Zabezpečení systému Windows 7

Security of system Windows 7

Martin Prusenovský

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin PRUSENOVSKÝ**
Osobní číslo:	**A09258**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení systému Windows 7**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma zabezpečení systému Windows a formulujte nejčastější hrozby současnosti.**
2. **Zaměřte se na systém Windows 7 a popište jeho funkce týkající se zabezpečení, které jsou dostupné již po instalaci.**
3. **V praktické části se zaměřte na rady pro správné zabezpečení systému Windows 7.**
4. **Vypracujte veřejný dotazník zkoumající povědomí uživatelů o zabezpečení systému.**
5. **Vyhledejte vhodné nástroje na testování a otestujte zabezpečení systému po instalaci a poté navrhněte vhodné programy, které zabezpečí systém proti hrozbám zmíněným v teoretické části.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KUČERA, Roman a Petr BROŽA. Bible Windows 7. Brno: Extra Publishing, c2009, 288 s. ISBN 978-807-4130-618.**
2. **SINCHAK, Steve. Windows 7: průvodce pro nové uživatele. Vyd. 1. Brno: Zoner Press, 2010, 375 s. Encyklopedie Zoner Press. ISBN 978-807-4130-830.**
3. **BOTT, Ed, Carl SIECHERT a Craig STINSON. Mistrovství v Microsoft Windows 7. Vyd. 1. Brno: Computer Press, 2010, 936 s. ISBN 978-802-5128-176.**
4. **CAFOUREK, Bohdan. Windows 7: kompletní příručka. 1. vyd. Praha: Grada, 2010, 326 s. ISBN 978-802-4732-091.**
5. **PROCHÁZKA, David. Windows 7: snadno a rychle. 1. vyd. Praha: Grada, 2010, 107 s. Snadno a rychle (Grada). ISBN 978-802-4732-541.**
6. **ROUNTREE, Derrick. Security for Microsoft Windows system administrators: introduction to key information security concepts. Boston: Syngress, c2011, 198 s. ISBN 15-974-9594-8.**

Vedoucí bakalářské práce:	**Ing. Jiří Vojtěšek, Ph.D.** Ústav řízení procesů
Datum zadání bakalářské práce:	**24. února 2012**
Termín odevzdání bakalářské práce:	**25. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Tato bakalářská práce se zabývá zabezpečením operačního systému Windows 7 proti nejčastějším aktuálním a nejčastěji se vyskytujícím hrozbám ze sítě Internet, a také proti možnému neoprávněnému lokálnímu přístupu. V teoretické části jsou popsány předchůdci tohoto operačního systému a internetové hrozby jako jsou Phishing, Trojské koně, DoS a DDoS útoky a jiné. Praktická část je rozdělena na tři úseky. V prvním jsou stanoveny rady pro uživatele k řádnému zabezpečení jejich systému, druhý se zabývá povědomím uživatele o zabezpečení a třetí je zaměřen na testování Windows 7.

Klíčová slova: zabezpečení, Windows 7, spyware, firewall, škodlivý software, Internetové útoky, lokální přístup, šifrování, Internetové hrozby

ABSTRACT

This thesis deals with security of the Windows 7 operating system against the most frequent threats appeared on the Internet network. It protects the system also from a possible unauthorized local access. There are predecessors of this operating system described in the theoretical part of the work, e.g. Phishing, Troja Virus, DoS, DDoS. The practical part is divided into three sections. The first one advises users to protect their system properly. The second section aims at user knowledge about the protection. The third one tests Windows 7.

Keywords: protection, Windows 7, spyware, firewall, damaging software, Internet attacks, local access, coding, Internet threats.

Tímto bych chtěl upřímně poděkovat panu Ing. Jiřímu Vojtěškovi, Ph.D. za podporu, připomínky, konzultace a veškerou odbornou pomoc při zpracování této práce.

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

Společnost Microsoft existuje více než 30 let. Za dobu, co vyvíjí své operační systémy Windows, se na tento operační systém objevuje spousta škodlivého software s cílem jeho poškození nebo minimálně znepříjemnění práce jeho uživatelům. Roku 2009 vychází doposud nejnovější oficiální verze těchto operačních systémů s názvem Windows 7.

V práci se budu zabývat zabezpečením Windows 7, aby byl schopen odolávat nejnovějším bezpečnostním hrozbám čelícím nejen z prostřednictví celosvětové sítě Internet, ale také z pohledu možného místního napadení. Než se společnost Microsoft dopracovala až k této verzi, předcházel tomu mnoholetý vývoj. Prvotní systémy neměly vůbec žádné bezpečnostní prvky. V době, kdy byly systémy uváděny, nebyly tyto prvky potřeba, protože Internet se zatím pouze rozvíjel. Postupem času se však vývoj Internetu dostal do fáze, kdy připojení k Internetu mělo stále více uživatelů. To znamenalo potřebu chránit svá data před únikem nebo jejich napadení skrz tuto celosvětovou síť.

Příkladem je dnes již základní bezpečnostní prvek, brána firewall. Ta byla Microsoftem poprvé dodána do operačního systému Windows XP a to až jako součást druhého Service Pack (implementována byla až do Windows Vista).

V dnešní době má připojení k Internetu téměř každý, proto je bezpečnost je stále více aktuální. Windows 7 je po instalaci doposud nejbezpečnějším vydaným systémem od Microsoftu, nicméně je potřeba jeho ochranu vylepšit o důležité chybějící programy. Tím nejdůležitějším je antivirový program, který tento operační systém v základu nenabízí.

S těmito skutečnostmi úzce souvisí bezpečnostní povědomí všech uživatelů připojených do sítě Internet. To je bohužel nedostatečné a mnozí z nich nemají ponětí o tom, jak a proč by měl být jejich operační systém zabezpečen. Tato skutečnost byla zjištěna z veřejného průzkumu zpracovaného v praktické části.

Protože mnoho uživatelů nemá dostatečné znalosti z oblasti ochrany operačních sytému, je tato práce věnována převážně jim s cílem poučit je o jejich systému Windows 7, jeho stávajícímu zabezpečení a převážně jak toto zabezpečení zdokonalit a jak jej udržovat na kvalitní a „zdravé“ úrovni.

I. TEORETICKÁ ČÁST

1 INTERNETOVÉ HROZBY

1.1 Největší současné hrozby

V současné době se na scéně internetových hrozeb nejvíce objevují tři podvodné techniky: trojské koně, sociální inženýrství a jeho odvětví phishing. V pozadí těchto hrozeb jsou zaznamenávány útoky typu DoS a DDoS nebo Botnety. Všechny tyto typy útoků jsou rozebrány níže.

1.1.1 Sociální inženýrství

Sociálním inženýrstvím rozumíme ovlivňování cílových osob a to takovým způsobem, aby sociotechnikovi (tj. osoba, která provádí útok) sdělili potřebné informace telefonicky, prostřednictvím internetu, nebo dokonce i při osobní schůzce. Všechny operační systémy se zabezpečují proti hackerům softwarem, který jim odolává nebo brání přístupu. Nejslabším článkem celého systému se tak stává člověk, který jej obsluhuje (ne vždy se musí jednat o operační systémy, sociální inženýrství může být použito všude a závisí jen na cíli sociotechnika). Před vlastním útokem se musí sociotechnik na celou situaci řádně připravit a ve výsledku využívá slabin bezpečnostní politiky podniku. Informace čerpá z webových stránek, inzerátů, katalogů firem nebo pomocí internetových vyhledávačů. Z nich čerpá pro sebe důležité informace, jako jsou jména, telefony, emailové adresy a další, o kterých podnik ani netuší, že mohou být zneužity. Pokud sociotechnik potřebuje, nebojí se sáhnout i do „shromaždiště informací“ jako jsou kontejnery nebo popelnice (tuto techniku využívá i policie a speciální výzvědné služby), kam z podniku odnášejí pro ně nepotřebné dokumenty, jako jsou: staré účty za telefon, výpis z účtu u banky, různé pracovní materiály, dokumenty popisující aktuální stav firmy, její plány, kontakty, plány schůzek a podobně. Výjimkou nejsou ani vyhozené důvěrné informace, které nebyly skartovány, na nichž se můžou objevovat hesla, přihlašovací údaje, zdrojové kódy a jiné, pro útočníka potřebné informace. Pokud se sociotechnik dostane k adresáři s kontakty, má z části vyhráno – má iniciály osoby, za kterou se může vydávat.

Při telefonním útoku si sociotechnici velmi vhodně vybírají osoby opačného pohlaví. Ve výhodě jsou v tomto případě ženy s příjemným hlasem, žádající pouze nepatrnou informaci. Pokud je žena pro tuto „práci“ nadaná a má i určité herecké schopnosti, ukončuje telefonní hovor se získanou informací pro svůj prospěch. Důležité je vzbudit

v cílové osobě důvěru, neptat se ihned na požadovanou informaci a neukončovat hovor ihned po získání požadovaného. Potřebné vlastnosti jsou vnímavost a schopnost rychlého reagování na změnu situace v případě, že hovor neprobíhá podle plánu. Vhodné je rozhovor směrovat tak, aby si oběť myslela, že právě ona je pánem situace a má vše pod kontrolou. Úplně nejlepší je, pokud nabude dojmu z dobře vykonané práce. Celý hovor musí probíhat v přátelském duchu, bez vyvíjení nátlaku na oběť. 0

1.1.2 Phishing

Phishing je jedna z nejjednodušší formy sociálního inženýrství a tímto pojmem rozumíme lákání citlivých dat od uživatelů prostřednictvím podvodných emailových zpráv, které se na první pohled jeví jako reálné. Jedná se o propracované emaily převážně s bankovní tematikou. Mají stejný vzhled jako emaily odeslané ze skutečné banky. Tyto emaily odkazují na podvodné stránky (opět vypadají téměř identicky se stránkami banky), jen jejich URL je jiné. Na stránkách jsou uživatelé vyzváni k zadání svých přihlašovacích údajů do internetového bankovnictví. Dalším hackery získávaným údajem jsou informace o kreditní kartě (PIN, číslo, platnost, CVC kód). [2] Těmto útokům čelila před čtyřmi lety Česká spořitelna a.s.. Obdobnou metodou je tzv. Pharming. Ten napadá DNS server a přepisuje IP adresy, což způsobí přesměrování uživatele na podvrženou stránku. Touto technikou lze obelhat i zkušené uživatele.

Obr. 1. Podvržené stránky České spořitelny [3]

1.1.3 Trojské koně

Mezi škodlivým software se tento považuje za nejjednodušší. Smyslem je zaujmout uživatele a přimět jej k tomu, aby jej sám spustil. Trojský kůň může být založen na čistě vlastním kódu (je snadno analyzovatelný) nebo v sobě obsahuje nějakou funkci, která skrývá jeho pravý účel. Na rozdíl od virů se trojský kůň samovolně nešíří - šíří ho hackeři nejčastěji prostřednictvím emailových příloh. Existuje více variant spadající do skupiny trojských koňů, mezi nejznámější patří [2][4]:

- **Ovládání vzdáleného systému –** díky tomuto trojskému koni lze pracovat na vzdáleném počítači tak, jako byste u něj přímo seděli. Jejich spuštění je prováděno vždy po startu infikovaného systému a běží na pozadí.
- **Získávání hesel –** tento program běží ve většině případů jen jednou a to spuštěním příslušného souboru. Trojský kůň v systému hledá všechna přístupná hesla a odesílá je zpět k hackerovi.
- **Keylogger –** spouštějící se po startu systému zaznamenává v napadeném počítači stisknuté klávesnice. Následně je zaznamenává a poté odesílá hackerovi.
- **Destruktivní trojské koně –** jejich účelem je smazání obsahu celého disku nebo pouze předem definovaných souborů.
- **Zadní vrátka –** spuštěním tohoto software trojský kůň zajistí otevření síťového portu na cílovém počítači a poskytne hackerovi vstup do systému.

1.1.4 DoS útoky

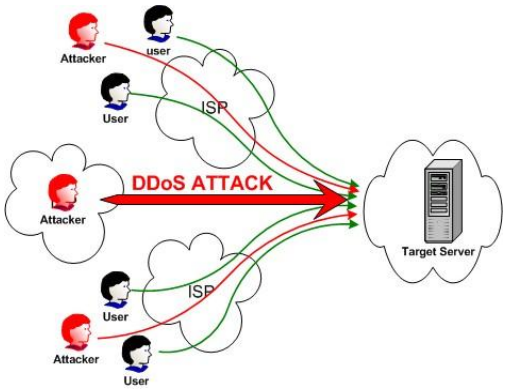
DoS neboli Denial of Service je typ útoku zaměřené na znepřístupnění jisté služby, systému nebo celé sítě. Při použití tohoto útoku se útočí z jednoho počítače a to tím způsobem, že z útočného počítače jsou stále odesílány požadavky na obsloužení. To způsobí nestabilitu, pád nebo restart systému. Použití tohoto typu útoku může být pouze jako dodatečná akce k jinému (hlavnímu) hackerskému útoku a pomocí DoS útoku pouze odlákat pozornost. Existuje několik druhů útoků[5]:

- **Ping of Death** – hacker v tomto případě vytvoří neobvykle velký IP paket a odešle jej na vzdálený systém, který po příjmu způsobuje nestabilitu, pád nebo restart systému.

- **SYN Flood** – na napadený počítač jsou odeslány stovky podvržených požadavků pro synchronizaci, jejich obvyklá úloha je synchronizace na začátku spojení. Systém zareaguje tak, že pro jednotlivé spojení a odeslání odpovědi vyhradí úsek systémových prostředků. Odpovědi se z důvodu podvržené IP adresy systém nedočká, systém se po nějaké době opět dotáže na odpověď a až po několika desítkách vteřin se uzavírá. Výsledkem této akce je z důvodu mnoha polootevřených spojení nemožnost obsloužit regulérní spojení vytvořené uživatelem.
- **LAD Attack** – obdoba SYN Flood, avšak na napadený počítač je v synchronizačním požadavku odeslán zdroj, cíl, IP adresa i port cílového počítače. Výsledkem může být zhroucení systému.
- **Teardrop –** díky nedokonalosti fragmentace odeslaných datagramů při cestě Internetem, přes velké množství směrovačů jsou datagramy rozdělovány do několika menších samostatných datagramů. Při rozdělování se do záhlaví vkládá offset, který určuje, kolik dat bylo přidáno do předchozího datagramu. Teardrop vytváří několik datagramů, které mají navzájem se překrývající offset. Důsledkem to je, že při jejich sestavování do původní podoby se systém zhroutí nebo restartuje.
- **Smurf** - na broadcast adresu určité sítě je odeslán datagram Ping. Broadcast zajistí, že tento datagram je rozeslán do všech počítačů v síti. V závislosti na počtu počítačů v síti roste její zatížení.

1.1.5 DDoS útoky

DDoS neboli Distributed Denial of Service Protection využívá pro provádění útoků více zařízení (až tisíce) nazývaných zombies. Zombies jsou zařízení mnoha uživatelů, kteří ani netuší, že hackeři používají právě jejích počítače k řízeným útokům (hackeři mají tyto zařízení plně pod svou kontrolou). Útoky jsou typu zasílání nekonečného proudu dat k přehlcení spojení mezi síťovým spojením a serverem. [5]



Obr. 2. Znázornění DDoS útoku [7]

1.1.6 Botnety

Jednoduše se dá říct, že to jsou roboti. Jsou tvořeny různou kombinací malware, třeba trojských koní a červů. Můžeme však modifikovat jejich vlastnosti nebo je spustit vzdáleně prostřednictvím Internetu. Takhle mohou být v cíleném počítači jakkoli dlouhou dobu a mohou být využity až v případě potřeby hackera. Šíří se prostřednictvím webových stránek, na kterých se roboti objevují nebo jako součást emailové přílohy. Pomocí Botnetů mohou útočníci rozesílat spam, získávat citlivé údaje, hesla nebo piny bankovních karet a to vše z cizího - vzdáleného počítače. [6]

1.2 Přetrvávající hrozby

Pojmem stále přetrvávající hrozby mám na mysli hrozby, které se objevily v minulosti, stále (ne však v takové míře jako hrozby popsané v kapitole 1.1) se vyskytují a jsou hackery stále používané. Škodlivý software můžeme klasicky rozdělit na viry, malware a spyware. Viry jsou charakteristické svou samovolnou šiřitelností, malware slouží k vniknutí do počítače (a následného útoku) a spyware bez vědomí uživatele odesílá jeho informace (data) útočníkovi. Škodlivého software je nepřeberné množství a každým dnem vznikají nové kopie. Níže uvedené programy nejsou kompletní, jen patří mezi nejčastěji využívané. Informace o nich čerpám z knihy o počítačových virech, kterou napsal Peter Szor. [2]

Viry

Počítačový virus je pojem, který poprvé použil matematik Dr. Frederick Cohen v roce 1984. Jeho definice viru zní: „*Virus je program, který je schopen infekce dalších programů*

a je schopen jejich modifikací zajistit, aby obsahovaly potenciálně se vyvíjející kopii jeho samotného.“ [2]

Jednoduše řečeno, virus je škodlivý software, který v počítači infikuje nejen soubory, ale také systémové prvky. Mohou pozměňovat odkazy vedoucí k těmto prvkům. Jakmile převezmou kontrolu nad určitým prvkem, starají se o svou reprodukci. Důležitou vlastností virů je, že ke svému šíření potřebují hostitele (operační systém nebo spustitelné soubory).

Počítačový červi

Na rozdíl od virů ke svému šíření nepotřebují hostitele a většinou vystupují jako samostatný program. Červi se šíří po síti a jakýkoli virus, šířící se po síti, je tedy považován za počítačového červa. Bez jakéhokoli zásahu uživatele, se červi mohou spouštět na vzdálených počítačích. Dělí se na:

- **Emailoví červi –** šíří se prostřednictvím odeslaných emailů a to jednotlivě, či hromadně. Každý červ odesílá email jinak podle toho, jak byl vytvořen.
- **Chobotnice –** je propracovanější, je umístěná na více počítačích v sítí a vytvořená více programy. Všechny části na síti spolu komunikují a provádějí určitou činnost.
- **Králici –** v celé síti existuje pouze jednou a pouze se přemisťuje mezi ostatními připojenými počítači.

Exploity

Exploity jsou zaměřeny na konkrétní zranitelnost. Cílem je jejich automatické spuštění na systému, na který útočí. Pomocí jednoho exploitačního kódu většinou útočí více hackerů. Prostřednictvím exploitů lze testovat možnost průniku do určitého systému.

Stahovače

Označovány také jako downloadery. Stahovače instalují nové softwarové položky na cílový počítač. Do počítače se dostává prostřednictvím emailu (jako příloha) a následně rozbalí a spustí škodlivý obsah stažený z internetu.

Dialery

Jejich výskyt v dnešní době není nikterak vysoký, protože jsou využívány v oblasti vytáčeného připojení, kdy mění vytáčené číslo na číslo s vysokým tarifem. O tom, že je

použito jiné číslo pro připojení se uživatel dozvídá až prostřednictvím vyúčtování za telefon.

Droppery

Dropper je druh škodlivého software, který slouží k přenesení a nainstalování viru do cílového počítače. Vir po nainstalování již funguje samostatně bez potřeby dropperu a stejně tak se i šíří.

Injektory

Injektory instalují do počítače kód viru. Většinou vkládá funkční kód viru na ovladače přerušení disku. Virus se začne šířit v okamžiku, kdy uživatel běžným způsobem přistoupí k disku. Injektory existují i v síťové formě, kdy vkládají virové kódy po síti.

Auto-Rootery

Tento způsob průniku využívají převážně začínající hackeři. Pomocí Auto-Rooterů se snaží změnit administrátorská práva ve svůj prospěch a to sadou exploitů, které spouštějí na cílovém počítači.

Kity

Jsou to generátory virů, které jednoduše dle požadavků uživatele generují nové viry. Pomocí těchto kitů, muže vytvořit nový škodlivý software i úplný laik.

Spam

Je jakákoli nevyžádaná příchozí zpráva ať už emailová, nebo jiná komunikační zpráva (ICQ, SMS a podobně). Pro hromadné odesílání spamu se využívají speciální programy. Spamové zprávy jsou v dnešní době nejrozšířenější odvětví útoku a trpí jim snad každý uživatel, co komunikuje prostřednictvím Internetu. Tyto nevyžádané zprávy úzce souvisí s phishingem, z čehož vyplývá, že spameři rozesílají obchodně tvářící se emaily, ze kterých lákají citlivá data uživatelů (př. bankovní emaily, ve kterých odkazují na podvrženou stránku a nutí k přihlášení pod hrozbou zrušení účtu).

Hoax

Je obdoba spamu avšak v řetězové formě. V jeho zprávách autor žádá o pomoc, informuje před virem, informuje o jeho škodlivosti a radí jak se mu vyhnout nebo jak jej odstranit.

Tento email vyzívá uživatele, aby zprávu odeslal dál co nejvíce lidem a všechny tak varoval před hrozícím nebezpečím.

Rootkity

Jakmile hacker při svém útoku získá administrátorská práva, využívá sadu hackerských pomůcek, které se nazývají rootkity. Díky nim může maskovat všechen nežádoucí software v počítači.

Hijacker

Pomocí něj může útočník v cílovém počítači měnit různá nastavení. V Internet Exploreru často mění domovskou stránku. Jiné typy se snaží vypnout bránu firewall či antivir.

2 MICROSOFT WINDOWS

Windows je označení operačních systému od společnosti Microsoft. V této části práce si zmíníme všechny verze Windows a rozebereme tři v dnešní době nejpoužívanější systémy od společnosti Microsoft z pohledu jejich zabezpečení a celkové bezpečnosti.

2.1 Starší verze

Microsoft Windows se každou novou verzí vyvíjel a tak se dopracovával až k dnešním operačním systémům. Celý vývoj byl dobře popsán na oficiálních stránkách Microsoft Windows, ze kterých čerpám následující informace 0:

2.1.1 MS-DOS

Roku 1980 byl vyvinut tento prvotní operační systém, který vyplňuje mezeru mezi hardwarem a programy a zároveň ovládá celý hardware počítače. Je určen pro počítače od firmy IBM a o rok později jsou tyto počítače uvedeny na trh. Veškeré ovládání systému spočívalo ve znalosti nového jazyka, který se zadával do příkazového řádku. Tento způsob byl pro běžné uživatele nevhodný, proto se firma Microsoft zaměřila na vývoj nového operačního systému.

2.1.2 Windows 1.0

Windows 1.0 byl na trh uveden roku 1985 jako první operační systém, ke kterému nebyla potřeba znalost speciálního jazyka. K jeho ovládání využíváme myš a okna zobrazovaná na obrazovce. Velkou nevýhodou bylo, že okna se nedala překrývat a byla řazena do fronty. Systém je dodáván s několika programy. Zahrnuje MS-DOS, Malování, Kalkulačku, Windows Writer, Kalendář, Notepad hru Reversi a jiné.

2.1.3 Windows 2.0

Nedostatky jako překrývání oken vyřešila roku 1987 rychlejší verze Windows 2.0. Poprvé zde byla možnost umístit ikony na plochu, měnit rozlišení obrazovky a k urychlení práce zde byly zakomponovány i klávesové zkratky.

2.1.4 Windows 3.0

Tento systém, který má 16-ti barevnou grafiku, zdokonalené ikony a je podstatně výkonnější než jeho předchůdci, byl uveden na trh roku 1990. O dva roky později byla uvedena jeho novější verze Windows 3.1. Díky těmto dvou verzím se společnost Microsoft stala majiteli nepoužívanějšího operačního systému na trhu. Za pouhé dva roky se jich prodalo více než 10 miliónů. Mezi nové funkce zde patří správce tisku a správce programů. Stále více se začínají počítače používat i v domácnosti, a proto byly do systému integrovány další jednoduché hry: Hledání min a karetní hry Solitaire a Srdce. Za zmínku stojí systém Windows for Workgroups 3.11 podporující sítě domény a pracovní skupinu.

2.1.5 Windows NT

V roce 1993 byl vydán tento pokročilý, zcela nový operační systém. Jedinou výraznou změnou byla podpora vědeckých a moderních technických programů a to díky tomu, že tento operační systém je 32bitový.

2.1.6 Windows 95

Byl vydán, jak je již zřejmé z jeho označení, roku 1995 a prolomil rekordní hranice prodaných kopií a to celých 7 milionů za neuvěřitelných 5 týdnů od jeho uvedení na trh. Úplně poprvé se zde naskytuje možnost každé otevřené okno maximalizovat, minimalizovat a zavřít jej. Do systému byl zakomponován hlavní panel s nabídkou START, vytáčené síťové připojení, nové technologie Plug and Play a nachází se zde integrovaná podpora internetu.

2.1.7 Windows 98

Posledním systémem založeným na MS-DOS je vydaný roku 1998 nese název Windows 98. V této době lidé stále více používají Internet doma, v práci nebo v internetových kavárnách. Pomocí Windows 98 lze s Internetem snadněji komunikovat. Novou podporu zde našlo čtení DVD disků a USB zařízení. Díky panelu Rychlé spuštění lze spouštět programy bez nutnosti jejich hledání v nabídce start či na ploše. Zdokonalené zde bylo otevírání a ukončování spuštěných programů.

2.1.8 Windows ME

Windows ME je poslední operační systém, který byl založen na kódu Windows 95. Nově byl do systému zakomponován program Windows Movie Maker, který umožňuje upravovat videa, ukládat a sdílet je. Velkou novinkou byla možnost vrácení konfigurace počítače, jeho software a dat k určitému času, pomocí funkce Obnovení sytému. Zdokonalení bylo v oblasti hudby, videa a domácích sítích. ME byla spolehlivější než předchozí verze.

2.1.9 Windows 2000 Professional

Windows 2000 Professional je založený na kódech systému Windows NT. Nahrazuje doposud všechny předchozí systémy od společnosti Microsoft. Tento systém je spolehlivější, snadněji se používá, má lepší kompatibilitu na internetu a podporuje více mobilních počítačových technologií. Vylepšená je zde podpora zařízení typu USB, infračervených a IEEE 1394. Další znatelně vylepšená podpora je u Plug and Play hardware a pokročilá podpora síťových a bezdrátových produktů.

2.2 Stále používané Windows

Windows 98, ME, 2000 s velkým úspěchem nahradila verze XP. Přinesla řadu novinek, ale i tak měla své chyby, které musely být nahrazovány aktualizačními balíky. Jejím nástupcem se stala Vista. Ta nebyla až tak oblíbená a oproti XP měla díky svým novým grafickým možnostem velké HW nároky. Nicméně byla dobře vybavená a hlavně díky svým novým bezpečnostním funkcím se stala, pro dobu kdy vyšla, dostačujícím a poměrně dobře prodávajícím se systémem. Oba tyto systémy se u nás stále používají, proto je rozeberu podrobněji a zaměřím se více na jejich bezpečnost.

2.2.1 Windows XP

Roku 2001 byl vydán nový operační systém, který byl označován jako použitelný, stabilní a rychlý (výkonný). Mezi jeho přednosti a novinky patří nové uživatelské rozhraní, vestavěná síťová podpora, programová kompatibilita, Windows Update, spousta průvodců (průvodce přidáním hardwaru, průvodce vyčištění plochy, průvodce novým připojením, průvodce přenosem souborů), další ovladače zařízení, efektivní správa uživatelů a spousty

dalších malých vylepšení jako uzamčení hlavního panelu, seskupování tlačítek panelu a podobně. Windows XP se vydává ve dvou edicích: XP Home a XP Professional. [8]

- **XP Home -** Tato verze se často dodávala k nově zakoupeným počítačům. Byla levnější. Určena byla pro malé sítě, ale především pouze pro domácí uživatele. Pod pojmem domácí uživatelé si představujeme ty, kteří nepotřebují složitý systém, nepřipojují se k větším sítím a už vůbec se nechtějí zabývat pojmem zabezpečení. Ze skupin, které jsou rozebrány v kapitole 2.2.1.3, obsahuje Windows XP Home pouze skupinu HelpServiceGroup. [9]
- **XP Professional -** Professional obsahuje vše, co najdete v jeho levnějším vydání. Více se však zaměřuje na bezpečnost systému. V základu obsahuje funkci ASR, což je zálohování a automatická obnova systému. Tato vylepšená edice umožňuje používat takzvané offline soubory. Ty nám umožňují pracovat s kopiemi souborů, které jsou uloženy na síťových discích i po odpojení z dané sítě. Pro zajištění bezpečnosti a nemožnosti zneužít tyto soubory na síťových discích jsou díky Windows XP Profesionál šifrovány. Pokud budeme tento systém instalovat na více počítačů, je nám k dispozici nástroj SYSPREP, pomocí něhož vytvoříme snímek disku, který nakopírujeme do jiného počítače a tím zjednodušíme celou instalaci.[8]

XP a jejich zabezpečení

Účelem systému XP je, že každý uživatel na počítači má svůj uživatelský účet. Bez správného přihlášení se do systému „nikdo“ nedostane. Je vždy potřeba nastavit každému uživateli svůj typ účtu. K dispozici jsou tři typy:

- **Správce počítače -** jak je již z názvu zřejmé, správce má všechna práva a může s počítačem dělat takřka cokoli. Tento neodstranitelný účet byl vytvořen při instalaci operačního systému. Umožňuje vytvářet nové a odstraňovat či měnit stávající účty, instalovat programy, sdílet složky, přebírat vlastnictví souborů a nahlížet do všech souborů, přidávat a odebírat HW zařízení.
- **S omezeným přístupem –** nemožnost instalovat software a měnit uživatelská jména je pro běžného uživatele tou pravou volbou. S tímto účtem má uživatel právo na změnu své ikony a hesla, může používat již nainstalované programy, spravovat soubory ve svých složkách a zobrazovat soubory ve sdílených složkách.

- **Host –** tento typ účtu není ze začátku aktivní. Je vhodný pro příležitost, kdy k počítači bude moci přijít jiná osoba, která nebude mít svůj účet založen, ale bude mít možnost se do počítače přihlásit.

Za zmínku stojí, že vedle uživatelských účtů jsou v tomto systému také skupiny, které mají předdefinované práva a oprávnění. Mezi ně patří:

- **Administrators** – absolutní správa počítače, kde nic není zakázáno.
- **Backup Operators** – tato skupina je určená uživatelům, kteří mají možnost vytvářet zálohy nebo z nich obnovovat systém.
- **Network Configuration Operators** – konfigurace sítě, nastavování sítě a telefonického připojení.
- **Power Users** – skupina uživatelů, kterým je umožněno přidávat sdílet tiskárny a složky, měnit priority procesů a systémový čas. Nemohou zálohovat, přebírat vlastnická práva souborů a instalovat ovladače.
- **Remote Desktop Users** – pokud je zapnuta možnost připojit se k vzdálené ploše, mohou se uživatelé s tímto oprávněním připojit vzdáleně k počítači.
- **Replicator** – možnost spravování replikovaných dat ze serveru.
- **HelpServiceGroup** – skupina uživatelů od společnosti Microsoft, kteří využívají funkci Vzdálená pomoc. Se souhlasem vlastníka počítače se mohou připojit k počítači za účelem odborné pomoci. [8][9]

Aktualizační balíky

Doporučení, která jsou kladena pro systémy XP jsou používat uživatelské účty, kterým se musí nastavit příslušná práva podle toho, o jaký účet se jedná. Tohle ale není zdaleka vše a bohužel v prvním vydání tohoto operačního systému nebyly dostupné základní bezpečnostní prvky jako je brána Firewall. Všechny tyto nedostatky se Microsoft snažil vyřešit pomocí svých aktualizačních balíků, které označoval Service Pack. Celkem byli tři:

- **Service Pack 1, 1a** – z hlediska zabezpečení tato aktualizace nepřinesla nic nového. Ovšem za zmínku stojí, že díky ní se systém XP stal kompatibilní se zařízeními USB 2.0 a dokáže spouštět programy napsané v jazyce Java.

- **Service Pack 2** – jednoduše řečeno, je tento balík zaměřen na doplnění děr týkající se bezpečnosti systému. Výraznou novinkou je pro něj doinstalovaná brána Firewall. Dále díky tomuto balíku systém poskytuje více informací o zabezpečení a uživatelé mohou rozhodovat, jakým způsobem zabezpečí svůj systém. [10]
- **Service Pack 3 –** poslední balík v sobě integruje všechny přechozí. Nepřináší, co se týče zabezpečení, žádnou výraznou změnu či novinku.

2.2.2 Windows Vista

Tento systém byl vydán roku 2006 a přináší s sebou řadu změn. Windows Vista v sobě v základu obsahuje systém s doposud nejsilnějším zabezpečením. Markantní změnou je opět nové grafické prostředí, které je oproti svým předchůdcům nejvíce propracované. Za cenu vysokých HW nároků dostáváte hezký a přehledný systém, který obsahuje vizuální systém zobrazení Aero (ve všech edicích kromě Home Basic). Velký důraz se klade na vyhledávání – je vylepšené. To co hledáte, najdete mnohem rychleji a snadněji. 0

Edice Windows Vista

Systém je dostupný v několika edicích, které se liší svými funkcemi. Mezi ně patří: Home Basic, Home Basic N, Home Premium, Business, Business N, Ultimate a Enterprise. Z hlediska bezpečnosti je dodáván ve čtyřech základních edicích [12]:

Tabulka 1: Porovnání edic z hlediska bezpečnostních funkcí Windows Vista

	Home Basic	Home Premium	Business	Ultimate
BitLocker Drive Encryption				✓
EFS (Encrypting File System)			✓	✓
Rodičovská kontrola	✓	✓		✓
Stínová kopie			✓	✓
Řízení uživatelských účtů	✓	✓	✓	✓
Centrum zálohování a obnovení			✓	✓
Windows Defender	✓	✓	✓	✓
Brána Windows Firewall	✓	✓	✓	✓
Centrum zabezpečení	✓	✓	✓	✓
Služba Windows Update	✓	✓	✓	✓

Bezpečnostní funkce

Windows Vista obsahuje řadu nových bezpečnostních funkcí, které z ní dělají poměrně kvalitně zabezpečený systém i po čisté instalaci. Všechny níže popsané bezpečnostní prvky jsou čerpány ze stránek Microsoftu zabývajícími se bezpečností tohoto operačního systému [12]:

- **BitLocker Drive Encryption** – BitLocker je nástroj, pomocí něj můžeme šifrovat veškerá data. Používá se k ochraně citlivých dat nebo pro osobní či pracovní účely.
- **EFS (Encrypting File System) –** v případě, kdy jeden počítač používá více uživatelů, může správce pomoci této funkce zašifrovat data každému tak, aby byla dostupná pouze jim. Ukládání klíčů je pomocí Windows Vista možné i na čipové karty.
- **Rodičovská kontrola –** jak z názvu vyplývá, jedná se o rodičovskou ochranu, kdy počítač dodržuje pravidla navolená rodiči před nevhodným webovým obsahem či hraní her a používáním programů v určitou denní dobu.
- **Stínová kopie –** je automaticky zapnuta. V průběhu práce, vytváří tato funkce v pravidelných intervalech kopie přírůstků změněných souborů. Nezabírá mnoho místa z důvodu ukládání přírůstku, ne celého souboru. Pomocí stínové kopie můžeme zpět získat dokumenty, které omylem smažeme.
- **Řízení uživatelských účtů –** ve spolupráci s Windows Defender, Internet Explorer ve verzích 7 a 8 snižuje následky spyware, virů či jiných hrozeb. Dále ve spolupráci s Rodičovskou kontrolou můžeme mít přehled o tom, které weby, programy nebo hry daný uživatelský účet používá či instaluje. Sama funkce brání potenciálnímu škodlivému softwaru provádět změny v počítači, bez souhlasu uživatele.
- **Centrum zálohování a obnovení –** je rozlišováno na dva typy: Zálohování Complete PC Backup, které provádí zálohu celého počítače, včetně operačního systému, a Automatické zálohování, které provádí zálohu pouze souborů a dat. Centrum zálohování a obnovení vytváří bod obnovy, ke kterému je možno přistoupit v případě problémů.
- **Windows Defender –** mnohými je považován za antivirový program od Microsoftu, ve výsledku ale neplní dostatečně všechny funkce jako čistě antivirový

program. Je to především ochrana před spyware a podobnému škodlivému softwaru.

- **Brána Windows Firewall –** okamžitě po nainstalování nového systému je brána Firewall zapnuta a chrání počítač před mnoha typy škodlivého softwaru. Pracuje na principu omezování prostředků systému, pokud se nechovají tak, jak je od nich očekáváno. Díky správné konfiguraci brány můžeme zabránit vniku škodlivého software přímo do počítače a tím i do celé sítě, ve které je počítač připojen.
- **Centrum zabezpečení –** hlídá aktuálnost a zobrazuje zabezpečovací prostředky. Mezi ně patří ochrana proti malware, automatické aktualizace, nastavení brány firewall a další nastavení, kde zobrazuje nastavení zabezpečení internetu a nástroj řízení uživatelských účtů.
- **Služba Windows Update –** Microsoft vydává pro Windows Vista mnoho aktualizací, které obsahují záplaty a nové bezpečnostní balíky. Aby byl systém aktuální, musí být povoleny automatické aktualizace ve službě Windows Update. Pokud je tato služba uživatelem povolena, program si automaticky vyhledá potřebné aktualizace, sám je stáhne a nainstaluje.

Aktualizační balíky

Stejně jako u předchozího operačního systému byly na tento Windows vydány aktualizační balíky nesoucí název Service Pack.

- **Service Pack 1 –** tento balík zvyšuje spolehlivost, výkon a bezpečnost. Co se týče spolehlivosti, tento balík vylepšuje oblast bezdrátových připojení (ad hoc a peer-to-peer). Díky zvýšenému výkonu je po instalaci balíku rychlejší kopírování a extrahování souborů, rychlejší probuzení z hibernace a úsporného režimu, velké obrázkové soubory jsou nyní rychleji načítány a podobně. V oblasti bezpečnosti je novou funkcí šifrování více než jednoho oddílu pevného disku nástrojem BitLocker (dostupné pouze v edicích Enterprise a Ultimate). Změny jsou dále v principu vyhledávání a paměť RAM již správně ukazuje svoji velikost (dříve ukazoval velikost, která může být systémem využita). [13]
- **Service Pack 2 –** tento aktualizační balík zvyšuje kompatibilitu programů, zvýšenou podporu hardware a Bluetooth. Dále po této aktualizaci dostáváme

podporu pro disky Blue-ray a Windows Search 4.0, což je vylepšené vyhledávání a indexování. [14]

2.3 Windows 7

Roku 2009 Microsoft vydává svou nejnovější verzi operačního systému. Nese název Windows 7. V době psaní této práce je to se 40,4 % druhý nejpoužívanější operační systém v České republice. Na prvním místě je stále Windows XP, kteří tvoří 44,6 % většinu (četnost Windows Vista je 10,93 %, Mac Os X – 0,85 %, Linux 0,77 %). [15] Jeho základy jsou postaveny na Windows Vista, nicméně obsahuje mnoho nových a spousty vylepšených stávajících funkcí. Tento systém je uživatelsky příjemný, a proto většina odpůrců Windows Vista zastánců XP přecházela až na tento systém.

2.3.1 Edice Windows 7

Jako tomu bylo u předchůdce Windows Vista, tak i u tohoto nového operačního systému je na výběr z několika edic, které se liší různými funkcemi. Nejvíce distribuované a Microsoftem podporované edice jsou Home Premium a Professional. Ostatní jsou pro specifické trhy – Starter (pro netbooky), Home Basic (standardně dodávaná s novými zařízeními), Enterprise (pro velké korporace) a Ultimate (pro nadšence). [16]

Tabulka 2: Porovnání edic z hlediska bezpečnostních funkcí Windows 7

	Starter	Home Basic	Home Premium	Professional	Enterprise a Ultimate
Windows Firewall	✓	✓	✓	✓	✓
Windows Defender	✓	✓	✓	✓	✓
Řízení uživatelských účtů	✓	✓	✓	✓	✓
Rodičovská kontrola	✓	✓	✓	✓	✓
Správce pověření	✓	✓	✓	✓	✓
Zálohování a obnova	✓	✓	✓	✓	✓
Centrum Akcí	✓	✓	✓	✓	✓
EFS (Encrypting File System)				✓	✓
Pokročilé zálohování a obnovení				✓	✓
Nástroj BitLocker					✓
BitLocker To Go					✓
AppLocker					✓
DirectAccess					✓

2.3.2 Novinky a vylepšení

Jako všechny nové verze operačních systému, tak i Windows 7 přichází s řadou změn a novinek. Mezi hlavní změny patří hlavní panel, funkce Jump List, propracovanější grafické rozhraní Aero, vylepšené sdílení a lepší práce s miniaplikacemi.

Hlavní panel

Hlavní panel je propracovanější a vylepšený co do ovládání. Zmizel panel Snadné spuštění, umístěný vpravo od tlačítka start, na nějž se umisťovaly ikony zástupců různých aplikací. Místo toho, aby se po spuštění aplikace zobrazilo dlouhé okénko se spuštěným programem, a jeho popiskem je to v tomto panelu vyřešeno elegantněji. Na tento panel je možno vkládat ikony po celé jeho délce a v případě spuštění jakéhokoli programu se jeho ikona zvýrazní průhledným rámečkem. Dále v případě najetí na ikonu spuštěného programu zobrazí jeho náhled, což je výhodou v případě vícenásobného spuštění a rozlišení toho pravého programu. [17]

Obr. 3. Hlavní panel

Jump List

Tato funkce není nic jiného než přístup k naposledy otevřeným dokumentům, hudebním souborům, videím a podobně. Přístupem se v tomto případě rozumí kliknutí pravým tlačítkem na ikonu na liště a následně se vyroluje nabídka posledních souborů. [17]

Aero

Grafické rozhraní aero má tři úplně nové funkce [17]:

- **Aero Peek** – tato funkce se spouští najetím do pravého dolního rohu. Zobrazí se plocha a na ni všechna otevřená okna v průhledných rámečcích se světlými průhlednými pruhy přes plochu. Pokud jsou pruhy přes celou obrazovku, značí to otevřené maximalizované okno.
- **Aero Shake** – v případě, že máme otevřených více oken vedle sebe a chceme, aby nám zůstalo pouze jedno okno a ostatní minimalizovat, stačí uchopit okno, co

chceme ponechat a zatřepat s ním. Neuchopená okna se minimalizují. Opětovným zatřepáním dostaneme okna do původní polohy.

- **Aero Snap –** chycením za horní okraj okna a přetáhnutí okna k pravému okraji se k němu okno zarovná z pravého okraje a roztáhne se až přesně do poloviny. Takovýmto způsobem můžeme jednoduše zarovnat dvě okna vedle sebe. Takhle lze také snadno okno maximalizovat a to přetáhnutím okna k hornímu okraji.

Sdílení

Oproti předchozím verzím je nastavování sdílení jednoduché a konečně funkční. Nastavení domácího sdílení opravdu jednoduché, pouhým zatrhnutím periferií, obsahu a nastavením hesla daný obsah sdílíme. [17]

Miniaplikace

Miniaplikace se poprvé objevili ve Windows Vista. Umisťovaly se na speciální postranní panel. Ve Windows 7 již postranní panel nenajdete, miniaplikace se umisťují přímo na plochu. [17]

2.3.3 Bezpečnostní funkce systému

Co se týče bezpečnostních funkcí, ve Windows 7 nejsou žádné nové (oproti Windows Vista), pouze vylepšené a na vyšší úrovni. Informace o bezpečnostních funkcích jsou čerpány z knihy o Windows 7, kterou napsal Steve Sinchak. [16]

Centrum akcí

Na centrum akcí bylo v tomto systému přejmenováno Centrum zabezpečení, které se objevovalo v systémech XP a Vista. Shromažďuje všechny dostupné bezpečnostní funkce nejen od Microsoftu, ale také doinstalované programy od jiných společností. V centru akcí najdeme stav brány Firewall, informuje nás o automatických aktualizacích (Windows Update) a nástroj Řízení uživatelských účtů. Najdeme zde také nastavení zabezpečení internetu (sleduje, zda zabezpečení má patřičnou úroveň), antivirovou ochranu, ochranu proti spyware a dalšímu nežádoucímu software. Je zde také zmíněno o architektuře NAP, což je platforma ke zvýšení zabezpečení sítě pro jeho správce.

Windows Firewall

Ve Windows 7 je brána Firewall mnohem bezpečnější, než u předchozích operačních systémů společnosti Microsoft. Po připojení k síti nabídne Firewall možnost zařadit danou síť do tří kategorií – veřejné, pracovní a domácí. Každá z těchto kategorií skýtá určitá pravidla a zabezpečení vhodná právě pro danou síť (jednotlivé nastavení lze konfigurovat). Firewall v tomto systému umí zachytávat příchozí i odchozí provoz. Windows Firewall se vyvíjel v každé verzi operačního systému. V tomto je na velmi vysoké úrovni a je to velice užitečný a potřebný bezpečnostní prvek operačního systému.

Řízení uživatelských účtů

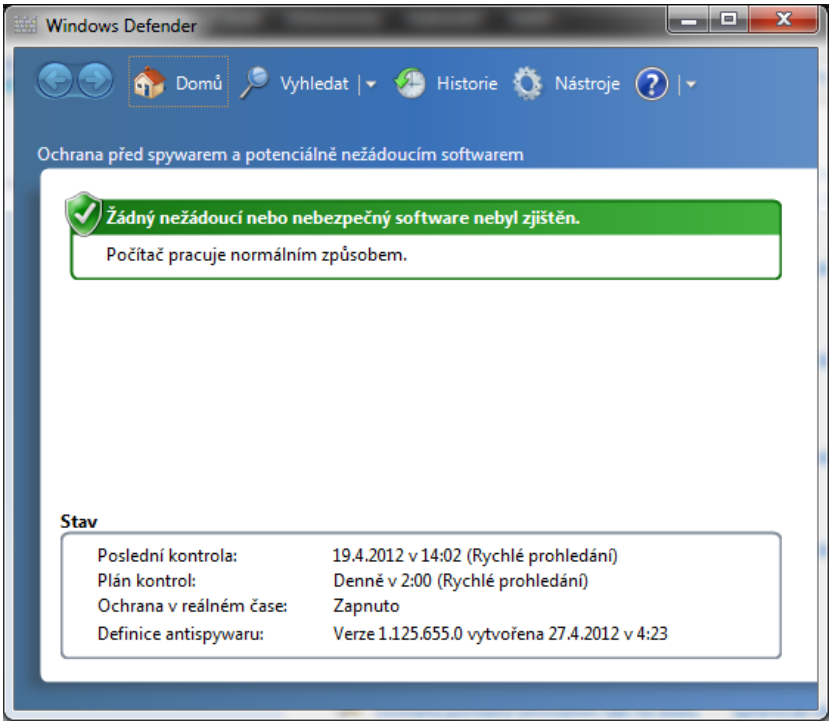
Poprvé se tato funkce objevila již ve Windows Vista, kde sice byla užitečným, ale pro většinu uživatelů velice otravným bezpečnostním doplňkem. Ve Windows 7 je tato funkce vylepšena a minimalizuje potřebu přerušovat uživatele při práci. Má úplnou kontrolu nad veškerými změnami probíhajících v systému. Instalace nežádoucího software je zde obtížnější. Všechna instalace musí projít nástrojem Řízení uživatelských účtů. Pokud je instalace schopna provést změnu nastavení systému nebo pokud prováděná činnost potřebuje vyšší oprávnění, je zobrazeno dialogové okno, které musí být uživatelem potvrzeno. Tato vylepšená funkce zamezuje automatické instalaci škodlivého software bez vědomí uživatele a její nastavení lze upravovat ve čtyřech stupních ochrany:

- **Vždy upozorňovat** - pokud se programy snaží nainstalovat software nebo provést změnu v počítači nebo pokud uživatel provede změnu v nastavení systému.
- **Výchozí** – pokud se snaží programy provést změnu v systému a neupozorňovat, když uživatel provede změnu nastavení systému.
- **Pouze programy –** upozorňuje, pokud se o změnu v systému pokoušejí programy, nereaguje na změnu systému uživatele.
- **Nikdy neupozorňovat –** ani v případě pokusů o změnu programy.

Windows Defender

Defender je anti-spyware program. V systému automaticky (podle nastavených hodnot) prohlíží soubory a registry, ve kterých hledá signatury škodlivých softwarů. Spolupracuje se službou Microsoft SpyNet, která zajišťuje aktuálnost hledaných signatur. V případě, že

Defender najde podezřele vypadající soubor, ale nebude schopen jistě určit, zda je škodlivý či není, informace o souboru zašle komunitě Microsoft SpyNet, která bude daný soubor nadále pozorovat. Defender, kromě monitorování a detekování souborů, sleduje právě běžící procesy v paměti a sleduje aplikace instalované ve skupině Po spuštění.



Obr. 4. Náhled na program Windows Defender

Zálohování a obnovení

Díky automatickým zálohám můžeme kdykoli systém vrátit zpět do předchozího stavu. V tomto systému je funkce poupravena tak, že při obnově stačí pouze „kliknout myší“. V případě, že systém bude infikován nějakým zákeřným virem, není nic jednoduššího než provést obnovu do doby, kdy vir ještě nebyl aktivní (nebyl stažen). Výhodou je nastavení záloh na automatiku, kdy počítač bude zálohy dělat pravidelně bez nutnosti zásahu uživatele.

Správce pověření

Tato funkce umožňuje ukládat uživatelská jména a hesla používaná k přihlašování k jiným počítačům v síti nebo k webovým stránkám. Systém Windows se bude schopen přihlásit k webové stránce či jinému počítači automaticky uživatele, který bude mít uložena svá pověření. Funkce pracuje s tzv. trezory, do kterých ukládá právě zmiňovaná pověření a ze kterých je může bezpečně využít k přihlášení. [18]

Pokročilé bezpečnostní funkce

Tyto čtyři funkce jsou dodávány pouze v distribucích Enterprise a Ultimate. Jak už bylo zmíněno u Windows Vista, tak i u Windows 7 je BitLocker určen k šifrování dat na disku. Nástroj BitLocker To Go slouží také k šifrování, ale přenositelných zařízení jako jsou USB a externí disky. AppLocker slouží k zamezení spouštění aplikací pro různé uživatele a DirectAccess umožňuje vzdálené připojení se do interní sítě.

2.4 Windows 8

V době psaní této bakalářské práce se již vyvíjel nový operační systém od společnosti Microsoft a to Windows 8. Tento systém jsem netestoval, protože ještě nebyla vydána oficiální verze. Měl jsem však možnost stáhnutí Consumer Preview a jeho lehkého prozkoumání. Hned na první pohled je vidět, že je tento systém bude spojovat osobní počítače a dotykové tablety. Zmizelo klasické tlačítko start a je umístěno v levém panelu (pro jeho zobrazení je třeba najet do levého horního nebo spodního rohu a panel se zobrazí), kde je dále možno vyhledávat, provádět nastavení, sdílet nebo spravovat připojená zařízení. Největší změnou je kompletně přepracovaná nabídka start, která je téměř identická s deskovým systémem nového Windows Mobile. Co se týče bezpečnosti, měl by tento nový systém dostat nové funkce. Neměly by to být žádné výrazné změny, pouze malé modifikace, díky kterým bude obtížnější průnik pro všechen škodlivý software. Mezi největší novinku bude jistě patřit zabezpečené bootování bránící napadení malware při startu systému, dříve než se aktivuje antivirová ochrana Windows. [19]

Obr. 5. Nabídka Start v prostředí Windows 8

II. PRAKTICKÁ ČÁST

3 RADY K ZABEZPEČENÍ

Útoky mohou být prováděny ze dvou pozic. V první může být hacker kdekoli v síti Internet a snaží se do cílového počítače dostat vzdáleně. Toto je v práci nazváno jako Ochrana před internetovými útoky. V druhém případě je útočník fyzicky přístupný k cílovému počítači - v práci nazváno jako Ochrana proti neoprávněnému přístupu. Obě pozice spolu úzce souvisejí a vždy je potřeba brát zřetel na to, že útočník se do počítače může dostat kdykoli. Cílenou osobou se může stát úplně každý, ať už je to podnikatel vlastnící malou firmu, který čelí cílenému vnitřnímu útoku nespokojeného zaměstnance, nebo velká korporace čelící velkému připravovanému útoku typu DDoS. Cílem se může stát i „obyčejná“ osoba, která je pouze zajímavá třeba pro hackera začátečníka, který si potřebuje vyzkoušet nově nastudované znalosti průniku z Internetu. Z tohoto vyplývá, že potřeba zabezpečit svůj systém platí pro každého a není vhodné spoléhat na klasickou větu: „Mě se to nemůže stát.“ V následující části uvádím rady k zabezpečení operačního systému Windows 7.

3.1 Ochrana před internetovými útoky

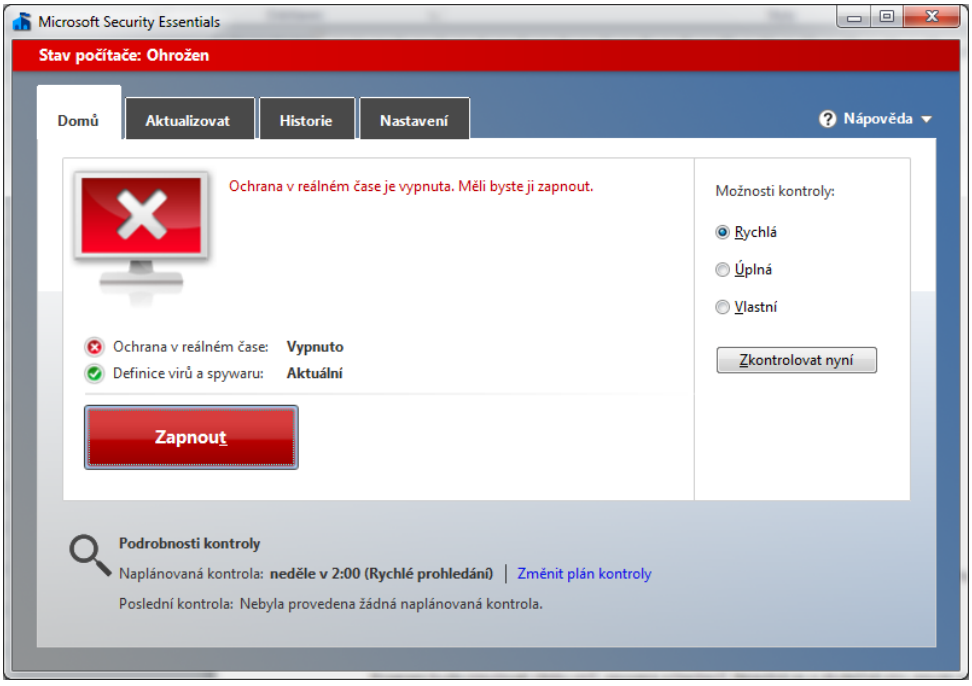
Pro standardní ochranu operačního systému je třeba mít aktivní tři bezpečnostní prvky. Jsou jimi brána Firewall, Antivirový a Antispyware program. Do této kategorie můžeme zařadit také inteligentní chování uživatele. Příkladem by uživatel neměl otevírat neznámé přílohy příchozích emailů, stejně tak jako stahovat nedůvěryhodné programy (a podobně). Je důležité, aby antivirový program a brána Firewall byly zapnuty ještě dříve, než bude počítač připojen k Internetu.

3.1.1 Brána Firewall

Jednoduše řečeno, brána Firewall slouží k oddělení provozu mezi domácí sítí a internetem. Podle definovaných podmínek propouští dvěma směry (do počítače, z něj). Díky tomu brání před neoprávněnými průniky do systému a odesílání dat z počítače bez vědomí uživatele. Brána Firewall je k dispozici ve všech distribucích Windows 7. Je automaticky zapnuta a je poměrně na kvalitní bezpečnostní úrovni, což nám ušetřuje starost hledat a stahovat (popřípadě platit) jinou. Windows Firewall je primární ochranou před internetovými útoky hackerů a různému škodlivému software. Doporučení je, aby v každém případě byla brána Firewall aktivní.

3.1.2 Ochrana proti virům

Bránit se proti virům je v dnešní době nejzákladnější forma ochrany operačních systémů. Instalace antivirového programu, by měla to být jedna z prvních akcí, které po nainstalování nového systému uživatel udělá. Antivirové programy by měly mít povolené automatické aktualizace z důvodu aktuálnosti virové databáze a měly by být nepřetržitě zapnuty. Bohužel, po instalaci Windows 7 se v systému nenachází žádný antivirový program. Microsoft však nabízí svůj antivirový program s názvem **Microsoft Security Essentials**, který je k dispozici zdarma. Microsoft o něm uvádí, že je to ochrana proti virům, spyware a jiným škodlivým software. Poskytuje ochranu v reálném čase a je určen pro domácnosti a malé firmy. Po jeho instalaci se jednou za 24 hodin automaticky aktualizuje. Pokud tento antivir nalezne nějakou hrozbu, signalizuje ji prostřednictvím žluté nebo červené ikonky na hlavním panelu. Při přístupu na ikonku nebo spuštění programu sám uživateli doporučí, jak by měl postupovat. V nepřítomnosti uživatele program sám provede výchozí akce a uživatel po návratu na pracoviště může akci zkontrolovat a eventuálně ji vrátit zpět. [20]



Obr. 6. Microsoft Security Essentials bez zapnuté rezidentní ochrany

3.1.3 Ochrana proti spyware

Jak už bylo uvedeno výše, spyware je nežádoucí software, který shromažďuje informace o cílené osobě a posílá je zpět k útočníkovi. Pracuje bez vědomí uživatele a mezi nejčastější činnost tohoto programu patří: stahování a instalování dalšího nežádoucí software, změna nastavení internetového prohlížeče, přesměrovává připojení a podobně. Protože se spyware nechová jako virus, antivirové programy je ve většině případů nedetekují. Z toho důvodu vznikly Antispyware programy. Windows 7 nabízí ve všech edicích svůj Windows Defender, který chrání před tímto typem škodlivého software. Antispyware program je třetím bezpečnostním programem, který by na žádném počítači neměl chybět.

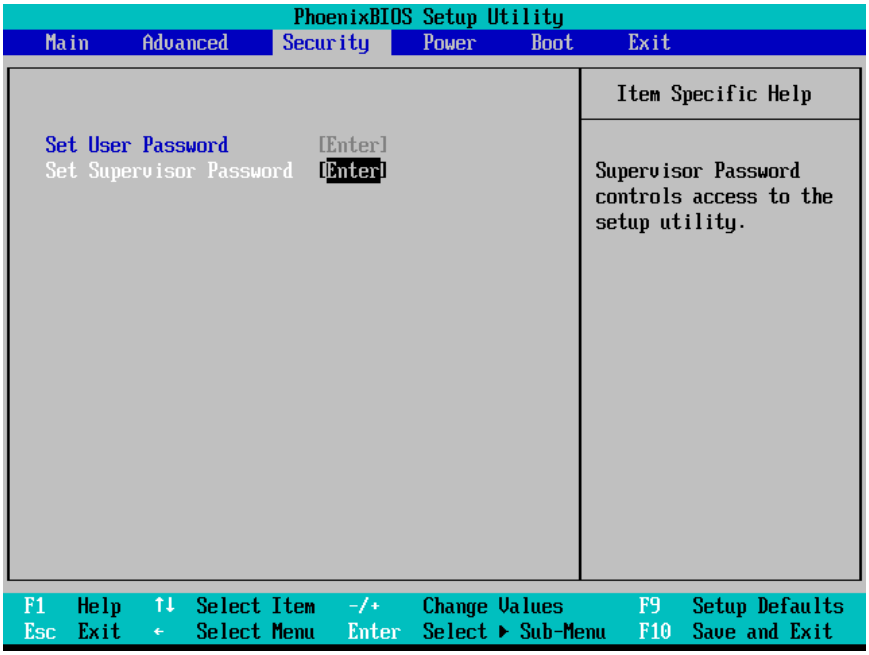
3.2 Ochrana proti neoprávněnému přístupu

Nejlepší ochranou proti neoprávněnému lokálnímu přístupu by zajisté bylo mít počítač střežený 24 hodin denně ochrankou. To je však nemyslitelné a přehnané, zvláště u obyčejných stolních počítačů. V dnešní době notebooků si tento neoprávněný lokální přístup pohlídá každý uživatel tím, že svůj notebook nebude vystavovat jiným osobám bez jeho dohledu. Pokud se ovšem jedná o osobní počítač, řekněme firemní nebo počítač ve studovně, a potřebujeme omezit přístup jen určitým osobám, musíme podle toho počítač nastavit. Do této kategorie spadají BIOS hesla a hesla pro vstup do operačního systému.

3.2.1 BIOS heslo

Zkratka BIOS znamená Basic Input Output System (v překladu základní vstupně výstupní systém), sloužící ke konfiguraci připojených zařízení, nastavení počátečních hodnot a spuštění operačního systému. Jednoduše řečeno, slouží k propojení hardware a software. Heslem můžeme zablokovat vstup do BIOSU nebo spuštění operačního systému. Není to často používaná metoda a navíc lze jednoduše prolomit. Existují tři druhy způsobů průniku. Prvním je zkoušení univerzálních hesel dle typu výrobce. Druhým je použití programů, které se dokáží dostat do paměti pro hesla a v nich heslo najít. Třetím, nejzaručenějším a pravděpodobně nejrychlejším způsobem, je restartování BIOSu. Restartovat lze softwarově pomocí speciálních programů nebo hardwarově prostřednictvím odpojení napájení (odpojení baterie nebo přehození Clear CMOS Jumperu dle návodu). Každopádně, pokud bude počítač vystaven veřejnému přístupu, je vhodné používat tohle

heslo. Zabráníme tak možnosti změnit inicializaci systému a konfiguraci hardware (příkladem může útočník změnit BOOT pořadí, spustit Live disk a tak se dostat k datům). V případě napadení počítače s tímto heslem, bude mít heslo minimálně zpomalující účinky pro průnik (v případě nezkušeného útočníka, zde jeho pokus o průnik ztroskotá).



Obr. 7. Nastavení hesla v BIOSU [21]

3.2.2 Heslo pro vstup do systému

Toto heslo by měl obsahovat každý systém, i když je snadno rozluštitelné. U novějších operačních systémů jako je Windows 7, je zjištění hesla obtížnější (u starších Windows, typu XP, lze heslo rozluštit v řádech několika minut pomocí nabootování live CD OPHCrack a jejich následné rozluštění). Pomocí zaheslovaných uživatelských účtů lze rozlišit několik uživatelů pro vstup do stejného operačního systému a zabránit jim vzájemné procházení souborů a složek. Stejně jako u BIOS hesla je pro neznalého útočníka překonání tohoto hesla nemožné. Pro zkušeného a znalého tohle heslo nebude i s patřičnou dávkou času velkou překážkou. Heslo pro vstup do účtu by mělo být silné. Guest je ve Windows 7 standardně vypnutý, to ale nestačí a nejlepším způsobem jak zabránit průniku přes tento účet je přejmenovat jej a vytvořit mu patřičně silné heslo (ponechat účet vypnutý). Je vhodné také vypnout, přejmenovat a dobře zaheslovat i administrátorský účet. Těmito způsoby se však škodlivého software nezbavíme, pouze ztížíme najít pro ně potřebné účty. [16]

3.3 Speciální ochrany dat

V případech, kdy se útočník pronikne do cíleného počítače, ať už vzdáleně nebo lokálně, existuje možnost, jak před ním data z počítače ochránit - pomocí **šifrování**. Šifrování je účinná metoda ochrany dat. Šifrovat lze soubory nebo celé disky či jeho oddíly. K tomuto se ve Windows 7 (pouze edice Enterprise a Ultimate) nachází speciální nástroj BitLocker. Tento nástroj umí zašifrovat jak disky, tak i oddíly, dokonce i ty, kde je nainstalován operační systém. Výhodou toho je, že operační systém nikdo nespustí bez přístupu k jednotce, na které je uložen šifrovací klíč. Start zašifrovaného systému spočívá v jeho spuštění a následném čekání na šifrovaný klíč nebo na zařízení USB, kde je klíč uložen. [16]

3.4 Další zásady zabezpečení

Bez ohledu na pozici útočníka existuje ještě několik zásad, které dopomáhají udržovat zabezpečený operační systém. Patří do nich aktuálnost všech bezpečnostních prvků, používání správného typu účtu, správně (bezpečně) zacházet a dodržovat zásady práce s hesly a v neposlední řadě sledovat zabezpečení operačního systému minimálně v nástrojích, které jsou již v systému zahrnuty.

3.4.1 Udržení aktuálního systému

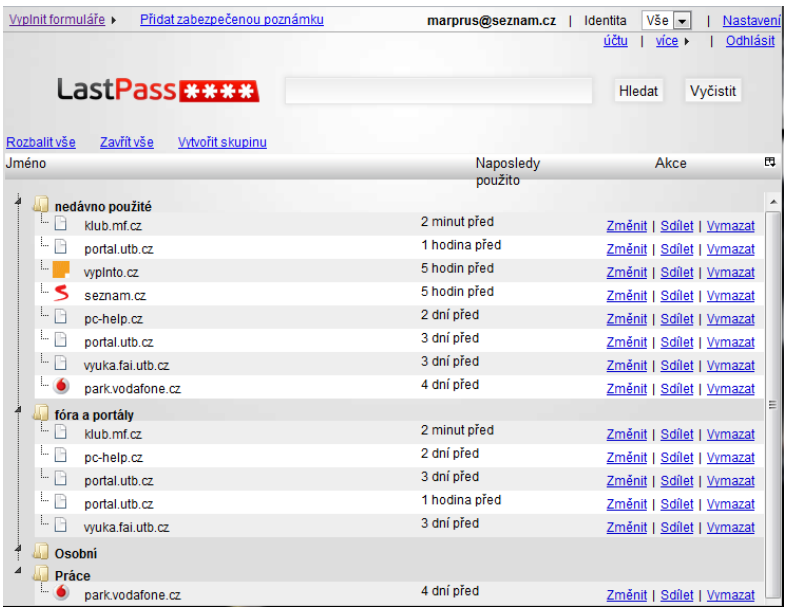
Stejně jako u Antiviru či Antispyware, tak i u vlastního operačního systému je třeba udržovat jeho aktuálnost. Tu zajistíme pomocí automatických aktualizací v nástroji Windows Update. I pro Windows 7 společnost Microsoft vydává aktualizace a bezpečnostní záplaty. Proto je důležité ponechat zapnuté automatické aktualizace a nechat systém, aby se sám v nastavený čas automaticky aktualizoval.

3.4.2 Používat správný typ účtu

Pro běžné používání počítače by uživatelé neměli používat administrátorský účet. Pro tuto činnost je vhodné používat běžné uživatelské účty s omezenými právy. Lze tím zamezit nechtěnému poškození či změnění systému. Všechny uživatelské účty by měly mít nastavené silné heslo pro vstup kvůli případnému lokálnímu pokusu o průnik.

3.4.3 Správná práce s hesly

Se zabezpečením úzce souvisí práce s **hesly**. V zásadě platí čtyři skutečnosti. První je používat silné heslo. To je složeno minimálně z 8 znaků kombinující malá a velká písmena, speciální znaky a číslice. Druhou je jejich pravidelné obměňování a tím tak možné přerušení hackerského útoku. Třetí je nepoužívat stejné heslo k více účtům. Tou poslední je hesla bezmyšlenkovitě neukládat v prohlížečích (nejlepší způsob úschovy je v lidském mozku). Pro třetí a čtvrtou situaci existuje varianta pomocných programů, které si za nás pamatují všechna hesla a k jejich spuštění stačí jedno (master) heslo. Na to je ovšem kladeno velký důraz - musí být opravdu silné. Dle mého názoru, je lepší si zapamatovat jedno nesmyslné a tím i řádně silné než 10 jiných snadno rozluštitelných hesel. Jako příklad mohu uvést program, který tohle umí – jmenuje se LastPass.



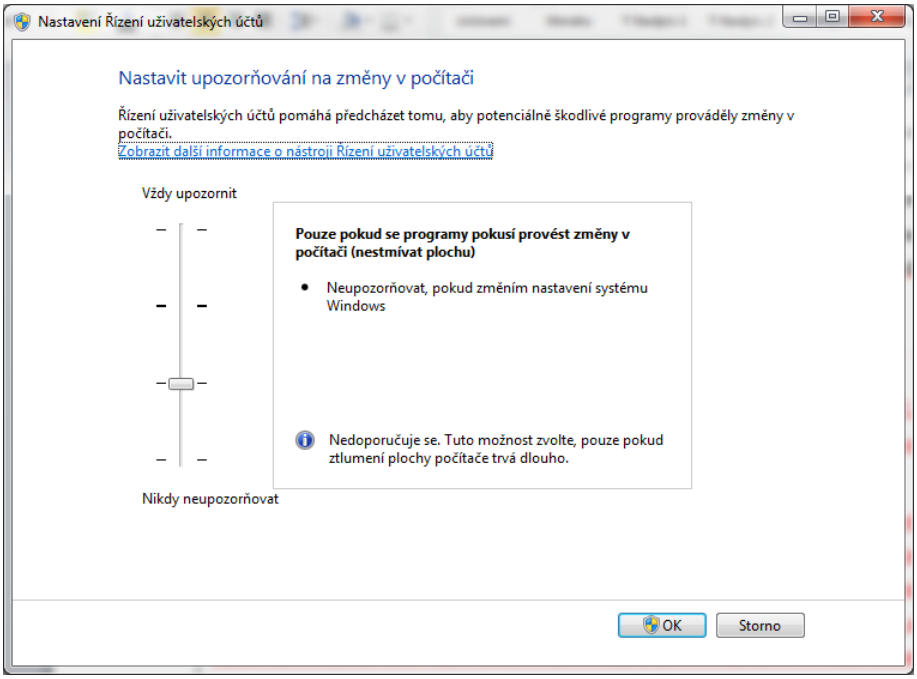
Obr. 1. Náhled na program LastPass

Tvorba silných hesel může být pro mnohé velmi obtížné. Existují programy i webové stránky, které generují náhodná hesla. Jako příklad mohu uvést online generátory http://www.pctools.com/guides/password/ nebo http://strongpasswordgenerator.com/, které generují hesla podle zadaných parametrů a nabízí k nim i klíč k zapamatování. Příkladem programových generátorů mohu uvést Password Generator nebo NeroFX Password Generator.

3.4.4 Systémové nastavení

Vhodné je sledovat **Centrum akcí**, které bylo popsáno v teoretické části kapitole 4.3.1. Jsou v něm vypsané všechny bezpečnostní prvky s popiskem o jeho zapnutí/vypnutí a jeho stavu. Vše je přehledné a hlavně je vše pohromadě na jednom místě.

Nástroj **Řízení uživatelských účtů** poskytuje kvalitní kontrolu nad všemi aplikacemi, které se instalují do počítače. Je vhodné ponechat minimálně výchozí nastavení, které je optimální mezi dostatečným zabezpečením a snesitelným, co se týče potřeby potvrzování uživatelem. Pokud uživatel na počítači nic neinstaluje, pouze jej v danou chvíli používá, a Řízení uživatelských účtů vypíše hlášku k potvrzení, je potřeba zjistit, co se snaží získat uživatelův souhlas. Pod tímto se může skrývat nějaký škodlivý software. [16]



Obr. 8. Nastavení řízení uživatelských účtů

4 POVĚDOMÍ UŽIVATELŮ O BEZPEČNOSTI

V této kapitole se zabývám povědomím uživatelů o zabezpečení a celkové bezpečnosti operačních systémů. Informace jsou získány na základě vypracovaného veřejného dotazníku na serveru Vyplnto.cz, která napomáhá vytvoření internetových průzkumů a jejich šíření. Tento průzkum byl šířen převážně přes Facebook a cílová skupina jsou mí přátelé. Dotazník celkově vyplnilo 185 respondentů a je součástí přílohy této bakalářské práce. Níže jsou rozebrány odpovědi na otázky a u některých jsou zobrazeny grafy pro zvýšení přehlednosti. Dotazník byl spuštěn celkově dvakrát, podruhé jsem jej doplnil o pět nových otázek týkajících se důležitých bezpečnostních zásad. Doplnění proběhlo z důvodu potřeby získání více informací pro kvalitnější zpracování dané problematiky. Oba dotazníky nebyly k vyplnění nabídnuty stejným respondentům.

Obr. 9. Náhled na dotazník ze serveru Vyplňto.cz

4.1 Otázky na hesla

Hesla jsou jedny z nejdůležitějších údajů, které si každý musí chránit. Nacházejí se téměř všude, ať už jsou to hesla k bankovnictví, platebním kartám či jako druhý údaj k přihlášení do emailu. V průzkumu byly položeny otázky zaměřeny na sílu hesla, jejich obměňování, ukládání v internetových prohlížečích a na jejich tvorbu.

4.1.1 Nejsilnější heslo

Na otázku, které heslo je nejsilnější, byly respondentům nabídnuty tři odpovědi. Správně, mlw51//Uy, odpovědělo 179 respondentů (96,7 %). Z toho vyplývá, že téměř všichni respondenti dokáží na první pohled rozlišit bezpečné heslo oproti jednoduchým.

4.1.2 Četnost změny hesla

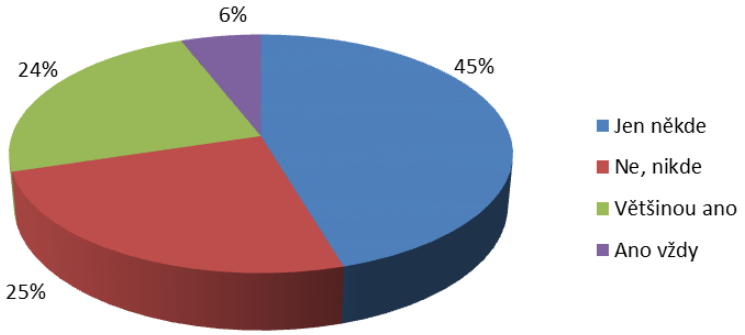
Z otázky „Jak často měníte heslo?“ je zřejmé, že respondenti stále nedbají bezpečnostních rad - 135 z nich si totiž své heslo vůbec nemění. Pouze 4 uživatelé (2,1 % ze všech vyplňujících) si své heslo mění pravidelně jedenkrát do měsíce.

4.1.3 Možnost vytvoření hesla

Nevhodně v otázce „Jak vytváříte hesla?“ odpovědělo 7 % respondentů. Při tvorbě hesel používají své osobní údaje, což je zásadní bezpečnostní chyba. Pouze tři procenta respondentů si při tvorbě hesel pomáhají generátory.

4.1.4 Ukládání hesel v prohlížečích

Z otázky „Ukládáte v prohlížečích Vaše hesla?“ je zřejmé, že uživatelé jsou opatrní při ukládání svých hesel v Internetových prohlížečích. Pouze 6% vyplňujících ukládá svá hesla všech stránek bez ohledu na jejich možné zneužití. Zbylí s hesly nakládají více opatrně.



Obr. 10. Graf ankety – otázka na ukládání hesel v prohlížečích

4.2 Otázky na uživatelské účty

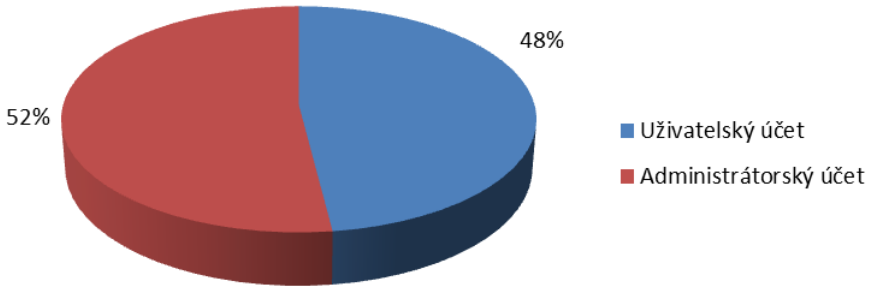
Práce s uživatelskými účty zahrnuje několik bezpečnostních zásad (ty jsou vyjmenované v radách pro zabezpečení). Pokládal jsem otázky na typ běžně používaného účtu, a zda uživatelé používají hesla pro vstup do operačního systému.

4.2.1 Vstup do operačního systému

Při položení otázky, zdali pro přihlášení do uživatelského účtu uživatelé používají heslo, odpovědělo 115 vyplňujících kladně. Téměř 40 % respondentů heslo pro vstup do operačního systému nepoužívá, což je základní bezpečnostní chybou.

4.2.2 Typ účtu

Otázce „Pro běžnou práci používáte:“ byly uživatelům nabídnuty dvě odpovědi – administrátorský účet a uživatelský účet. Z hlediska bezpečnosti odpověděla spatně nadpoloviční většina (52%) tím, že k běžné práci používá administrátorský účet.



Obr. 11. Graf ankety – otázka na typ účtu pro běžnou práci

4.3 Zabezpečení a bezpečnostní funkce

Pod pojmem zabezpečení a bezpečnostní funkce by si uživatelé měli představit software, který jim umožní udržovat počítač ve stavu, který je pro něj vhodný. Tímto mám na mysli stav, kdy je systém chráněný proti všem útočníkům a veškerému škodlivému software. Namátkou jsem vybral tři důležité bezpečnostní prvky – antivirový program, Firewall a Windows Defender (jako ochranu proti spyware). Poté jsem položil otázku, zda se uživatelé zabývají zabezpečením svého systému, a pokud ano, jestli nějakým způsobem testovali jeho zabezpečení. Následující otázky byly na šifrování a zálohu systému.

4.3.1 Antivirový program

V této otázce uživatelé mohli vybrat z předvyplněných antivirů nebo dopsat jejich vlastní, který používají. Chybějící antivirus je zásadní bezpečnostní chybou, které se dopouští 11 vyplňujících. Jako nejvíce používaný antivir zvolilo 55 respondentů Avast!.

4.3.2 Firewall

Otázkou „Brána Firewall poskytuje aktivní ochranu počítače.“ jsem mířil na povědomí o jednom ze základních bezpečnostních prvků. Celkem 57 respondentů odpovědělo špatně a domnívá se, že brána Firewall neposkytuje aktivní ochranu počítače.

4.3.3 Typ Firewallu

Na otevřenou otázku „Firewall používám…“ bylo možně odpovědět několika předvyplněnými odpověďmi, případně mohl vyplňující uvést jiný typ. Celkem 61 % respondentů používá pouze základní Windows Firewall, což je základní minimum. Vhodněji, „Základní + nějaký doplňkový,“ odpovědělo 12 % vyplňujících.

4.3.4 Windows Defender

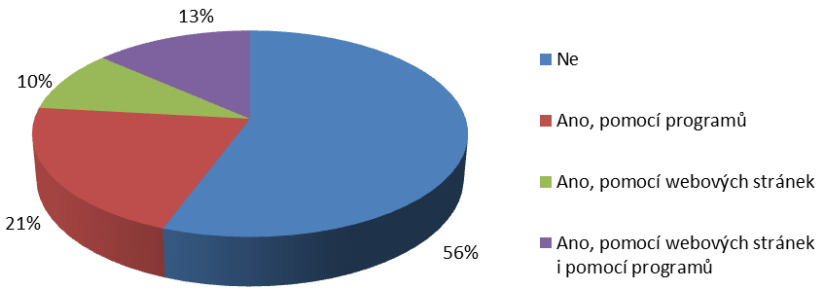
Další otázka na znalost bezpečnostních aplikací zněla: „Aplikace Windows Defender funguje tak, že…“ Respondenti měli doplnit jednu ze tří možností. Správnou odpověď „Prohlíží registry a soubory a v nich hledá signatury podvodných aplikací,“ zvolilo 114 odpovídajících. Špatně na tuto otázku odpovědělo 71 vyplňujících.

4.3.5 Zájem o zabezpečení

Na otázku „Zajímáte se o zabezpečení vašeho systému?“ byly respondentům nabídnuty odpovědi Ano – Ne. Zájem o zabezpečení má 141 respondentů, 44 nikoli - což není z hlediska bezpečnosti vhodné.

4.3.6 Testování bezpečnosti

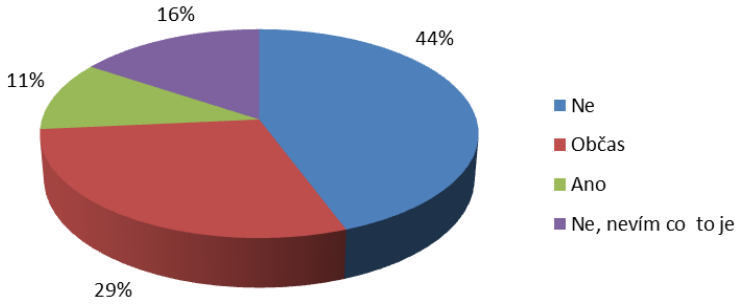
U otázky „Testovali jste někdy zabezpečení vašeho systému?“ odpovědělo záporně 103 respondentů. Z hlediska bezpečnosti 56 % vyplňujících odpovědělo nevhodně.



Obr. 12. Graf ankety – otázka na testování bezpečnosti

4.3.7 Šifrování

„Šifrujete data?“ byla otázka, na kterou šlo vybrat ze čtyř odpovědí. Záporně na tuto otázku odpovědělo 82 vyplňujících. 29 odpovídajících nemá ponětí, co je to šifrování. Na grafu můžeme vidět, jak velké množství vyplňujících neprojevuje zájem o bezpečnost svých dat.



Obr. 13. Graf ankety – otázka na šifrování

4.3.8 Záloha systému

Na otázku, zda uživatelé provádí zálohu systému, jich odpovědělo negativně 31 %. Pouze 14 % respondentů má vhodně nastavenou automatickou zálohu. Z bezpečnostního hlediska splňuje podmínku dobrého zabezpečení pouze těchto 14 respondentů.

4.4 Škodlivý software

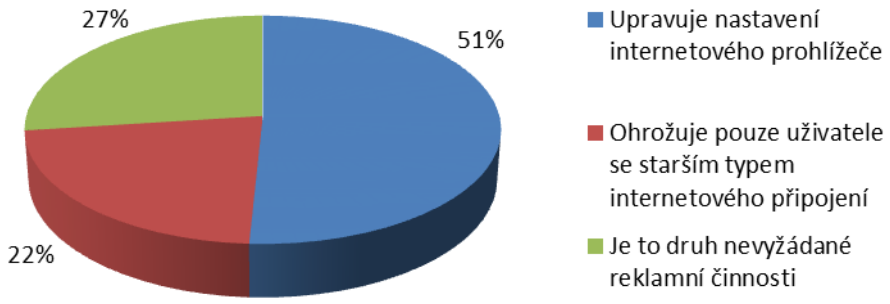
Škodlivému software byla v této práci věnována celá první kapitola. Zajímal jsem se, zda odpovídající znají základní podvodné techniky. Pokládal jsem otázky na viry, trojské koně, Hijacker, Phishing a Spam.

4.4.1 Viry

Na znalostní otázku z problematiky škodlivého software „Viry jsou,“ odpovědělo správně 183 odpovídajících. To poukazuje na základní znalosti téměř všech vyplňujících v této kategorii. Pouze dva odpověděli špatně.

4.4.2 Hijacker

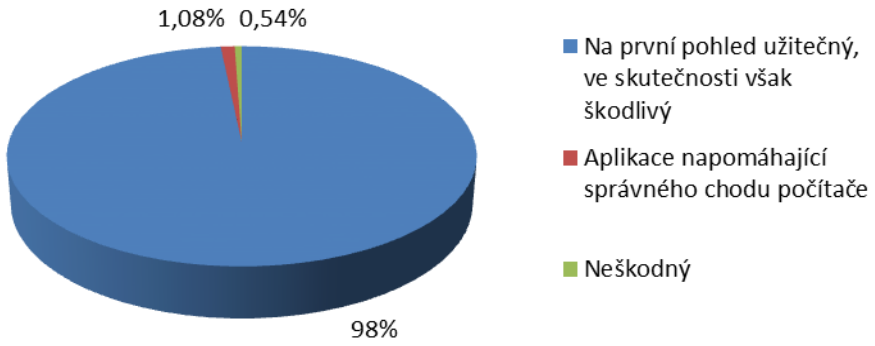
Na otázku, co je to Hijacker, odpovědělo 94 vyplňujících správně. Zbytek, téměř polovina, odpověděla špatně. Z toho vyplývá, že druh tohoto škodlivého software není mezi vyplňujícími až tak známý.



Obr. 14. Graf ankety – otázka na Hijacker

4.4.3 Trojské koně

Správně na otázku „Trojský kůň je…“ odpovědělo 172 respondentů. Z toho vyplývá, že téměř všichni vyplňující mají základní znalost, co je to trojský kůň.



Obr. 15. Graf ankety – otázka na Trojské koně

4.4.4 Phishing

Otázka „Phishing je,“ měla správnou odpověď: „Lákání citlivých dat od uživatelů.“ Takto odpovědělo 140 vyplňujících. Špatně na tuto otázku odpovědělo 45 vyplňujících. Tímto údajem se Phishing řadí mezi druhý nejméně známý škodlivý software (pomyslné první místo drží Hijacker) mezi uživateli vyplňujícími tento dotazník.

4.4.5 Spam

Otázku „Označení spam se používá pro“ špatně vyplnili pouze 4 respondenti. Což mezi uživateli vyplňující tento dotazník dělá Spam poměrně známým softwarem.

5 TESTOVÁNÍ WINDOWS 7

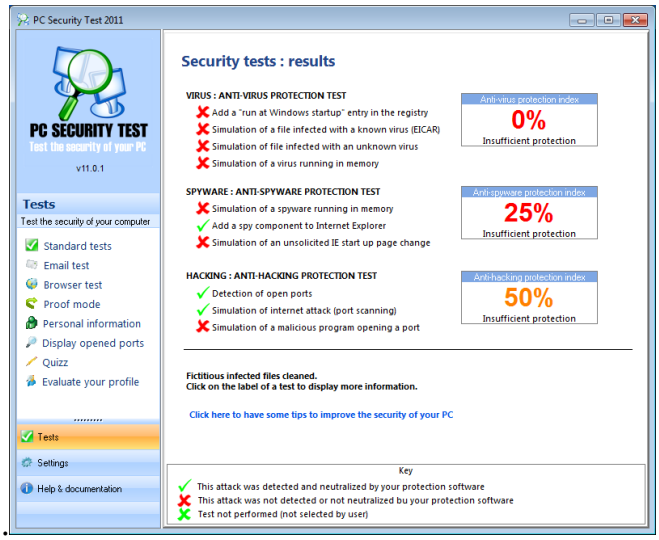
Testování proběhlo na notebooku HP Pavilion dv6000 s instalovaným systémem Windows 7 Home Basic. Při instalaci systému jsem nezapínal automatické aktualizace z důvodu možného stahování update. Připojení k internetu proběhlo u mě doma s použitím Domácího profilu. Před počátkem každého testu jsem vždy zformátoval disk a přeinstaloval systém.

5.1 PC SECURITY TEST 2011

Stažení a nainstalování tohoto programu bylo poměrně rychlé (program má jen něco málo přes 1,5 MB). Tento program zjišťuje zabezpečení počítače proti virům, spyware a hackerským útokům. Pro test hackerských útoků je třeba mít při testu připojený počítač k sítí Internet. Testování probíhá ve čtyřech krocích:

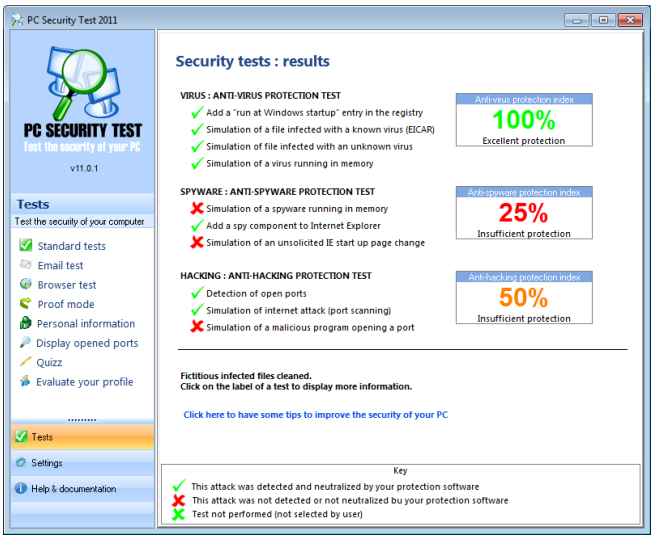
1. Fiktivní útoky - program bude simulovat útoky virů, spyware a hackerů. Nejedná se o skutečné viry, pouze o simulaci. Cílem tohoto kroku je aktivovat bezpečnostní prvky systému a zkontrolovat, zda byly všechny hrozby detekovány a zneškodněny.
2. Reakce systémové ochrany - jakmile je systém infikován, bezpečnostní software (antiviry, anti-spyware, firewall) bude tuto skutečnost alarmovat (tohle je správná reakce bezpečnostního software).
3. Zobrazení výsledků - v tomto kroku PC Security Test spočítá index bezpečnosti a nabídne tipy ke zlepšení bezpečnosti systému.
4. „Čištění“ fiktivních útoků - po dokončení celého procesu testování, PC Security Test odstraní všechny fiktivní infikované soubory.

Po prvním standartním testu jsou výsledky podle očekávání. Antivirový program v počítači není nainstalován, proto dostal patřičné hodnocení 0 %. Ochrana před hackerskými útoky a Windows Firewall obstál na 50 %. Pouze Windows Defender se útokům spyware ubránil jen na 25 %.



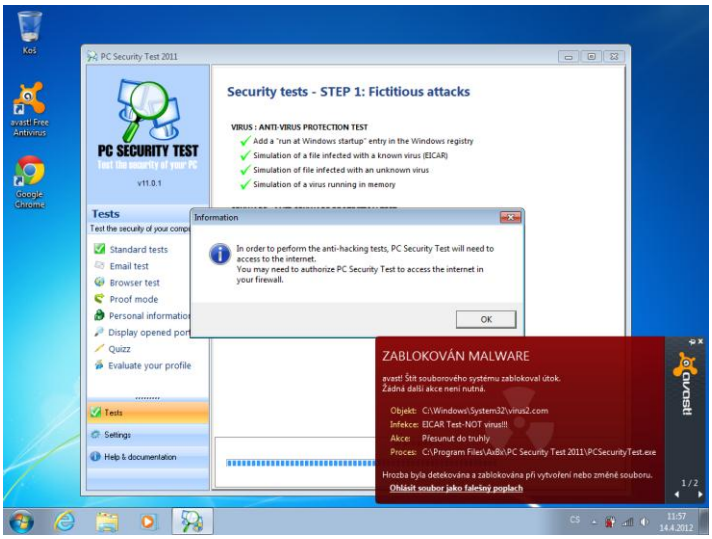
Obr. 16. Výsledky prvního testu

Prvním krokem, který ihned bez jakýchkoli rad programu udělám, je doinstalování antivirového programu. Pro test vyzkouším Avast! Free Antivirus. Výsledky jsou jednoznačné. Avast se svou rezidentní ochranou splňuje podmínky PC Security Testu a dostává patřičné hodnocení 100%.



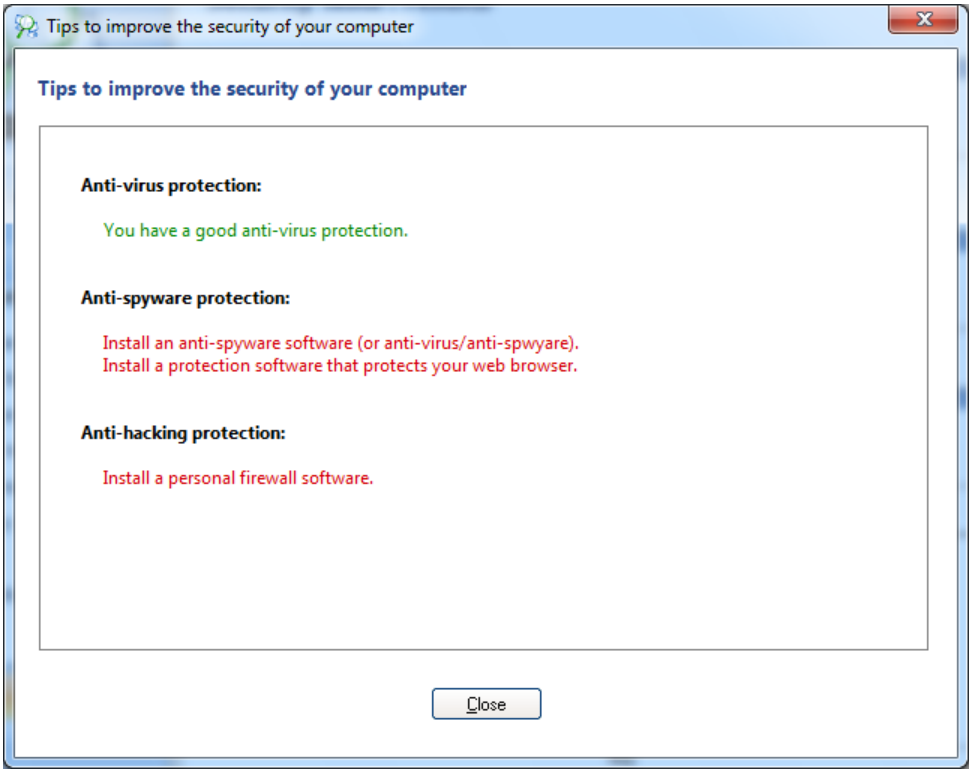
Obr. 17. Výsledky po doinstalování antiviru.

V průběhu testu jsou programem na počítač simulovány útoky škodlivého software. Pozitivní zprávou je, že antivirový program všechny tyto akce zachytí a vyhlásí. Programem je tato akce vyhodnocena kladně – samotný program dává antivirům dvě minuty na zareagování. Pokud tento časový test splní, je vše v pořádku. V opačném případě antivirový program u testu propadá.



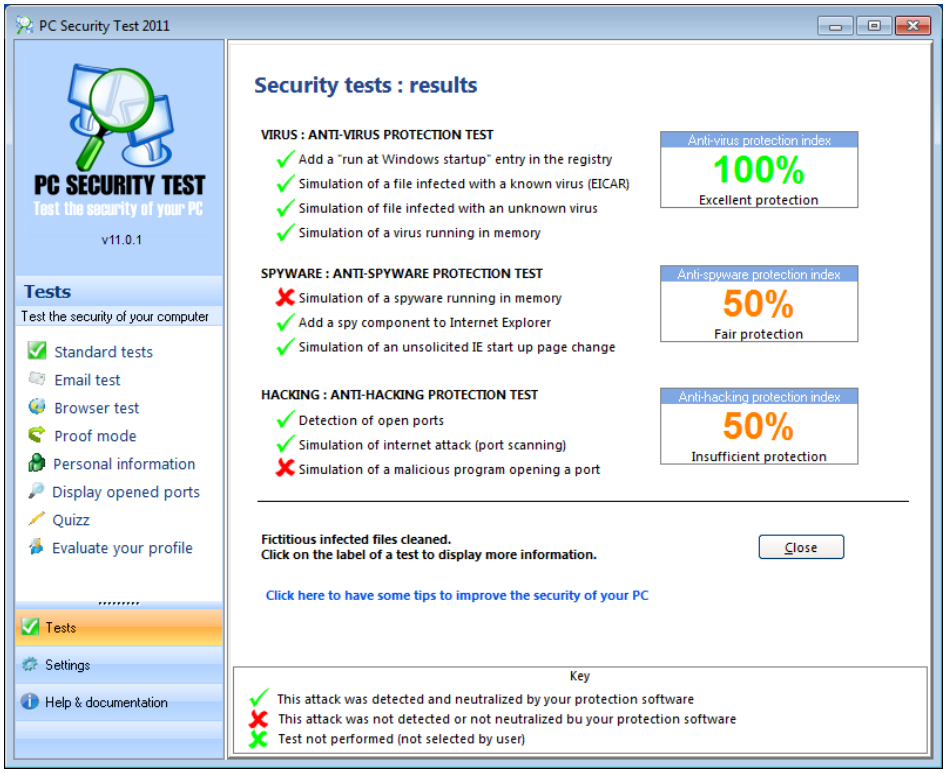
Obr. 18. Průběh testu – zablokován malware.

Nyní se zaměřuji na rady programu. Jak je možné vidět na obrázku níže, program ve svých radách kladně (zeleně) hlásí přítomnost antivirového program. Anti-spyware ochrana značí absenci ochranného anti-spyware software a také ochranný software pro webový prohlížeč (na obrázku značeny červeně). I v poslední části ochrany, ochrana proti hackerským útokům, je jeden nedostatek. Program zde doporučuje doinstalování osobního firewallu.



Obr. 19. Rady k zlepšení bezpečnosti počítače

PC Security Test posílá útoky typu Hijacker a prostřednictvím nich se snaží změnit domovskou stránku internetového prohlížeče. Program dává na výběr z několika typů používaných prohlížečů, které v průběhu testu ověřuje. Mozilla Firefox a jemu podobné prohlížeče nebyly napadeny, ovšem Internet Explorer, základní prohlížeč od Microsoftu, neuspěl. Ani nejnovější „devátá“ verze tohoto programu. Problém s absencí ochranného software pro prohlížeč řeším instalací programu **Anti-Hijacker**, po kterém bylo opětovné testování se znatelně lepšími výsledky. Anti-Hijacker je dostupný z: http://www.slunecnice.cz/sw/anti-hijacker/.



Obr. 20. Vyhodnocení po testu s programem Anti-Hijacker

V této chvíli program doporučuje doinstalovat ochranu proti spyware a osobní firewall. Jako ochranu proti útokům hackerů jsem vybral program Comodo Firewall dostupný z: http://personalfirewall.comodo.com/. Ochranu proti spyware jsem vybral Spyware Terminator 2012 dostupný z: http://www.pcrx.com/cs/spywareterminator/default.aspx.

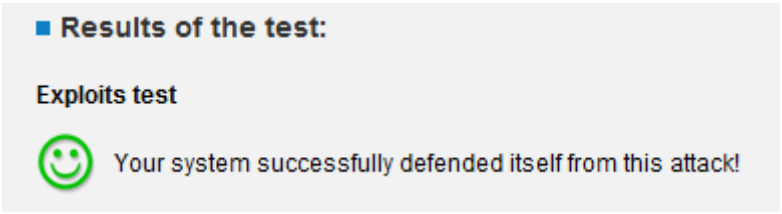
Po kompletní instalaci jsem znovu spustil test. Bohužel, výsledek byl stále stejný jako na obrázku 22. Zkoušel jsem i jiné alternativy firewallu (Outpost Firewall, ZoneAlarm, Sunbelt Personal Firewall) a Antispyware (Spyware Doctor, Security Scanner, Spybot), ale ani v jednom případě se výsledek nezměnil. Tímto jsem ukončil PC Security Test a v následujících testech jsem se zaměřil jednotlivě na antispyware a firewall.

5.2 Testování Firewallu

Vzhledem k výsledkům PC Security Testu budu nyní zkoumat bezpečnost Windows Firewallu. Zaměřím se na testování pomocí exploitů, které jsou dostupné na stránce: http://www.pcflank.com/ a pomocí programu LeakTest dostupného na: http://www.grc.com/lt/leaktest.htm.

5.2.1 Exploity

Jak už bylo zmíněno v teoretické části, exploity jsou kódy zaměřené na určitou zranitelnost. Na výše zmíněné stránce je k dispozici několik těchto kódů, pomocí nichž lze otestovat jejich možný průnik do počítače. Žádný z nich není primárně určen pro Windows 7 (ale pro starší typy Windows), proto je předpokládán kladný výsledek. Po vybrání všech dostupných exploitačních kódu a spuštění testu byl zobrazen očekávaný výsledek – systém se úspěšně ubránil těmto útokům.



Obr. 21. Výstřižek po testu na pcflank.con

5.2.2 LeakTest

Exploity testovaly průnik do systému. Pomocí LeakTestu jsem provedl kontrolu opačného směru. Tento test simuluje pokus o spojení do sítě Internet bez vědomí uživatele. Nejprve jsem otestoval Windows Firewall, který v tomto testu neobstál.

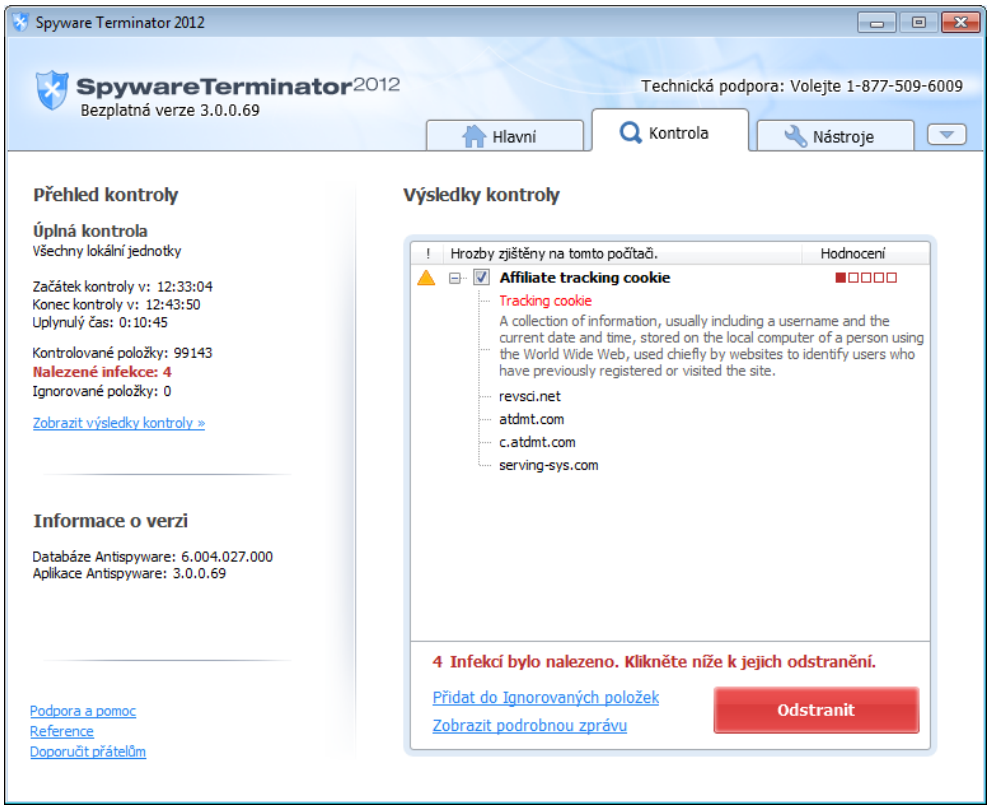
Obr. 22. LeakTest

Z tohoto důvodu jsem nainstaloval Comodo Firewall, který úspěšně vyřešil tento problém. Při spuštění testu upozornil na pokus o odchozí spojení souboru leaktest.exe, který jsem zamítnul. Tím pádem test nemohl odeslat svá data do sítě Internet, což znamenalo vypsání upozornění o nemožnosti připojení se k Internetu, což v této situaci znamená kladný výsledek.

Obr. 23. Úspěšný LeakTest

5.3 Spyware

Zdali čistě nainstalovaný systém obsahuje tento škodlivý software, bylo zkoumáno za pomoci antispyware programu Spyware Terminator. Jakmile jsem tento program stáhnul a nainstaloval, provedl jsem úplnou kontrolu systému. Přestože byl systém nainstalován jen zhruba hodinu, obsahoval již bezpečnostní prvky, jako je implementovaná ochrana proti spyware Windows Defender, a Windows Firewall, vyhodnotil program 4 infekce. To mohlo být následkem stahování tohoto programu z Internetu. Spyware Terminator tyto infekce v dalším kroku odstranil. Je vhodné, aby antispyware program pracoval jako rezidentní štít.



Obr. 24. Spyware Terminator – nalezené infekce

5.4 Internetové online scannery

Existuje celá řada online scannerů, které online kontrolují stav operačního systému a slouží jako scannery infikovaných souborů. Tyto testy vytváří převážně výrobci antivirových programů a téměř všechny testy končí závěrečným doporučením sdělujícím potřebu doinstalovat právě jejich antivirus, což může působit nevěrohodně. Jako příkladem těchto testů uvádím ESET Online Scanner, jehož cílem bylo zjistit, zda systém po jeho instalaci tyto sobory neobsahuje. Je dostupný z: http://www.eset.com/cz/domacnosti/produkty/online-scanner/. Před spuštěním je potřeba odsouhlasit podmínky pro používání od společnosti ESET. Pro testování online je zapotřebí stránku spustit v Internet Exploreru. V případě použití jiného prohlížeče stránka zobrazí ke stažení ESET Smart Installer (aplikaci, která nainstaluje a spustí tento scanner) a pomocí něj lze test provést i v jiném prohlížeči.

V prvním kroku lze nastavit parametry kontroly. Test umožňuje odstranit infikované soubory a zvládá kontrolovat archivy. V rozšířených možnostech detekuje potenciálně nechtěné a nebezpečné aplikace. Využívá také technologie Anti-Stealt, která umožní

detekci aktivních rootkitů v operační paměti. V tomto kroku program také zjistil přítomnost bezpečnostního software, kterým byl Windows Defender. Druhým krokem testu program aktualizuje virovou databázi. V případě prvního spuštění tato akce trvá několik minut, v závislosti na rychlosti internetového připojení. V případě opětovného spuštění testu se pouze kontrolují virové databáze a případně se aktualizují na novější verzi. Třetí krok je samotná kontrola disků, ve kterých Scanner hledá infikované soubory. Posledním, čtvrtým krokem, jsou výsledky kontroly. Program nenalezl žádné infikované soubory a jeho doporučením bylo nainstalovat ESET Smart Security nebo ESET NOD32 Antivirus. Toto doporučení, dle mého názoru, je spíše reklamním tahem než skutečným poznatkem a to z důvodu, že tento online test nekontroluje kvalitu instalovaných bezpečnostních prvků, nýbrž pouze kontroluje, zda se v systému nenachází infikované soubory.

Obr. 25. Doporučení ESET Online Scanner

5.5 Doporučené programy

Součástí dobře zabezpečeného operačního systému jsou doinstalované bezpečnostní programy, bez kterých by ochrana nebylo kompletní. Některé tyto programy již Windows 7 obsahují, nicméně pro kvalitnější zabezpečení doporučuji používat následující freeware programy:

Antivirový program: Avast! Free Antivirus (verze 7.0.1426; velikost 71,3 MB)

Antispyware program: Spyware Terminator (verze 3.0.0.69; velikost 11,32 MB)

Firewall: Comodo Firewall (verze 5.5.195786.1383; velikost 60,72 MB)

Ochrana prohlížeče: McAfee SiteAdvisor (verze 2.9; velikost 3,09 MB)

Ochrana prohlížeče proti Phishingu: Netcraft Anti-Phishing Toolbar (verze 1.5.6, velikost 2,78 MB)

Zde bych chtěl podotknout, že tyto programy se každou chvíli mění v závislosti na nejnovějších hrozbách. V okamžiku kdy píši tuto práci, jsou na špičkové úrovni, ale za pár měsíců tomu tak být nemusí. Proto doporučuji sledovat stránky, které se touto problematikou zabývají. Mohu uvést dvě webové stránky:

- http://www.av-comparatives.org/ - zabývá různými testy, převážně antivirů,
- http://www.matousec.com/ - zabývá se prostupností do operačních systémů.

ZÁVĚR

Zjištění bezpečnosti operačního systému je tou nejdůležitější skutečností v oblasti informační technologie dnešní doby. Je tomu tak důsledkem rozvíjející se celosvětové síti Internet a nárůstu počtu jeho uživatelů. Tyto uživatele spojuje potřeba hledat na této síti informace, pracovat, bavit se a vzájemně komunikovat. Při této činnosti se mohou, ať už vědomě nebo ne, dostat na nebezpečné či podvržené webové stránky. V jejich zájmu by mělo být tyto stránky rozpoznat a nejen zabezpečit sebe (své osobní údaje), ale také zabezpečit svůj operační systém, a především svá data.

Microsoft přišel na trh roku 1981 se svým prvním operačním systémem MS-DOS, práce s tímto systémem však nebyla jednoduchá – uživatel musel znát speciální jazyk pro zadávání příkazů. Do kategorie jeho významných systémů dále patří výkonnější a graficky propracovanější Windows 3.0 a verze Windows 95, která se začíná vzhledově přibližovat dnešním moderním systémům. Nejbližšími předchůdci systému Windows 7 byli Windows XP a Windows Vista. Ty jsou v práci zmíněny podrobněji i z hlediska jejich bezpečnosti.

Významným zjištěním bylo, že Windows 7 ještě není nejpoužívanějším systémem. Je jím stále Windows XP, jehož podíl na trhu však pomalu klesá díky Windows 7. Osobně očekávám významný pokles pro XP až po roce 2014, kdy má skončit jejich oficiální technická podpora aktualizací zabezpečení a uživatelé tak budou muset přejít na vyšší systém. Může se stát, že tito uživatelé však Windows 7 přeskočí a své počítače osadí, v té době již oficiálně vydanou, verzí Windows 8 (případně novější).

Windows 7 je na poměrně dobré bezpečnostní úrovni (ve srovnání s jeho předchůdci), převážně díky vylepšené bráně firewall a antispyware programu Windows Defender. Tuto skutečnost jsem testoval. Překvapením pro mě bylo zjištění, že i přes vylepšení brány firewall (oproti předchozím verzím), ji pořád nelze dobře nakonfigurovat, aby zabránila neoprávněným akcím. K úspěšným testům jsem ji musel nahradit Comodo Firewallem.

Při analýze veřejného dotazníku zabývající se povědomím uživatelů o zabezpečení, bylo nemilým zjištěním, že uživatelé dělají stále stejné bezpečnostní chyby, jako jsou používání k běžné práci administrátorské účty, vstup do systému neošetřen heslem apod.

K tomu, aby byl Windows 7 dokonale izolován od škodlivého software vyskytujícího se na Internetu, je zapotřebí nespoléhat se pouze na jeho základní zabezpečení, ale je potřeba doinstalovat některé bezpečnostní programy. Ty uvádím v posledních kapitolách práce.

ZÁVĚR V ANGLIČTINĚ

Security of an operating system is the most important in the field of a recent information technology. It is a result of worldwide Internet network development and of an increase in the number of users. There is a common need of users to communicate, work, have fun and search for information. These activities might lead to visiting some dangerous or counterfeit websites. Users should be interested in their computer and datas protection.

Microsoft corporation developed its first operating system MS-DOS in 1981. However, working with this system was not easy because users had to know a special language to issue a command. Version Windows 3.0 and Windows 95 were the next successful and more efficient systems. Windows 95 seems to be more similar to modern systems. The closest Windows 7 predecessors were Windows XP and Windows Vista, security of these is mentioned in this work.

Significant finding is that Windows 7 has not been the most used system yet. Windows XP is still in this position, but Windows 7 marketability index has increased. In my opinion, there will be visible decrease of using Windows XP after year 2014. By that time Windows XP official technical support of protection update will end. Therefore, its users will have to start using a higher level system. What might happen is that these users will miss Windows 7 and start using Windows 8 version (or a newer version).

There is quite a good security level of Windows 7, according to a comparison to predessors one. The reason is that Firewall System and antispyware programme Widows Defender have improved. I have tested that. I had not expected, even with the improvement of Firewall System, that it is still not easy to configure it well enough to prevent from unauthorized actions. To achieve successful results, I had to substitute Firewall System for Comodo Firewall.

Evaluation a public questionnaire leads to a fact, that users still make mistakes when they try to protect their system and datas. They use their administrator accounts for any work, no password to access the system etc.

If Windows 7 was supposed to be absolutely insulated from damaging software, appeared on the Internet network, it would be necessary to rely on more than one basic protection and to install some protection programmes. Those are mentioned in last chapters of this work.

SEZNAM POUŽITÉ LITERATURY

[1] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[2] SZOR, Peter. *Počítačové viry: analýza útoku a obrana.* Vyd. 1. Brno: Zoner Press, 2006, 608 s. ISBN 80-868-1504-8.

[3] POLZER, Jan. Česká spořitelna a phishing – kdy už to skončí?. *Maxiorel.cz | software/ weby/ programování* [online]. 12.3.2008 [cit. 2012-05-10]. Dostupné z: http://www.maxiorel.cz/ceska-sporitelna-phishing-kdy-uz-skonci

[4] Trojské koně: co jsou zač a jak se bránit. *O počítačích, IT a internetu - Živě.cz* [online]. 30.3.2005 [cit. 2012-03-25]. Dostupné z: http://www.zive.cz/clanky/trojske-kone-co-jsou-zac-a-jak-se-branit/sc-3-a-123708/default.aspx

[5] Denial of Service (DoS), Distributed DoS (DDoS). *AdminXP.cz: Průvodce pro začátečníky a administrátory. Tipy, triky, návody, odpovědi a odkazy.* [online]. © 2000-2012 [cit. 2012-03-25]. Dostupné z: http://www.adminxp.cz/security/index.php?aid=193

[6] HEGER, Adam. Botnet - vir současnosti. *EMag.cz - Technologický magazín* [online]. 27.2.2007 [cit. 2012-03-25]. Dostupné z: http://www.emag.cz/botnet-vir-soucasnosti/

[7] MIKULEC, Martin. Bezpečnost v síti (4.díl), síťové útoky. *Owebu.cz , webhosting , domény , hosting* [online]. 29. 4. 2009 [cit. 2012-04-30]. Dostupné z: http://owebu.bloger.cz/PC-site/Bezpecnost-v-siti-4-dil-sitove-utoky

[8] MINASI, Mark. *Windows XP Professional.* 1. vyd. Praha: Grada, 2002, 800 s. Profesional. ISBN 80-247-0326-2.

[9] BOTT, Ed. Mistrovství v Microsoft Windows XP: Windows XP do nejmenších podrobností a do posledního detailu. 2. vyd. Brno: Computer Press, 2003, 608 s. ISBN 80-722-6980-1.

[10] Aktualizace Windows XP Service Pack 2, balíček pro síťovou instalaci určený odborníkům a vývojářům z oblasti IT. *Microsoft Download Center* [online]. 5.9.2004 [cit. 2012-03-12]. Dostupné z: http://www.microsoft.com/downloads/cs-cz/details.aspx?FamilyID=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A

[11] Historie systému Windows. *Microsoft Windows* [online]. © 2012 [cit. 2012-02-28]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows/history

[12] Zabezpečení a bezpečnost. *Microsoft Windows* [online]. © 2012 [cit. 2012-03-13]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows-vista/products/features/security-safety

[13] Co je součástí aktualizace Service Pack 1 (SP1) systému Windows Vista. *Microsoft Windows* [online]. © 2012 [cit. 2012-03-13]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows-vista/Whats-included-in-Windows-Vista-Service-Pack-1-SP1

[14] Součásti aktualizace Windows Vista Service Pack 2 (SP2). *Microsoft Windows* [online]. © 2012 [cit. 2012-03-13]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows-vista/Whats-included-in-Windows-Vista-Service-Pack-2-SP2

[15] Operating systems » gemiusRanking CZ — english version. *GemiusRanking CZ — english version* [online]. © 2000 - 2012 [cit. 2012-04-05]. Dostupné z: http://www.rankings.cz/en/rankings/operating-systems.html

[16] SINCHAK, Steve. *Windows 7: průvodce pro nové uživatele.* Vyd. 1. Brno: Zoner Press, 2010, 375 s. Encyklopedie Zoner Press. ISBN 978-807-4130-830.

[17] KUČERA, Roman a Petr BROŽA. *Bible Windows 7*. Brno: Extra Publishing, c2009, 288 s. ISBN 978-807-4130-618

[18] Co je Správce pověření?. *Microsoft Windows* [online]. © 2012 [cit. 2012-05-01]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows7/What-is-Credential-Manager

[19] Windows 8 dostanou nové bezpečnostní funkce. *Computerworld.cz | Deník pro IT profesionály* [online]. 20.09.2011 [cit. 2012-05-01]. Dostupné z: http://computerworld.cz/software/windows-8-dostanou-nove-bezpecnostni-funkce-43845

[20] Informace o produktu Microsoft Security Essentials. *Microsoft Windows* [online]. © 2012 [cit. 2012-03-13]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows/products/security-essentials/product-information

[21] Setting a BIOS Password. *Lockdown.co.uk - The Home Computer Security Center* [online]. 10.7.2009 [cit. 2012-04-04]. Dostupné z: http://www.lockdown.co.uk/?pg=biospsw

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VEŘEJNÝ DOTAZNÍK

1. Jaký používáte operační systém?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Procenta
Windows 7	128	69,19%
Windows XP	21	11,35%
Windows Vista	19	10,27%
Linux	7	3,78%
MacOS X	3	1,62%
Win 7 + Ubuntu	1	0,54%
Win2000, XP, 7 i Linux	1	0,54%
Windows XP + Vista + 7	1	0,54%
7 a Vista	1	0,54%
UNIX based	1	0,54%
Windows 7, Vývojářskou verzi Windows 8	1	0,54%
Windows 8 preview	1	0,54%

2. Používáte při vstupu do svého uživatelského účtu heslo?

Povinná otázka, respondent se musel rozhodnout mezi odpověďmi „ano" a „ne".

Odpověď	Počet	Procenta
Ano	115	62,16%
Ne	70	37,84%

3. Pro běžnou práci používáte:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Administrátorský účet	52	52,00%
Uživatelský účet	48	48,00%

4. Jak často měníte heslo?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Heslo neměním	135	72,97%
1x za rok	24	12,97%
1x za půl roku	22	11,89%

1x za měsíc	4	2,16%

5. Nejsilnější heslo je:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
mlw51//Uy	179	96,76%
martin55	6	3,24%
123456	0	0,00%

6. Jak vytváříte hesla?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Procenta
Náhodně	42	42,00%
Podle určitých pravidel	33	33,00%
Ze svých osobních údajů	17	17,00%
Pomocí generátorů	4	4,00%
Slovo, které má pro mě	1	1,00%

7. Ukládáte v prohlížečích vaše hesla?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Jen někde	84	45,41%
Ne, nikde	46	24,86%
Většinou ano	44	23,78%
Ano, vždy	11	5,95%

8. Šifrujete data?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Ne	82	44,32%
Občas	54	29,19%
Ne, nevím co to je	29	15,68%
Ano	20	10,81%

9. Brána Firewall poskytuje aktivní ochranu počítače:

Povinná otázka, respondent se musel rozhodnout mezi odpověďmi „ano" a „ne".

Odpověď	Počet	Procenta
Ano	128	69,19%
Ne	57	30,81%

10. Firewall používám:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Procenta
Základní Windows Firewall	61	61,00%
Základní + nějaký	12	12,00%
Comodo Firewall	5	5,00%
nevím	3	3,00%
AVG	2	2,00%
žádný	2	2,00%
Eset smart security	2	2,00%
Sunbelt Personal Firewall	2	2,00%
nod internet sec.	1	1,00%
Zone Alarm	2	2,00%
avast	1	1,00%
ESET	1	1,00%
Linux	1	1,00%
Little Snitch	1	1,00%
vzhledem k povaze systému Mac využívám standartní	1	1,00%
základní a jediný linuxový firewall	1	1,00%
součást AVG	1	1,00%
Firewall integrovaný v antivirovém programu od firmy ESET	1	1,00%

11. Jaký používáte antivirový program?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.

Odpověď	Počet	Procenta
Avast!	55	29,7%
NOD32	41	22,2%
AVG	25	13,5%

Microsoft Security Essentials	24	13,0%
Žádný	14	7,6%
Avira	5	2,7%
Norton AntiVirus	5	2,7%
Různé	3	1,62%
Eset	3	1,62%
F-Secure profi antivirus	2	1,08%
Zone Alarm	1	0,54%
nevím	1	0,54%
ESET Smart Security	1	0,54%
Fsource	1	0,54%
Avast a AVG	1	0,54%
GFI Vipre	1	0,54%
COMODO	1	0,54%
Kaspersky	1	0,54%

12. Zajímáte se o zabezpečení vašeho systému?

Povinná otázka, respondent se musel rozhodnout mezi odpověďmi „ano" a „ne".

Odpověď	**Počet**	**Procenta**
Ano	141	76,22%
Ne	44	23,78%

13. Testovali jste někdy zabezpečení vašeho systému?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	**Počet**	**Procenta**
Ne	103	55,68%
Ano, pomocí programů	39	21,08%
Ano, pomocí webových stránek i pomocí programů	25	13,51%
Ano, pomocí webových stránek	18	9,73%

14. Aplikace Windows Defender funguje tak, že…:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Prohlíží registry a soubory a v nich hledá signatury podvodných aplikací	114	61,62%
Zablokuje všechny porty počítače vůči virům a útokům z internetu	47	25,41%
Zašifruje soubory a spustí antivirus, který v nich hledá viry	24	12,97%

15. Viry jsou:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Škodlivý software	183	98,92%
Programy pro počítač	1	0,54%
Nezbytné pro chod počítače	1	0,54%

16. Trojský kůň je:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Na první pohled užitečný, ve skutečnosti však škodlivý	182	98,38%
Aplikace napomáhající správného chodu počítače	2	1,08%
Neškodný	1	0,54%

17. Hijacker:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Upravuje nastavení internetového prohlížeče	94	50,81%
Ohrožuje pouze uživatele se starším typem internetového připojení	51	27,57%
Je to druh nevyžádané reklamní činnosti	40	21,62%

18. Phishing je:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Lákání citlivých dat od uživatelů	140	75,68%
Zaznamenávání všech úhozů do klávesnice	29	15,68%
Nevyžádaná zpráva	16	8,65%

19. Označení spam se používá pro:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Nevyžádanou (reklamní) poštu	180	97,30%
Všechnu příchozí i odchozí poštu	4	2,16%
Duplicitně příchozí emaily	1	0,54%

20. Zálohu systému:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Provádím náhodně sám/sama	55	55,00%
Neprovádím	31	31,00%
Mám nastavenou automaticky	14	14,00%

21. Rozdělení diskového prostoru:

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Procenta
Mám dva oddíly, jeden pro systém, druhý pro data	50	50,00%
Mám více oddílů	26	26,00%
Mám pouze jeden oddíl	19	19,00%
Co to je?	5	5,00%