

Tabulka 1 Vyhodnocení testovaných softwaru na systému 49
Graf 1 Vlastníte osobní počítač? [7] 51
Graf 2 Za jak zdatného se považujete při práci na PC? [7] 52
Graf 3 Užíváte prvky uvedených sociálních sítí? [7] 53
Graf 4 Víte co to je Sociální inženýrství? [7] 54
Graf 5 Slyšel jste někdy jméno Kevin Mitnick? [7] 55
Graf 6 Znáte Phishing a setkali jste se s ním? [7] 56
Graf 7 Co děláte po přijetí neznámého emailu? [7] 57
Graf 8 využíváte Internet banking? 58
Graf 9 Setkali jste se s tím , že vám přišel email z vašeho finančního institutu a žádal po vás přihlášení? [7] 59
Graf 10 Jaký požíváte Antivirový systém? [7] 60
Graf 11 Setkali jste se někdy s počítačovým virem ve svém počítači? [7] 61
Graf 12 jaký používáte firewall? [7] 62
Graf 13 Používáte různá hesla pro přihlášení? [7] 63