Jak správně zabezpečit systém Windows

How to set up correctly security settings of Microsoft Windows

Roman Talaš

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Roman TALAŠ**
Osobní číslo:	**A08380**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Jak správně zabezpečit systém Windows**

Zásady pro vypracování:

1. **Sestavte literární rešerši na téma zabezpečení systému Microsoft Windows a tzv. sociálního inženýrství.**
2. **Formulujte bezpečnostní rizika, se kterými se musí uživatel potýkat po instalaci Windows a uveďte dostupné prostředky pro obranu před těmito riziky.**
3. **Sestavte a realizujte veřejnou anketu pro zjištění podvědomí veřejnosti o bezpečnostních rizicích systému Windows.**
4. **V praktické části sestavte návod, jak postupovat při instalaci Windows a co provézt po instalaci holého systému.**
5. **Výstupem práce budou také obecné rady, jak se bránit sociálního inženýrství.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BITTO, Ondřej. Jak zabezpečit domácí a malou síť Windows XP : Účty, práva, firewally, antiviry a další nástroje . 1.vydání. Praha : Computer Press, 2006. 216 s. ISBN 80-251-1098-2.
2. SMITH, Ben; KOMAR, Brian; MICROSOFT SECURITY TEAM. Zabezpečení systému a sítě Microsoft Windows. Praha : Computer Press, 2007. 700 s. ISBN 80-251-1260-8.
3. BOTT, Ed; SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Praha : Computer Press, 2004. 696 s. ISBN 80-722-6878-3.
4. SOSINSKY, Barrie. Mistrovství - počítačové sítě : [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.
5. LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.
6. THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.

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

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

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

V práci je nejprve v úvodu teoretické části ukázán současný pohled dnešního světa na počítačovou bezpečnost a uvedeny hlavní důvody, které nás nutí mít náš počítač dobře zabezpečený. Dále je uveden postupný vývoj operačních systémů Microsoft Windows, s následným porovnáním jednotlivých verzí systémů. Následuje podrobná kapitola, která se věnuje všem bezpečnostním hrozbám, kterými by se měl běžný uživatel zabývat. Teoretickou část zakončuje představení nástrojů, které nám slouží k zabezpečení Windows 7. Dále je zde vypracována veřejná anketa, která pomohla ukázat pohled širší veřejnosti na tuto problematiku, z jejichž výsledků vznikly podněty, jakými směry by se práce měla ubírat více a jakými méně. Praktické část je krok po kroku věnována jednotlivým nastavením bezpečnosti, které by v celku měly dát dostatečně zabezpečený počítač s operačním systémem Windows 7.

Klíčová slova:

Počítač, operační systém, Windows, bezpečnost, nastavení, sociální inženýrství.

ABSTRACT

In the introduction of the theoretical part of the work there is at first presented current view of computer safety of today's world and there are stated main reasons that force us to have our computer well secured. Furthermore there is introduced gradual evolution of operating systems Microsoft Windows with consequential comparison of particular versions of the system. Following detailed chapter is attended to all security threats that each common user should consider. The theoretical part is concluded by an introduction of instruments for securing Windows 7. Then there is elaborated a public inquiry that helped to show general public's view of these questions and its results gave suggestions to which directions the work should follow more than the others. Practical part is step by step addressed to particular security set-ups that should altogether result in sufficiently secured computer with the operating system Windows 7.

Keywords:

Computer, operating system, Windows, security, settings, social engineering.

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Jiřímu Vojtěškovi, Ph.D. za jeho cenné připomínky, rady, pomoc a čas, který mi věnoval.

Dále bych chtěl poděkovat svému kamarádovi Dušanovi Machů za pomoc s přeložením abstraktu a závěru do angličtiny.

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

Tématem bakalářské práce je zabezpečení operačního systému Windows. Vzhledem k jejich rozšířenosti a mnoha edicím by samozřejmě nebylo možné se na tak malém prostoru věnovat všem a ještě k tomu alespoň trochu podrobně. Z tohoto důvodu je práce zúžena na nejnovější systémy. Operační systém Windows Vista je vynechán z důvodu jednak z malé rozšířenosti, ale hlavně vzhledem k mnoha nedostatkům, které přiznala i samotná vyvíjející firma Microsoft. Veškerý prostor je tedy věnován pouze systémům Windows XP a Windows 7. Systémy jsou si z bezpečnostního hlediska dosti podobné, tudíž základem práce je Windows 7 a k tomu jsou zmíněny případné větší rozdíly, které má systém Windows XP. Windows 7 byl zvolen z důvodu, že se jedná o nejnovější verzi systému a snad o nejrychleji se prodávající operační systém v historii firmy Microsoft. Dále je jen otázkou času, kdy se stane jedničkou na trhu a bylo by tak trochu zbytečné, věnovat se 10 let starému, byť stále nejpoužívanějšímu, systému XP.

Vzhledem k neustále rostoucímu počtu počítačů, jejich pronikání prakticky do každého oboru a stále se zvyšujícím počtem lidí připojených do sítě Internet, je otázka počítačové bezpečnosti čím dál více aktuálnější a důležitější. S počtem uživatelů se samozřejmě zvyšuje i počet různých hrozeb a nebezpečí. Když se k tomu připočte fakt, že operační systémy Windows jsou suverénně nejpoužívanější, vychází z toho, že se jedná o zajímavý námět na bakalářskou práci.

Toto téma jsem si zvolil, protože mě tato problematika zajímá a mám k ní kladný vztah. Sám jsem spokojeným uživatelem systému Windows 7 a zatím jsem nikdy žádný problém s bezpečností neměl a myslím si, že dokážu počítač s operačním systémem Windows dobře zabezpečit. Ve svém volném čase se snažím sledovat novinky v oblasti bezpečnosti operačních systémů a podle toho se následně i starat o svůj počítač.

Cílem této bakalářské práce je přiblížit problematiku počítačové bezpečnosti širší veřejnosti, ukázat její hrozby a možnosti obrany. Snahou bylo navrhnout jednu z mnoha možných cest, jak si zabezpečit počítač s operačním systémem Windows. Výsledná cesta byla volena tak, aby si systém mohli jednoduše zabezpečit i ne úplně zkušení uživatelé.

I. TEORETICKÁ ČÁST

1 SHRNUTÍ STAVU POČÍTAČOVÉ BEZPEČNOSTI

Hlavní zdroj všech hrozeb a rizik pro dnešní počítače se nachází v celosvětové síti Internet, která vznikla již na začátku 70. let, tehdy ještě se jménem Arpanet. V té době samozřejmě nebylo k Internetu ještě připojeno tolik uživatelů po celém světě jako dnes, od čehož se odvíjelo i množství možných bezpečnostních hrozeb. V samotných začátcích sítě Internet k ní bylo připojeno pouhých 50 počítačů, které z většinové části byli armádní, nebo patřily nějakým jiným obdobným institucím. Možnost používat počítače připojené k Internetu tedy měli většinou pouze proškolení a pověření lidé. Internet ovšem nezůstal čistě armádním projektem a během několika let se rozšířil mezi univerzity či akademická pracoviště. Stále ovšem nebyl dostupný široké veřejnosti jako v dnešní době, byl používán pouze pro akademické či vědecké účely a 3/4 veškeré internetové komunikace tvořila e-mailová pošta. Podle očekávání se brzy objevily první bezpečnostní problémy. V roce 1980 se poprvé objevil virus, který zapříčinil pád celé sítě Internet. O rok později byla nabourána velká americká telekomunikační firma AT&T a v jejím systému bylo pozměněno účtování hovorů z denního tarifu na noční a naopak. Roku 1988 byl vytvořen první internetový červ, který napadl větší část počítačů. Konkrétně se tehdy jednalo o celých 10 % všech světových počítačů. Poté se objevily jména jako Kevin Mittnick, Vladimir Levin nebo Tsumota Shimomura, které je jistě netřeba představovat lidem, zajímající se o počítačovou bezpečnost. Stále se však jednalo o počátky počítačové kriminality a terčem útoků byly především velké firmy. To se začalo postupně měnit od začátku 90. let, kdy síť Internet začal pronikat mezi širší veřejnost. Počítače se stávaly čím dál více výkonnější, propracovanější, propojenější a hlavně rozšířenější. To zákonitě muselo vést k tomu, že se staly taky více zranitelné. [1]

V polovině 90. let, to znamená ještě v době, kdy byl Internet stále ještě ve svém raném stádiu svého rozšíření, bylo autoritami v oblasti počítačové bezpečnosti ohlášeno nalezení 171 vážných zranitelných míst v nejčastěji používaných operačních systémech a aplikacích. Na začátku minulého desetiletí v roce 2001 už byl tento počet navýšen na více než 2500. Ani nejsou třeba žádná vyjádření odborníků na to, aby každému bylo jasné, že počet zranitelných míst bude vzhledem k rozšiřující se složitosti jednotlivých aplikací, systémů, a taky jejich množství, nadále prudce vzrůstat. Statistická čísla by toto jen a jen potvrdily. Bezpečnostní hrozby existují samozřejmě pro všechny systémy či hardwarové platformy a nejen pro uživatele systémů Windows. Ale vzhledem k tomu, že jde jednoznačně o světově

nejpoužívanější operační systém, tak se logicky jedná o nejatraktivnější cíl pro útočníky a díky jeho struktuře asi i cílem nejjednodušším. Tučné titulky o destruktivních a rychle se šířích hrozbách můžeme pravidelně nacházet ve zpravodajství určených pro širší veřejnost. Sem se ovšem dostanou jenom ty nejhorší hrozby a je tudíž potřeba si uvědomit, že na každou takovou hrozbu můžou připadat stovky či tisíce menších, ale stále velmi nebezpečných hrozeb.[2]

S tím, jak se pro nás počítače stávají důležitou součástí a zasahují prakticky do každé lidské činnosti, vzrůstá i množství možných škod, které nám můžou viry, nastražené webové stránky nebo elektroničtí zloději způsobit. V případě úspěšného útoku můžeme přijít o naše soubory v počítači nebo o peníze uložené na našem bankovním účtu, můžou být naším jménem posílány podvržené e-mailové zprávy nebo jenom vykonávány útoky na jiné počítače z toho našeho.

O jak velké částky se může jednat, to si lze názorně ukázat na jednom příkladu. Internetový červ Code Red, který řádil již v roce 2001, infikoval stovky tisíc počítačů. Později se na světlo světa dostal údaj, který udává, že přímé náklady na odstranění červa a návrat napadených systému do normálního stavu dosáhly jedné miliardy dolarů. A to ještě nepočítáme ztrátu několika dalších miliard, která byla způsobena nepřímo. [2]

1.1 Proč je důležité mít zabezpečený počítač

Každým rokem se zvětšuje počet lidí, kteří jsou připojeni k Internetu. Co se ale nezvyšuje, je počet lidí, kteří by si uměli počítač dostatečně zabezpečit proti možným hrozbám. Většina uživatelů osobních počítačů postupuje následovně: Po koupi nového počítače a následnému nainstalování operačního systému (počítače s předinstalovaným operačním systémem už většinou alespoň nějaké základní bezpečnostní procedury mají za sebou) se okamžitě připojí k síti Internet, aniž by si uvědomovali hrozící nebezpečí. Přitom z některých průzkumů se dalo vyčíst, že 50% nezabezpečených a neaktualizovaných systémů Windows bude během 12 minut po připojení k Internetu vystaveno nějakému záludnému softwaru, kterému pravděpodobně podlehne. Nic na tom nemění ani známý fakt, že infikovaný počítač často nekončí jinak než formátováním disku a reinstalací celého systému. [4]

Další takovou neřestí obyčejných uživatelů je, že si nedokážou připustit velikost možného nebezpečí, kterou samozřejmě poté poznají, až když už je pozdě. Někteří uživatelé na podobné informace reagují stylem, že zrovna jim nikdo nemůže nic udělat a kdyby náhodou ano, tak v počítači stejně nic důležitého nemají. Ano, v počítači opravdu nemusí mít žádná data a už vůbec ne důležitá. I tak se ho podobné hrozby týkají a podobné reakce jsou samozřejmě jenom důkazem neznalosti či nesprávného myšlení. A právě takoví uživatelé jsou nejčastěji terčem útočníků. Útočníkům totiž sice často opravdu nejde o uživatelova data, ale stačí jim pouze to, že jeho počítač dostanou pod svou kontrolu a můžou ho používat k dalším útokům, což je pro ně většinou to hlavní. Proč by riskoval útok ze svého počítače, když to může podniknout z cizího? Nebo ho prostě použijí k nějakým „běžným" činnostem, jako je např. umístění nelegálního materiálu nebo zřízení phishingové stránky. K tomu se dále váže jedna nepříjemná věc, že útočník většinou u napadených počítačů nepotřebuje administrátorská práva dotyčného počítače, jak si často někteří nezkušení administrátoři myslí. Stačí jim běžná oprávnění s přístupem na síť.

Druhým nejčastějším terčem útoků bývají samotná data v počítačích. A nemusí se přitom jednat pouze o nějaká významná data velkých firem. V každém počítači se určitě něco dá najít. Například nějaké soubory s hesly sloužící k přihlašování do firmy či školy, díky kterým by pak útočník mohl v té konkrétní firmě nebo škole způsobit nějakou škodu, která by byla samozřejmě na uživatele, jelikož neutajil přihlašovací údaje. Škodu by samozřejmě uživatel musel uhradit. Dále může jít o data typu nelegálních multimédií nebo softwaru. Ty si z napadeného počítače může útočník pohodlně stáhnout a potrestán bude případně opět pouze jenom uživatel za poskytování nelegálních dat.

Všechny tyto útoky jsou obvykle prováděny přes napadené špatně zabezpečené a neaktualizované počítače. Tyto počítače nejsou pro útočníky problém pomocí automatizovaných softwarových nástrojů nalézt a ovládnout. Snaží se jich získat co nejvíce, aby je pak mohli sdružovat do skupin, ke kterým mají rychlý přístup a dají se jednoduše ovládat. Takovým skupinám, které poté provádějí různé nepříjemné aktivity či dokonce DDos (Distributed Denial of Service) útoky, se pak říká botnety.

Útočníci to všechno dělají kvůli spoustě různým motivů. Ať už je to uznání, pocit vzrušení, kompenzace nějakých vlastních chyb nebo pouhé zlomyslnosti. Nejčastější formou motivace ale není samozřejmě nic jiného, než peněžní či jiný zisk. Na závěr této části je dobré zopakovat, že důležité je mít zabezpečený počítač hlavně z toho důvodu, že případná

odpovědnost za škody je vždycky na majiteli počítače a argumenty typu, že se mu někdo dostal do počítače, nikoho nezajímají.

1.2 Proč se bezpečnost týká především systémů Windows

Snad by se ani nikde na světě nenašel člověk, kromě zaměstnanců firmy Microsoft, který by nesouhlasil s následujícími řádky. Většina uživatelů systémů Windows jednou dojde k pocitu, že tento systém rozhodně není dokonalý, což sice ani není možné, a dává uživatelovi o sobě vědět spoustou nepochopitelných programových chyb, které jsou v počeštěném výrazu často označovány jako bugy. Příkladem může být situace, kdy systém při 10. zapnutí počítače zapomene rozpoznat zapojenou klávesnici, i když v předchozích 9. případech žádný problém nebyl. Nebo se občas taky vyskytne nějaká bezdůvodná chyba, která se jako zázrakem vyřeší restartováním systému. Časem jsou podobné chyby častější, je jich čím dál více a tak většinou nezbývá nic jiného, než přeinstalovat systém. Osobně znám uživatele, kteří pravidelně reinstalují systém třeba i 2x za rok.

Většina uživatelů tyto „běžné“ nedostatky pochopí a přejde je. Jenomže v systému je možné najít spoustu dalších nedostatků v rámci bezpečnosti, které jsou na první pohled těžko postřehnutelné, o to více však vážnější a vystavují tak kolikrát uživatelův počítač před nebezpečí zmocnění útočníkem. O bezpečnosti Windows už toho bylo napsáno a řečeno mnoho, situace se sice pořád zlepšuje, ale pořád ne tak, jak by si asi většina odborníků a hlavně uživatelů přála. Windows už mají takovou pověst a to hlavně díky tomu, že z hlediska bezpečnosti taková prostě jsou a fakt, že s každou další verzí systému těchto bezpečnostních děr ubývá, moc na věci nemění. Hlavní problém je nejspíše ten, že u Windows jednoduše řečeno platí „co není zakázáno, to je povoleno“, na rozdíl od většiny ostatních operačních systémů, kde je to přesně naopak.[3]

Toto je jedna strana problému, ta méně závažná. Tou druhou a zároveň daleko závažnější jsou sami uživatelé. Windows by se totiž nestal i přes své pěkné grafické rozhraní nejrozšířenějším systémem, kdyby data uživatelů nabízel útočníkům na zlatém podnose. Takže největší podíl problému je vždy u uživatele. Většině z nich totiž zabezpečení počítače mnoho neříká a příliš se v tom nevyznají a neorientují. Hlavní pro ně je, že jim počítač funguje a o bezpečnost se začnou zajímat, až se jich to bezprostředně týká, což je už kolikrát pozdě.

Spousta uživatelů, jak už bylo řečeno v předchozí kapitole, taky žije v domnění, že počítač s Windows je po jeho nainstalování okamžitě připraven k bezpečnému použití, pokud už je neotravují vyskakující okna a jiné neřesti, které v systému byly před reinstalací. A pokud už se rozhodnou pro zabezpečení něco udělat, tak většinou to, že zapnou triviální firewall integrovaný přímo ve Windows a k tomu si stáhnou nějaký průměrný antivir z internetu, většinou z první reklamy, kterou uvidí, a myslí si, že jsou zachráněni. To však bohužel není pravda. Kvalitám Windows Firewall je věnována pozdější kapitola a antivirus není ten „všemocný zachránce“. Jedná se totiž o ne moc složitý software, který hledá známé virové sekvence v omezeném prostoru. Většinou v operační paměti a souborech na disku, některé antiviry mají navíc e-mailovou ochranu. Přestože většina antivirových softwarů využívá heuristickou analýzu, což je intuitivní metoda sloužící k hledání nových virů, tak na nalezení nových a moderních virů a trojských koní většinou nemají. Zabezpečení počítače je tedy potřeba chápat jako proces. Nestačí jenom nainstalovat firewall s antivirem, je potřeba taky vhodně nastavit zabezpečení počítače a podniknout preventivní kroky proti nebezpečí. Nejedná se sice o nic primitivního, ale zároveň nejde o nic, co by běžný uživatel nemohl zvládnout. O tom všem ale až v dalších kapitolách.

Projevy špatně zabezpečeného a napadnutého počítače:

- Často vyskakující a otravná okna s nevyžádanou reklamou
- Velmi zpomalený počítač s častým zasekáváním
- Při vytáčeném připojení jsou vytáčena exotická čísla s vysokou sazbou
- Počítače slouží k odesílání spamů a k útokům na jiné počítače
- Uživateli je odpojeno internetové připojení kvůli šíření viru

2 OPERAČNÍ SYSTÉMY MICROSOFT WINDOWS

Většina uživatelů si ani jiný operační systém než Microsoft Windows v počítači nedovedou představit. Většinou se jedná o jejich poslední verze. Nejnovější Windows 7, který se prosazuje den ode dne víc, jeho nepříliš povedený předchůdce Windows Vista nebo stále světově nejpoužívanější systém, i když už téměř 10 let starý, Windows XP. Celkově jsou systémy Windows asi na 90 % všech počítačů. Zbylý podíl si z větší části dělí systémy firmy Apple a linuxové distribuce. I když jsou Windows v dnešní době tak rozšířené, ne vždy tomu tak bylo a z počátku si Windows taky neprošly lehkými časy.[5]

2.1 Historie verzí Microsoft Windows

Na následujících řádcích jsou stručně popsány všechny jejich verze: [6]

MS-DOS: Jednalo se o systém, který byl původně vytvořen Microsoftem pro firmu IBM jako její konkurenční operační systém pro Apple. V porovnání s dnešními systémy je uživatelsky poměrně nepřívětivý a omezený. Pracoval pouze v textovém režimu.

Windows 1.0: Jednalo se prakticky jenom o grafickou nadstavbu systému MS-DOS. Využíval konceptu oken řazených do fronty a podporoval tzv. multitasking – běh více aplikací najednou.

Windows 2.0: Tento systém představil vylepšenou práci s okny a spoustu zajímavých aplikací jako např. rané verze editorů Word a Excel. Podporoval rozhraní DDE (Dynamic Data Exchange) a chráněný režim s rozšířenou pamětí procesoru 80386.

Windows 3.0: Systém s vylepšeným uživatelským rozhraním a multitaskingem. Jednalo se o velmi dobře prodávaný systém s dobrou podporou hardwaru. Dále představil službu Windows for Workgroups s řadou nástrojů a funkcí pro práci v počítačové síti a s podporou pro P2P sítě.

Windows NT: Jednalo se o první plně 32bitový systém, určen jak pro pracovní stanice, tak pro servery. Jako novinky systém představil podporu více procesorů, integrovaná podporu sítě nebo souborový systém NTFS. Systém používal plně preemptivní jádro, takže špatně naprogramovaná aplikace nemohla ohrozit běh celého systému.

Windows 95: Systém uvedl výrazné vylepšené uživatelské rozhraní s vylepšenou stabilitou systému z NT, integrovanou podporu TCP/IP, plug-and-play či FAT32, zároveň taky

ovšem nebývalý nárůst nároků na operační paměť. Později z něho vyšel Windows NT 4.0, který skloubením Windows 95 s NT 3.0 nabídl lepší práci se sítí.

Windows 98: Systém uvedl opět zlepšené grafické rozhraní a začleněné programy Internet Explorer a Outlook. Podporoval porty USB, rozhraní FireWire, grafické karet AGP, disky DVD a až osm monitorů najednou. V Second Edition verzi přibyly aktualizovaný Internet Explorer 5.0, DirectX 6.1a sdílené připojení k Internetu. Systém byl kompatibilní s NT 4.0.

Windows ME: Systém nabídl zamaskování MS-DOS a funkci System Restore pro obnovu poškozených systémových souborů. Byla to ovšem značně nespolehlivá a nestabilní verze, která měla problémy s kompatibilitou.

Windows 2000: Systém byl určen pro firemní sféru jako nástupce NT 4.0 vyznačující se vysokou spolehlivostí a rychlostí. Byly přidány i multimediální funkce z Windows 98 a podpora moderního hardware jako byly infraporty nebo bezdrátové sítě. Dále systém nabídl lepší integraci do podnikových sítí, Remote Desktop, podporu VPN a řadu dalších vylepšení.

Windows XP: Systém, jenž završil spojení stability a robustnosti NT systémů s multimediální využitelností Windows 9x. Vylepšil podporu pro starší aplikace a pracoval na jádru z verze NT 4.0. Dále také nabídl vyšší spolehlivost a zabezpečení oproti předchozím verzím, nový systém sdílení souborů a vylepšené bezpečnostní funkce.

Windows Server 2003: Jednalo se o čistě serverový produkt nabízející propracovanější bezpečnost, lepší robustnost a správu systémů. Byl to základ pro celou další sérii serverových produktů Microsoftu.

Windows Vista: Systém s téměř „revolučním“ uživatelským prostředím, inspirovaným systémy Mac OSX i linuxovými distribucemi. Byl velmi kritizovaný kvůli ovládání, bezpečnostním chybám a velké náročnosti na hardware. I samotná firma Microsoft nakonec přiznala, že tímto systémem šlápla tak trochu vedle.

Windows server 2008: Vychází ze stejného kódu jako Windows Vista a automaticky tak těží z několika výhod: IPv6, nativní podpora bezdrátových sítí, zvýšená rychlost a bezpečnost. Nabízí lepší podporu instalačních obrazů, spouštění a zálohování, širší možnosti diagnostiky, monitoringu a záznamu událostí serveru, lepší bezpečností prvky

(Bitlocker, vylepšená ochrana proti přetečení paměti, vylepšený Windows Firewall), .NET Framework 3.0, vylepšení jádra a správy paměti a procesů. [7]

Windows 7: Systém nabízí řadu změn a vylepšení oproti předchozím verzím systému Windows. Použitelnější rozhraní, rychlejší nastartování systému, nižší náročnost na hardware, lepší podpora více jádrových procesorů, podpora pro virtuální pevné disky, vylepšené a zmenšené jádro. Těží z ponechání povedených prvků z Windows Vista a přepracování těch méně povedených. Největší bezpečnostní vylepšení je v aplikacích „*Řízení uživatelských účtů*“ a Internet Explorer. [7]

2.2 Verze Windows XP

Základní a všeobecně známé a používané verze: [8]

Windows XP Home Edition – Verze určená hlavně pro domácí použití a běžné uživatele. Oproti verzi Professional chybí hlavně některé síťové funkce. Ideální pro hry, multimédia a Internet. Náhrada Windows 9x, ME, 2000 v domácích prostředích, ve firmách se používají jenom výjimečně.

Windows XP Professional Edition – Verze určená hlavně pro firemní sféru. Má oproti Home verzi hlavně rozšířenou podporou síťových služeb u počítačů, které se často připojují do domény (výhodou je možnost použít doménové uživatelské účty spolu s uživatelskými profily - uživatel se může přihlásit a pracovat na libovolném PC s Windows XP, připojeným do domény). Jedná se o verzi „bez kompromisů“, tzn. se všemi možnými funkcemi.

Verze XP Professional v porovnání s verzí XP Home obsahuje navíc:

- Soubory a složky offline; Vzdálená plocha
- Podpora až dvou symetrických procesorů
- Zabezpečení NTFS
- Uživatelské rozhraní s podporou více jazyků; Internetový informační servis
- Síťová podpora; Systémová politika; Síťové cestovní profily
- Šifrování EFS
- Zálohování a Automatický systém obnovy

- Řízení přístupových práv
- Protokol SNMP pro správu sítě

2.3 Verze Windows 7

Operační systém Windows 7 je možno zakoupit v následujících verzích: [7]

Windows 7 Starter Edition

Nejjednodušší verze dostupná hlavně v rozvojových zemích. Absence grafického rozhraní AERO a omezený multitasking na 3 spuštěné aplikace jsou hlavními omezeními této verze.

Windows 7 Home Edition

Verze dostupná opět jenom pro rozvojové země za patřičně sníženou cenu. Absence grafického prostředí AERO a možnosti sdílení internetového připojení v síti. Cílem verze je nahradit verzi Windows Vista Media Center.

Windows 7 Home Premium

Klasická a nejprodávanější verze, přikládána k množství hotových počítačů. Obsahuje prakticky všechny novinky systému, které běžný uživatel využije.

Windows 7 Professional

Verze hlavně ve znamení výrazně zlepšené bezpečnosti a opravdu širokých možností zapojení do sítě. K tomu přibyly zakódované datové systémy (EFS) a rozšířené zálohovací funkce pro síťová řešení. Dalšími doplňky jsou možnost připojení k doméně, podpora Vzdálené plochy, tisk podle umístění a offline adresáře.

Windows 7 Enterprise a Windows 7 Ultimate

Prakticky identické verze, jenom určené odlišným uživatelům (Firmy a osoby). V těchto verzích najdeme bezpečnost dohnanou na absolutní maximum a to díky aplikacím Bitlocker (ochrana dat), Applocker (správa pc). Dále možnost bootovat přes virtuální harddisky.

3 HROZBY A RIZIKA UŽIVATELŮ

Většina lidí si díky titulkům zpravodajských medií může myslet, že jedinými opravdu vážnými hrozbami našeho počítače jsou viry šířené emailovými zprávami a hackeři vykrádající bankovní účty. To je samozřejmě naprostá nepravdivá informace. Hrozí nám prakticky cokoliv, kdykoliv, odkudkoliv a hlavně od kohokoliv. Např. jeden průzkum v USA ukázal, že 38% všech dotazovaných firem bylo někdy zasaženo neautorizovaným přístupem svých zaměstnanců – ať už současných nebo bývalých. Na následujících řádcích je uvedeno, jaké druhy hrozeb nám můžou hrozit? [2]

3.1 Hrozba číslo 1: Fyzické útoky

Jedná se jednoznačně o nejzákladnější možnost k útoku, ke kterému útočník nepotřebuje žádné znalosti ohledně počítačů. Ponecháte-li někde bez dozoru svůj notebook v místě, kde vám ho může někdo odcizit, velmi lehce se tak může stát. Pokud se tomu tak stane, rozhodně vás nezachrání sebelepší zabezpečení počítače nebo zašifrování jeho dat. Útočník bude mít totiž prakticky neomezený čas z počítače získat vše, co potřebuje a pokud něco opravdu bude chtít, tak to s dostatkem času získá přes jakékoliv zabezpečení. Odcizení stolních počítačů je samozřejmě o něco složitější, zdaleka ne však nemožné.

Dále útočníkovi ani nemusí jít o odcizení počítače. Pokud necháte svůj počítač bez dohledu, útočník si může lehce zkopírovat potřebná data nebo nainstalovat špionážní software a vy absolutně nic nepoznáte. Obrana proti tomuto druhu hrozby je celkem jednoduchá. Nenechávat svůj notebook bez dozoru, stejně tak jako stolní počítač v otevřené místnosti. U stolního počítače je vhodné taky nějaké mechanické zabezpečení, které může alespoň snížit útočníkovi případnou krádež.

3.2 Hrozba číslo 2: Ukradená hesla

Hesla jsou stále nejpoužívanější identifikační metodou k prokázání totožnosti, ať už je to k přihlášení do systému nebo na webových stránkách. A ještě dlouho dobu budou. Výhodou této metody jsou velmi nízké pořizovací a provozní náklady. Pokud se k vašemu heslu tedy někdo dostane, dostane tím i naprosto stejnou pravomoc jako vy. Co všechno to může znamenat, asi není potřeba rozvádět. Od čtení e-mailových zpráv, jednoduchým posíláním

pošty pod vaším jménem, až třeba po přístup s vašimi právy do vaší firmy. Samozřejmě jako vždy, všechna způsobená škoda je jen a jen na vás.

Za velký bezpečnostní nedostatek můžeme považovat to, že stále nejrozšířenější operační systém Windows XP nijak nepředchází nevhodnému zacházení s hesly. Po instalaci Windows XP vůbec nemusíte zadávat žádná hesla a hned dostanete účet bez hesla s plnými administrátorskými oprávněními. Tento nedostatek nebyl odstraněn ani přes několik „Service packů“, stejně tak ani v novějších systémech Windows Vista a Windows 7. Alespoň je vyžadováno zadání hesla při pokusu o přístup ke sdílení. Dost nešťastným doplňkem je nápověda hesla při přihlašování. Heslo by si měl každý pamatovat a jakákoliv nápověda pomáhá sice i vám, ale hlavně případnému útočníkovi.

Hesla se doporučují používat minimálně osmi-znaková. Vzhledem k faktu, jak lehce jsou hesla do Windows rozluštitelná, bez ohledu na verzi, tak je velmi dobré používat heslo se 16 – ti znaky a víc. Samozřejmostí je kombinace velkých písmen, malých písmen, číslic a interpunkčních znamének. A pokud možno používat zkombinování toho všeho v něco, co nedává žádný smysl, ale to už je samozřejmě horší na zapamatování. Velmi špatným zvykem většiny lidí je zvolení si hesla podle jednoduchých a snadno zjistitelných údajů, jako jsou data narození, jména svých přátel, domácích mazlíčku apod. Dále si někteří, pro ještě jednodušší zapamatování hesla, volí kombinace typu „12345“ apod. Další velkou chybou je, že většina uživatelů z důvodu pohodlnosti, kdy si nemusí pamatovat více hesel, používá stejné heslo jak do nějakého diskuzního fóra, tak i internetovému bankovnictví.

3.3 Hrozba číslo 3: Zvědaví síťoví sousedé

Důvěra je jedna z největších lidských slabostí, pokud se budeme stále držet v počítačové bezpečnosti. Typický příkladem může být podcenění ochrany počítače a souborů před kolegy v práci. Sdílení souborů může výrazně vylepšit produktivitu práce, ale zároveň při špatném bezpečnostním nastavení způsobit velké bezpečnostní problémy. Zde jsou tři nejčastější bezpečnostní problémy se sdílením souborů:

1) Důvěrné soubory jsou sdíleny. Taková situace nastává buď nedopatřením, nebo nepozorností. Typickým příkladem je sdílení složky, která má spoustu podsložek a v některé z nich jsou soubory, které by měly zůstat důvěrné. Bezpečnostním opatřením,

kterým můžeme podobným situacím předcházet, je vytvoření pravidel, které udávají, co se s kterými typy souborů může provádět. Samozřejmostí je proškolení uživatele.

2) Neomezený přístup ke sdíleným souborům. Jedná se např. o soubory, které je nutno sdílet mezi úzkou skupinou uživatelů a s nesprávně nastavenými oprávněními, která jsou příliš široká, k nim má přístup daleko více lidí. Tento problém se např. ve Windows XP nejčastěji vyskytuje P2P sítích, kdy je použita konfigurace „Zjednodušené sdílení souborů".

3) Změny souborů bez povolení. Správně by měl mít přístup ke změnám v jednotlivých souborech co nejomezenější počet lidí. Pokud má přístup zbytečně mnoho lidí, lehce se stane, že nějaký neopatrný či škodolibý uživatel zničí jednoduše spoustu práce dalších lidí. Takovým problémům se lze vyhnout hlavně správnou konfigurací sdílených prostředků.

3.4 Hrozba číslo 4: viry, červi a jiné nepřátelské programy

Jestli něco z počítačové bezpečnosti zná snad opravdu každý člověk, tak jsou to pojmy vir a červ. Je to poměrně logické, jelikož v případě rozšíření nějakých nebezpečnějších pravidelně zaplňují titulky většiny masmédií s údaji o způsobených škodách. Vzhledem k tomu, že takových velmi škodlivých virů a červů bylo za poslední roky spousta, tak je smutným faktem, že spousta uživatelů věnuje pozornost těmto hrozbám až v okamžiku, kdy už je vir značně rozšířen, což už je taky kolikrát pozdě. Tito uživatelé bývají nejčastějšími oběťmi těchto hrozeb. Nejčastějšími hrozbami jsou:

Počítačový vir – Obdoba biologického viru. Jedná se programový kód, který je schopen se sám replikovat připojením k jinému objektu. V systémech Windows napadají registry, systémové soubory, případně poštovní programy. Viry jsou dále schopny porušovat či mazat datové soubory. Část programu, která se stará o hlavní destruktivní část se nazývá efektivní kód.

Počítačový červ – Jedná se o nezávislý počítačový program, který se dokáže sám kopírovat z jednoho počítače na další. Většinou tak činí přes síť nebo přílohy e-mailových zpráv. Dnešní červi už jsou natolik silní, že dokáži prakticky odrovnat operační systém.

První škodlivé programy a počítačové viry se objevily na počátku 80. let. Z počátku se šířili přes obyčejné diskety, poté přes poštovní programy a v posledních letech díky velkému rozmachu Internetu samozřejmě přes něj, kde se jejich činnost často zamaskovává nějakým

multimediálním či jiným obsahem. Dnešní viry jsou navíc čím dál více nebezpečnější a „multifunkční“. Autoři je dokáží vybavit inteligentní instalací, složitým šifrováním nebo automatickou aktualizací z internetu. Navíc dokážou „mutovat“, což znesnadňuje jejich případné odstraňování, jelikož pak každý vypadá jinak, a taky se skrývat před antiviry.

Viry a červi se stále nejvíce rozšiřují přes elektronickou poštu, ale už to není zdaleka jediný způsob jejich šíření. Můžou se šířit přes síťové sdílení, emailové zprávy v HTML formátu nebo přes ovládací prvky skriptů ActiveX. Nejznámější a nejnebezpečnější viry se většinou šíří více cestami, tedy kombinovaně. Jenom tak pro zajímavost, na Internetu se dá nalézt spousta jednoduchých nástrojů, pomocí kterých si dokáže vytvořit destruktivní vir i naprostý laik.

Z dalších škodlivých programů je nejznámější spyware. Jedná se o docela široký pojem, který zahrnuje vše od programů sponzorovaných reklamou sledující uživatelovu činnost až po programy, které automaticky otvírají okna se stránkami sponzora softwaru. Jednoduše ale můžeme říct, že se jedná o jakýkoliv program, který byl nainstalován většinou nějakým klamavým způsobem bez uživatelova vědomí a s jeho plným souhlasem, zobrazuje nevyžádanou reklamu a monitoruje uživatelovu činnost. Souhrnně všechny tyto neřesti, zmíněné v této kapitole, často označujeme jako malware.

3.5 Hrozba číslo 5: Vnější nepřítel a oběti trojských koní

Většina hackerů nejsou takoví, jak si asi většina lidí myslí. Představují si je jako vysoce inteligentní lidi, kteří se během několika vteřin dokážou nabourat kamkoliv si zamanou. Většina hackerů z reálného světa samozřejmě není tak skvělých ve svém oboru, přesto ale i tak dokážou napáchat spousty škody, pokud jim to usnadníme svým špatně zabezpečeným počítačem. Spousta z nich se nezaměřuje pouze na jeden konkrétní počítač či jednu počítačovou síť. Většinou používají předem připravené nástroje stažené z Internetu, které nabourávání systémů automatizují. Umí taky procházet tisíce IP adres, na kterých hledají bezpečnostní díry.

Někteří profesionálové v oblasti počítačové bezpečnosti jsou někdy hákliví na pojem „hacker“. Zde je uvedeno upřesnění: „Hackeři“ jsou útočníci, kteří napadají cizí počítače za účelem nalézt jejich slabá místa. Naopak útočníci, kteří se nabourávají do systémů s

úmyslem provést nějakou škodu či jenom z pouhého pobavení, jsou označování jako „crackeři“. V práci je nadále používán obecný pojem „hacker“, nebo spíše útočník.

Útočníci se nejčastěji zaměřují na následující:

Nechráněné sdílené prostředky. Zde využívají toho, že jedna ze základních bezpečnostních zásad nebývá často dodržena a ke sdíleným souborům tak mají přístup i uživatelé jiných počítačů, než pro které jsou soubory určeny. Takovýto bezpečnostní nedostatek může taky vést k tomu, že útočník může pohodlně nainstalovat nějaký software pro vzdálenou správu počítače.

Otevřené porty služeb. Zde útočníci využívají toho, že uživatel nemá nainstalovány některé opravné balíčky, které napravují bezpečnostní chyby běžících serverových služeb a testují je na známé bezpečnostní díry či slabá hesla. Nejčastěji se jedná o webové servery, FTP či IM komunikaci nebo programy pro vzdálený přístup.

Trojské koně. Jedná se o skryté programy, díky kterým může uživatel nepozorovaně převzít kontrolu nad napadeným počítačem. Už z názvu vyplývá, že se tyto programy tváří jako neškodné aplikace a uživatelé si je tak snadněji nainstalují. Počítače, které byly napadeny programem v podobě trojského koně, se někdy označují jako zombie. Trojské koně jsou někdy označovány jako „backdoor“ neboli „zadní vrátka“.

3.6 Hrozba číslo 6: Zásahy do soukromí

Zde útočníci nepozorovaně využívají toho, že Internet Explorer, který byl ještě donedávna nejpoužívanější internetový prohlížeč, o vás úmyslně nebo i bezděčně prozrazuje spoustu informací. Například verzi vašeho prohlížeče, které pluginy máte nainstalované, vaši IP adresu nebo taky odkaz, z kterého jste vstoupili na tu a tu stránku. Tyto údaje možná nejsou až tak důležité a taky slouží hlavně pro zlepšení komunikace vašeho prohlížeče se stránkami, které uživatel navštěvuje. O to méně bezpečná je jiná funkce, kterou obsahují všechny prohlížeče - soubory cookies. Jedná se o malé datové soubory, které obsahují trvale zaznamenané informace o vás a o vaší komunikaci s konkrétní webovou stránkou. Cookies obsahují osobní informace pouze v případě, že jim to sami povolíte. Na druhou stranu, na některých webech se bez nich vůbec neobejdete. Soubory cookie většinou pouze zaznamenávají jakési identifikační čísla, na jehož základě webové stránky poznají, že se např. vaše návštěvy opakují. Soubory cookie jsou výhodné zejména pro aplikace

internetového nakupování a pro servery, kde je potřeba se při přístupu prokázat svojí identitou. Na druhou stranu, na některých webových serverech můžete např. vyplnit nějaký registrační formulář a jeho data se do cookie uloží také. Většina hrozeb ohledně cookies je ale způsobena cookies třetích stran, kdy nějaké reklamní systémy monitorují váš pohyb po internetu. S těmito cookie se snaží prohlížeče zacházet podle jiných pravidel, než s těmi běžnými. Existuje také spousta nástrojů pro všechny prohlížeče, které pečlivěji kontrolují jednotlivé cookie soubory.

Dalším problémem ještě může být ukládání historie prohlížených stránek. Standardně se ukládají poslední tři týdny. I z těchto informací se můžou útočníci dozvědět spoustu informací a zahladit úplně stopy po prohlížení není vůbec tak jednoduché, jak se může zdát.

3.7 Hrozba číslo 7: Hrozby z elektronické pošty

Jak už bylo několikrát zmíněno, e-mailová pošta je stále hlavním nástrojem, který přenáší viry. Ovšem to není jediná bezpečnostní nepříjemnost s ní spojená. Pokud pošlete e-mailovou zprávu, tak ta putuje přes desítky různých zařízení, jako jsou směrovače či servery. Kdekoliv může být vaše zpráva zachycena a přečtena, ba dokonce i změněna. Dále nemusíte mít žádné špičkové znalosti ohledně počítačů, abyste dokázali poslat zprávu z jakéhokoliv jména či adresy. Z toho plyne velké varování – nikdy neposílejte elektronickou poštou žádné důvěrné informace a nikdy nedávejte elektronické poště přednost před osobním setkáním např. v důležitých jednáních. Není to úplně bez komplikací, ale řešení na tyto problémy se dá najít. Obsah zpráv se dá zabezpečit velmi silným šifrováním a pravost odesílatele se dá ověřit díky digitálnímu podpisu.

Poslední problémem elektronické pošty, sice ani ne tak bezpečnostním, je nevyžádaná pošta – spam. Spam tvoří drtivou většinu všech e-mailů a pro uživatele většinou nepřestavuje ani tak bezpečnostní hrozbu, jako spíš nepříjemnost. Na druhou stranu, spam s sebou může taky nést viry a podobné neřesti.

[2]

3.8 Sociální inženýrství

Internetové vandaly a zloděje pro lepší přehlednost rozdělujeme do tří základních a všeobecně známých kategorií:

1) Script kiddies – Tímto termínem jsou označovány většinou mladí a začínající hackeři, kteří nemají ani tak moc velké znalosti programování. Ke svým útokům většinou používají nástroje, které se lehce dají nalézt na Internetu a které uživatele můžou ohrozit pouze v případě, kdy jeho systém obsahuje nějakou významnou a dlouho známou bezpečnostní díru. Tito útočníci většinou nemívají žádné vážnější cíle. Často pouze nadělají škody typu vymazání všech dat a k tomu přidají nějaký vysmívající se vzkaz. O nějakém maskování útoků a podobných věcech u tohoto typu útočníků nemůže být ani řeč, proto je většinou hned jasné, že se v počítači něco dělo.

2) Střední třída – V této skupině už jsou hlavně útočníci, kteří mají výborné programovací schopnosti a dokonalé znalosti operačních systémů, na které útočí. K útokům taky většinou používají nástroje připravené někým jiným a pouze v případě potřeby si je trochu poupraví. Na rozdíl od první kategorie se často nesoustředí pouze na jeden počítač, ale na více počítačů v síti. Snaží se také pracovat nepozorovaně. Mezi jejich nejčastější činnost patří ukradení dat s následným vrácením za určitý finanční obnos.

3) Top class – Tato kategorie je naprostou špičkou hackerského oboru. Mají elitní znalosti ohledně programování a operačních systémů. Jsou to právě oni, kdo vytváří a pak nabízí či prodává hackerské nástroje pro první dvě skupiny. Při svých útocích, které bývají většinou organizované a míří na velké firmy, používají také špičkové maskovací nástroje. Následky útoku od této kategorie útočníků nebývá vůbec lehké a levné odstranit.

Běžný člověk se samozřejmě s posledním typem útočníků asi těžko potká. Na rozdíl však od prvních dvou, se kterými se může setkat prakticky kdykoliv a proto je dobré vědět, jak se jejich útokům bránit. Na útoky od první kategorie hackerů většinou stačí dodržovat základní bezpečností zásady a mít správně zabezpečený a zaktualizovaný operační systém. Útoky od druhé skupiny už však bývají více promyšlené a většinou tu nejde ani tak od data uživatele, jako spíš o kontrolu nad nějakým jeho účtem, či už bankovním nebo e-mailovým, nebo o informace. Kromě programátorských znalostí však bývá z velké míry používáno sociální inženýrství neboli sociotechnika.

Tento termín zavedl Američan Kevin Mitnick a slouží k označování činností, při kterých sociotechnik přesvědčuje lidi, aby pro něho konali věci, které by za normálních okolností asi nedělali. Využívá přitom svého šarmu a „umění mluvit“. Útočník většinou postupuje tak, že si většinou zjistí ne až tak důležité informace, které pak použije při získávání těch, o které má zájem. Jenom tak na ukázku nějaký praktický příklad: Útočník zavolá do vaší firmy, představí se jako pracovník technické podpory, využije svých dovedností a dříve získaných informací a bez problému přesvědčí pracovníka u telefonu, aby si například nainstaloval nějaký nový antivirový software, který však ve skutečnosti není nic jiného než obyčejný spyware nebo trojský kůň. Co to pro data firmy může znamenat, si už asi každý dokáže představit. V celé oblasti sociálního inženýrství využívá hlavně důvěry lidí.

Nejběžnější techniky sociálního inženýrství:

Podvržení identity – Naprosto základní a běžná věc. V dnešní době není potřeba ani žádných hackerských schopností k tomu, abyste například odeslali e-mailovou zprávu, která vypadá jako by ji poslal kdokoliv jiný. K tomu taky není problém e-mailovou zprávu nastavit tak, aby došla zpět na vaši adresu.

Phishing – Jedná se asi o nejznámější techniku sociálního inženýrství a zároveň velmi podobnou té předchozí. Nejběžnějším příkladem bývá podvržený e-mail s nějakým problémem, který se tváří jako oficiální a požaduje po klientovi kliknutí na odkaz ve zprávě a následné zadání osobních údajů či hesel. Pokud se tomu tak stane, dojde k přesměrování na tu stránku, kterou uživatel čekal. Vypadá tak ovšem jenom na pohled. Ve skutečnosti jde o podvrženou stránku, kterou útočník nastražil a ze které lehce odebírá data uživatelů. Použití této metody bývá pro útočníky velmi jednoduché. Odešlou e-mail na spoustu adres a pak jen čekají, kolik neznalých uživatelů se nachytá.

Pretexting – Jedná se o techniku, při které útočník využije smyšleného scénáře, ke kterému přihodí trochu pravdivé informace kvůli věrohodnosti, za účelem přesvědčení oběti, aby vykonala pro útočníka potřebnou činnost. Tuto techniku často využívají soukromí detektivové při získávání různých informací, které pak můžou pomáhat v dalším pátrání. Jedním z hlavních důvodů, proč se tato technika hojně používá je, že spousta firem a institucí stále identifikují osoby podle relativně snadno dostupných informací typu rodné číslo. Při použití této techniky útočníkovi prakticky stačí s dostatečně přesvědčivým obsahem konverzace jenom být přichystán na možné kontrolní otázky.

Pharming – Zde se jedná o techniku, která se používá na Internetu. Opět se jedná o podvodnou techniku, při které je cílem získat citlivé údaje obětí. Při této metodě jde o napadení DNS serveru a následné přepsání IP adresy, které způsobí oběti přesměrování určených stránek na stránky připravené útočníkem. Tyto stránky jsou samozřejmě dokonale podobné a najít mezi nimi rozdíl dělá potíže i zkušeným uživatelům. Tato technika se často překládá do češtiny jako „farmaření".

Odcizení identity – Tato technika se z následujících důvodů využívá především v USA. Metoda se používá na Internetu tam, kde je po uživateli požadován pouze jeden způsob ověření totožnosti. Útočníkovi tedy většinou stačí znát číslo občanského průkazu nebo kreditní karty.

Všechny výše uvedené metody se netýkají, jak by se mohlo na první pohled zdát, jenom nějakých významných osob a firem, ale hlavně i obyčejných lidí. Sociální inženýrství se rok od roku čím dál více rozšiřuje a přesto stejně spousta lidí ani neví, co tento pojem znamená, natož jak se proti němu bránit. Samozřejmě se to všechno týká i naší země, kde bylo již zaznamenáno spoustu případů např. pro odčerpání nemalých částek z bankovních účtů díky úspěšnému provedení technik sociálního inženýrství. V podobných situacích banky samozřejmě vinu pohodlně přesunou na uživatele, aniž by je alespoň nějak informovali o možných nebezpečích sociálního inženýrství. Cílem útočníků nebývají jenom bankovní konta, ale z velké části i jenom samotné informace. Je toho opravdu mnoho, co vše lze získat díky „obyčejným" informacím typu rodné číslo, kopie různé smlouvy nebo i lékařský záznam. Přesto, že v případě úspěšného útoku je vina vždy na straně oběti, tak metody a techniky obrany proti sociálnímu inženýrství u nás vznikají a rozšiřují se velmi pomalu. Jak je dobré se podobným útokům bránit? V takových případech je nejdůležitější především znalost, osvěta a informovanost uživatelů. Všechny tyto věci v kombinaci se zdravým rozumem. Pokud se tedy věnujeme počítačovému zabezpečení, nesmíme každopádně zapomenout na obranu před sociálním inženýrstvím.

[1]

4 PROSTŘEDKY SLOUŽÍCÍ K ZABEZPEČENÍ VE WINDOWS 7

Systém Windows Vista přinesl několik znatelných funkcí zabezpečení, ovšem ne všechny byly přijaty s chválou. Proto byly některé v systému Windows 7 přepracovány a vylepšeny. Jedná se hlavně o nástroj Řízení uživatelských účtů, program Windows Defender a bránu Windows Firewall. V tomto systému taky přibyla řada skrytých vylepšení a funkcí pro zabezpečení počítačů ve velkých sítích, které jsou primárně v zájmu vývojářů softwaru a profesionálů pohybujících se v oblasti informačních technologií. Ale taky i hackerů, pro které tyto nové funkce představují nové výzvy a překážky. Dále jsou uvedeny hlavní novinky trochu blíže.

4.1 Windows Firewall

Firewall je základní částí v ochraně počítače proti nebezpečným útokům. Jedná se o hlavní hradbu mezi počítačem a sítí, hlavně tedy Internetem, a zabraňuje před nechtěnými síťovými příchozími či odchozími připojeními. Přestože je používání firewallu nesmírně důležité a zároveň velmi snadné, mnoho uživatelů toto přehlíží.

Firewall se nachází v systému Windows již od verze XP a s každou další verzí se vylepšoval. V poslední verzi systému najdeme obousměrný stavový - paketový filtr. V případě zablokování některých paketů nás program neotravuje oznamováním, pouze pokud bychom si to přáli. V počáteční konfiguraci je nastaven následovně:

- Brána firewall blokuje veškerá příchozí spojení kromě těch, která jsou explicitně povolena některou z vytvořených výjimek.
- Je povolen veškerý odchozí provoz, pokud neodpovídá nakonfigurované výjimce.

Často je námětem diskuzí, proč je ve výchozím nastavení odchozí provoz povolen. Je to z důvodu, že brána Windows firewall byla navržena k ochraně a údržbě zabezpečeného počítače. Pokud by nějaký škodlivý program vytvářel odchozí připojení, váš počítač by již byl napaden. Zde by špatně odvedl svou práci antivirový software. Dále by blokování odchozích připojení vedlo k mnoha upozorněním, což by mohlo mít za následek, že by je uživatelé ignorovali.

Srovnání nejnovější verze firewallu s verzí pro XP:

- Podpora sledování a řízení jak příchozího, tak i odchozího síťového provozu.

- Podstatně více možností konfigurace (např. protokol IPset) a možnost vzdálené správy. Díky novému průvodci lze také snadněji vytvářet a konfigurovat pravidla.
- Dříve šli nastavit jenom běžná kritéria jako adresy, protokoly nebo porty. Nyní lze nastavit pravidla brány firewall i pro služby, účty a skupiny služby Active Directory, zdrojové a cílové IP adresy pro příchozí a odchozí provoz, přenosové protokoly jiné než TCP a UDP a mnoho dalšího.

4.2 Windows Update

V případě zabezpečování počítače je po použití firewallu na druhém místě v důležitosti udržet si aktualizovaný systém. K tomuto ve Windows 7 slouží program Windows Update. Tento software vyhledává, stahuje a následně aktualizuje opravné záplaty, které většinou opravují kódy, u kterých byla zjištěna nějaká závada nebo bezpečnostní chyba. Windows Update stahuje a instaluje automaticky, pokud si to uživatel nepřeje, může si v to konfiguraci softwaru změnit.

V posledních letech vycházejí aktualizace mnohem dříve, než tomu bývalo v dřívější době. Většinou je bezpečnostní problém vyřešen dříve, než způsobí nějaký větší problém většině uživatelů. I přes tato pozitiva je smutným faktem, že se stále najde spousta uživatelů, kteří systém neaktualizují. Právě tito uživatelé bývají nejčastěji napadeni nějakým škodlivým softwarem.

4.3 Blokování virů a červů pomocí antivirového programu

Windows 7 v základu neobsahuje žádný antivirový software, stejně jako ve všech předchozích verzích. Z toho může plynout otázka: Je vůbec takový software zapotřebí? Mnoho uživatelů, často i odborníků, totiž žádný antivirový software nepoužívá. Většinou je to z následujících důvodů:

- Zvláště odborníci tvrdí, že není třeba používat tento druh softwaru, když vydání aktualizace na nové hrozby kolikrát trvá i 24 hodin.
- Antivirový software představuje další programovou vrstvu v počítači, tudíž další možné skulinky pro útočníky
- Antivirový software si stejně jako každý jiný sw bere část výkonu procesoru.

Všechny důvody jsou už ale v dnešní době prakticky neopodstatněné. Microsoft možná i proto už nyní nabízí svůj antivirový software Microsoft Security Essentials. Stejně tak se dá najít na trhu spousta jiných výborných programů, ať už ve freeware verzi, nebo placené. Tyto programy se dají dohledat i přímo v systému.

Dále Microsoft nabízí asi každých 14 dní přes službu Windows Update obslužný nástroj pod názvem Malicious Software Removal Tool. Tento program slouží k pročištění systémů, které byly infikovány známými a rozšířenými viry a jinými formami škodlivého softwaru. Po skončení práce se program opět vymaže. Alternativou můžou být webové služby některých výrobců antivirového softwaru na vyhledávání virů. Ale ani pravidelné kontroly programem Malicious Software Removal Tool nebo jiným online nástrojem vám neposkytnou nepřetržitou ochranu před viry a jinými neřestmi. K dosažení trvalé ochrany musíte mít nainstalovaný a spuštěný antivirový program.

4.4 Microsoft Security Essentials

Jedná se o bezplatnou a komplexní ochranou počítače přímo z dílen Microsoftu, která pomáhá uchránit počítač před viry, trojskými koňmi, spyware a dalšími bezpečnostními riziky. V nezávislých testech dosahuje velmi dobrých výsledků a Microsoft ho nabízí ke stažení také přes službu Windows Update. Program běží na pozadí a prakticky nezatěžuje výkon procesoru. Mezi jeho hlavní funkce patří ochrana před různými rootkity, realtimová ochrana jádra systému nebo například služba dynamických porovnání.

4.5 Windows Defender

Jedná se o antispywarový program integrovaný ve Windows 7. Jedná se o antispywarové řešení pro domácí počítače a počítače malých podnikových sítí. Program pracuje ve dvou režimech. V prvním pracuje se známými a škodlivými nehodnotnými programy, které bez obtěžování uživatele odstraní nebo uloží do karantény. V druhém režimu, v tzv. šedé zóně, pracuje s programy, které jsou podezřelé spywarům. V tomto případě se uživatele s radou dotáže, jakou akci má provést. Dále program ještě kromě realtimové ochrany provádí i pravidelné kontroly souborů v počítači uživatele.

Windows Defender běží v počítači jako služba, nikoliv jako proces, což umožňuje chránit všechny uživatele. K běžným činnostem program nevyžaduje vyšší oprávnění, než ta běžného uživatele. Ve výjimečných případech však ano.

4.6 Řízení uživatelských účtů

Tento nástroj byl nejpřevratnější změnou z hlediska bezpečnosti v systému Windows Vista. Jedná se o upozornění, které se objeví vždy, když se uživatel nebo program pokouší provést nějakou systémovou úlohu a před pokračováním vyžaduje souhlas administrátora. Původní verze tohoto nástroje se setkala s velkou nevolí uživatelů, protože se jim jevil jako příliš dotěrný a otravný, což nejednou vedlo k vypnutí tohoto nástroje. Proto ho najdeme ve Windows 7 značně přepracovaného.

Nástroj je nyní mnohem méně otravný pro uživatele. A to hlavně z toho důvodu, že uživatelé se standartními oprávněními nyní mohou provádět mnohem více činností, hlavně při procházení systému, jelikož při provádění změn budou stále často požadovat oprávnění správce. Změnou jsou především možnosti instalování aktualizací či nastavování síťových adapterů. Dále došlo díky sloučení ke zmenšení celkového počtu upozornění a taky nyní nástroj nabízí větší možnosti konfigurace.

Účinnost tohoto nástroje je nyní na takové úrovni hlavně proto, že ve Windows 7 jsou všechny účty, na rozdíl od minulých verzí systému a účtu administrátora, vytvářeny jako neadministrátorské s omezenými oprávněními. I přes to ale pod nimi jdou provádět všechny činnosti, které běžný uživatel potřebuje. K tomu ale i účty administrátora nepracují tak, jak bývalo zvykem. Správce počítače pracuje s oprávněními běžného uživatele s výjimkou úloh, které potřebují administrátorská oprávnění. Stejný způsob privilegií účtů už ale není možné převést zpět na Windows XP, jelikož všechny dřívější aplikace byly napsány s tím, že uživatelé mají úplná oprávnění. Novější programy jsou už však s ohledem na bezpečnost psány bez požadavků na oprávnění administrátora.

Co se týče zprovoznění starších programů pod Windows 7, tak na to má systém několik metod, díky kterým si program myslí, že je spuštěn pod administrátorem. Nejčastěji využívaným z nich je virtualizace souborů a registru (také známá jako přesměrování dat).

4.7 DALŠÍ BEZPEČNOSTNÍ NOVINKY V SYSTÉMU WINDOWS 7

- Internet Explorer 8 – Internetový prohlížeč firmy Microsoft měl poslední dobu spíše pověst „otevřené branky do systému“ než kvalitního a bezpečného prohlížeče. To se ale s verzí dostupnou pro Windows 7 změnilo. Internet Eplorer zde efektivně běží v chráněném režimu a izolovaném prostoru s omezenými právy, což zaručuje menší pravděpodobnost nainstalování škodlivých programů. Data zapisuje pouze do dočasných a uzamčených složek, dokud nedostane od uživatele jiné povolení. Dalšími hlavními bezpečnostními vylepšeními jsou omezení prvků ActiveX, filtr SmartScreen pro lepší ochranu proti phishingu nebo filtr InPrivate pro anonymní surfování. Nedávno vyšel Internet Explorer v nové verzi s číslem 9.

- Biometrická služba systému Windows - Windows 7 podporuje biometrická zařízení pro čtení otisků prstů, takže například pro přihlášení k počítači můžete použít čtečku otisků prstů.

- Šifrování dat – Windows 7 ve verzích Enterprise a Ultimate nabízí šifrovací nástroj BitLocker Drive Encryption a BitLocker To Go, který dokáže šifrovat i celé disky, stejně tak vyměnitelná úložiště.

Bezpečnostní novinky v porovnání se systémem Windows XP:

- Přesměrování dat – Programy, které běží pod neadministrátorským účtem a pokoušejí se zapisovat do chráněné systémové složky, jsou transparentně přesměrovány do virtuálního úložiště souborů. Stejně tak bývají přesměrovány registry do virtuálních klíčů. Takováto virtualizace souborů a registru dále dovoluje, aby standardní uživatelé mohli spouštět i starší aplikace (hlavně z XP) a současně zabraňuje škodlivým aplikacím v zápisu do oblastí, kde by mohly způsobit havárii celého systému.

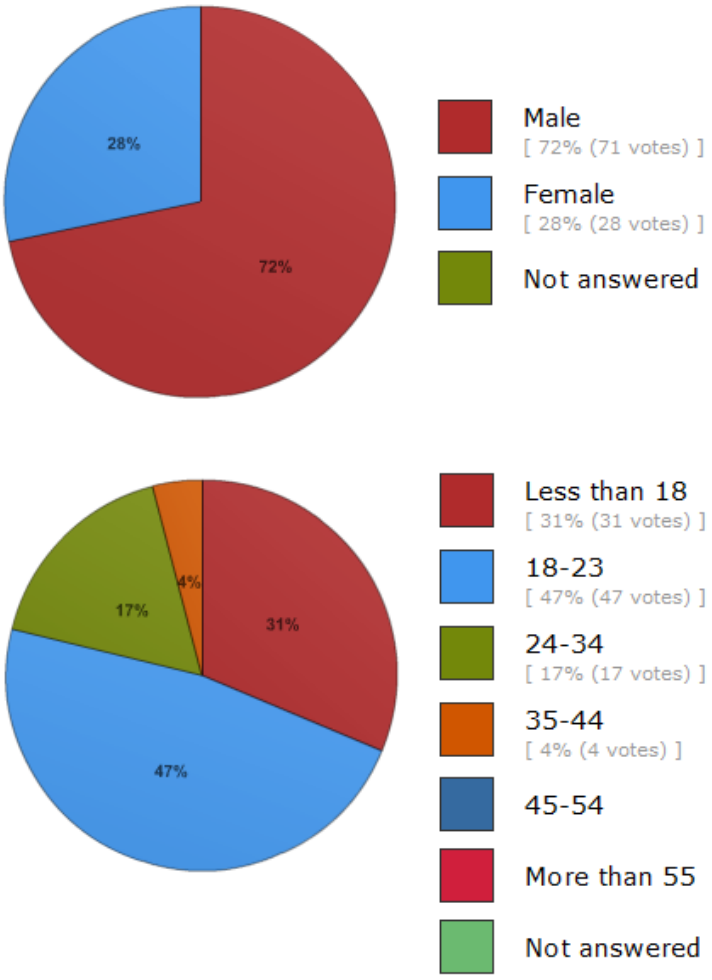
- Ochrana proti přetečení zásobníku – Systém Windows 7 obsahuje podpůrnou technologii ASLR, která pomáhá chránit před útoky využívající přetečení zásobníku. Spočívá v tom, že při každém spuštění systému Windows načte systémový kód do jiných paměťových oblastí.

- Přídavná bezpečnost na 64bitových počítačích - Na 64 - bitovou verzi systému Windows 7 lze nainstalovat jen digitálně podepsané ovladače zařízení. Toto slouží k tomu, že kódy na úrovni jádra pocházejí ze známých zdrojů. [7]

II. PRAKTICKÁ ČÁST

5 VEŘEJNÝ DOTAZNÍK

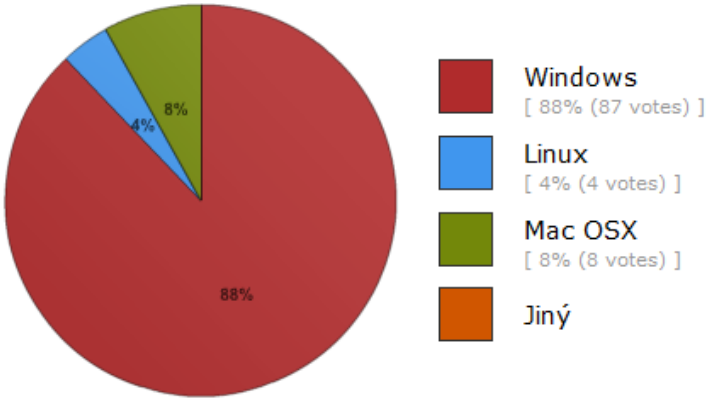
Jako první úkol v praktické části jsem zhotovil veřejnou anketu, která mi pomohla zjistit podvědomí širší veřejnosti o bezpečnosti počítačů. Zvolil jsem dotazník internetovou formou, konkrétně jsem si zvolil stránku http://twtpool.com (http://twtpoll.com/g53byb), která je sice v anglickém jazyce, ale za to nabízí zdarma široké možnosti nastavení dotazníků či případně anket. Dotazník byl posléze nabídnut lidem na 2 nejpoužívanějších sociálních sítích. Asi 180 lidem na síti Twitter, kde se celkově asi nachází lidé více znalejší této problematiky, a 200 lidem na síti Facebook, kde se nachází většinou spíše laická veřejnost. Celkově na dotazník odpovědělo 99 dotázaných a jejich demografické informace si můžeme prohlédnout na následujícím obrázku. Nahoře najdeme rozdělení pohlaví dotázaných a dole jejich věk. Na dalších stránkách vysvětlím, jaký přínos pro mou práci měla každá otázka.



Obrázek 1 – Demografické informace k účastníkům ankety

Otázka č. 1 – Jaký na svém počítači používáte operační systém?

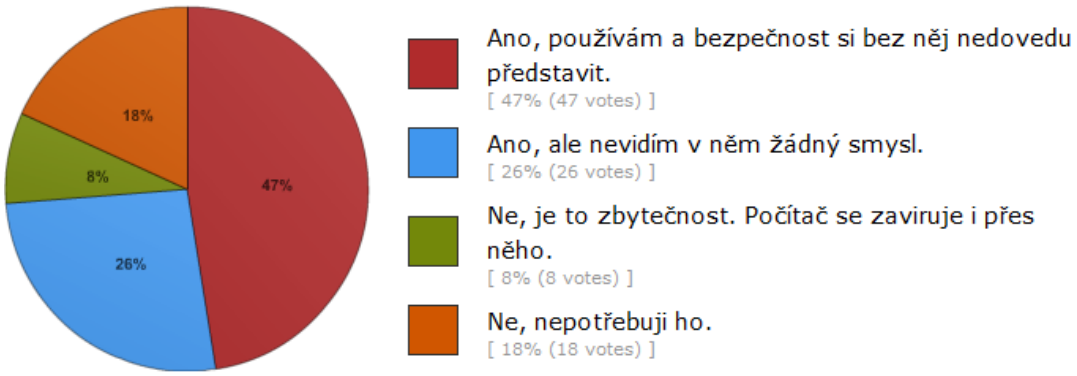
První otázkou jsem se chtěl ujistit, zda je dobře zvoleno téma práce, kde se věnuji zrovna operačnímu systému Microsoft Windows. Dotazník potvrdil, že drtivá většina uživatelů využívá právě tento systém.



Obrázek 2 – Graf odpovědí na otázku číslo 1

Otázka č. 2 – Používáte antivir? Myslíte si, že má nějaký smysl?

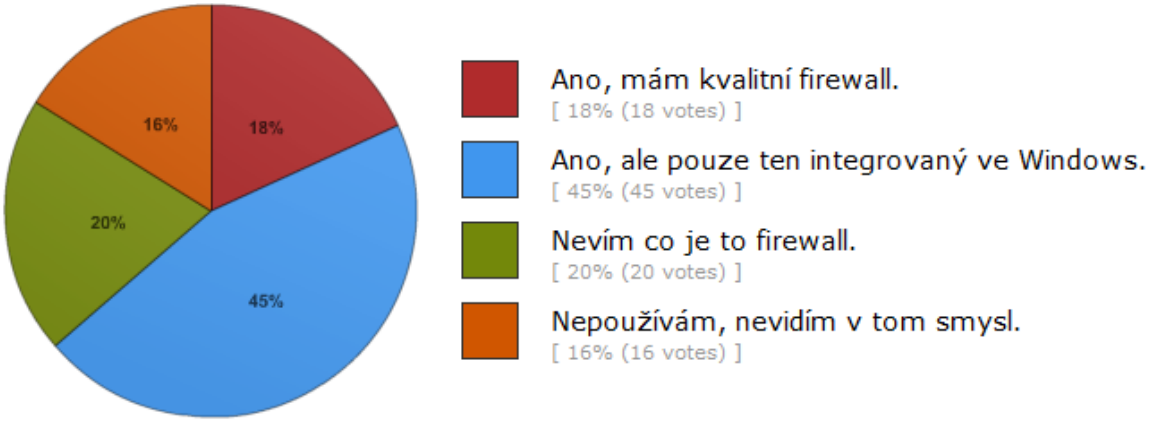
Otázka na antivirový software. Ukázalo se, že více než polovina dotázaných nevěnuje používání či konfigurování antiviru dostatečnou pozornost.



Obrázek 3 – Graf odpovědí na otázku číslo 2

Otázka č. 3 – Používáte Firewall?

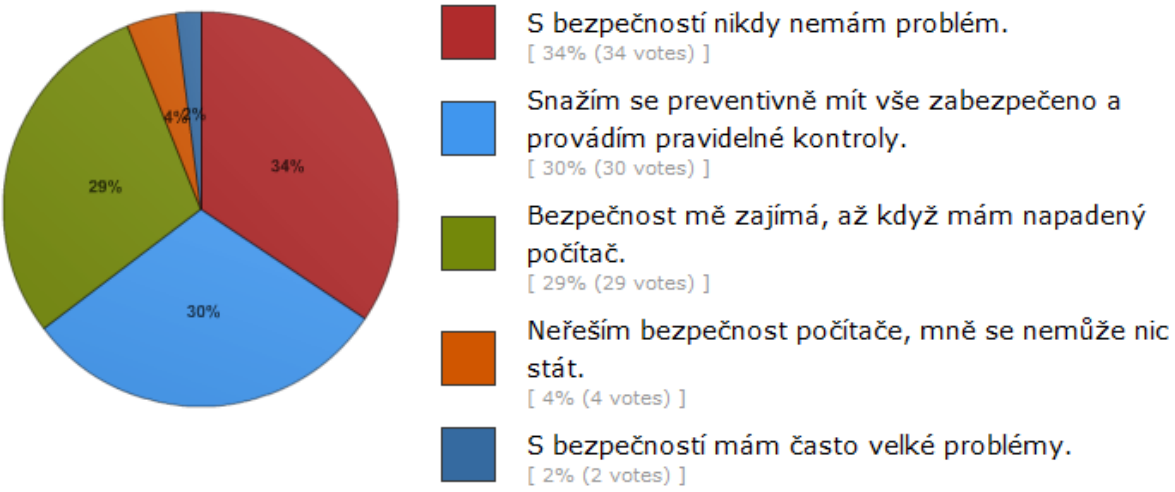
Při otázce na firewall se ukázala první velká kritická chyba veřejnosti. Přes 80 % dotázaných nepoužívá kvalitní a dostatečně nakonfigurovaný firewall, který je základem počítačového zabezpečení.



Obrázek 4 – Graf odpovědí na otázku číslo 3

Otázka č. 4 – Co vy a bezpečnost vašeho počítače?

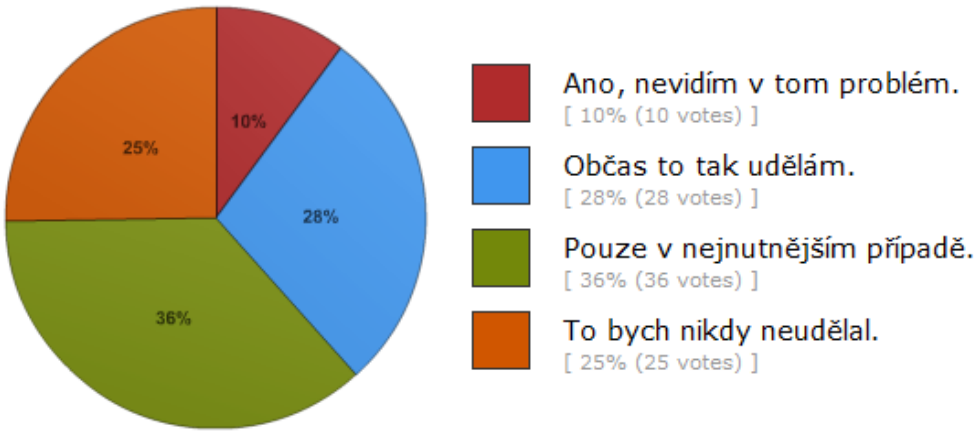
Výsledek otázky ohledně zájmu uživatelů o bezpečnost počítače mě celkem překvapil. Pouze třetina dotázaných bezpečnost neřeší nebo k ní nepřistupuje správným způsobem.



Obrázek 5 – Graf odpovědí na otázku číslo 4

Otázka č. 5 – Přihlásíte se ve veřejné Wi-Fi síti do internetového bankovnictví nebo e-mailové schránky?

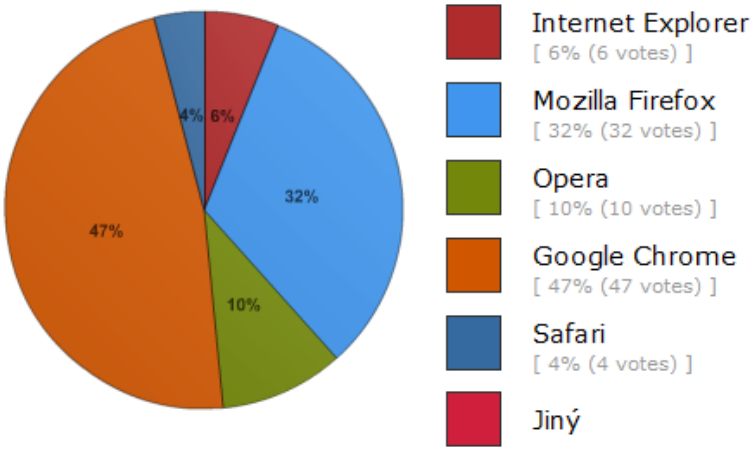
Druhá velká bezpečnostní chyba. Každý druhý uživatel se klidně přihlásí s citlivými údaji do otevřené bezdrátové sítě a „nabídne“ je tak prakticky komukoliv.



Obrázek 6 – Graf odpovědí na otázku číslo 5

Otázka č. 6 – Jaký používáte webový prohlížeč?

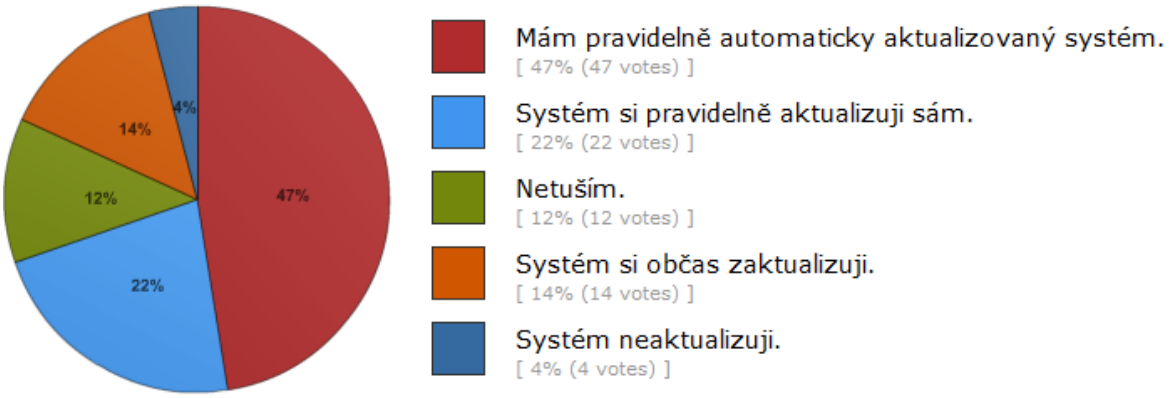
Dotaz na prohlížeče potvrdil, že Internet Explorer, dlouhá léta označovaný za nejméně bezpečný webový prohlížeč, je čím dál více na ústupu a uživatelé raději využívají alternativní a bezpečnější software.



Obrázek 7 – Graf odpovědí na otázku číslo 6

Otázka č. 7 – Co vy a aktualizace operačního systému?

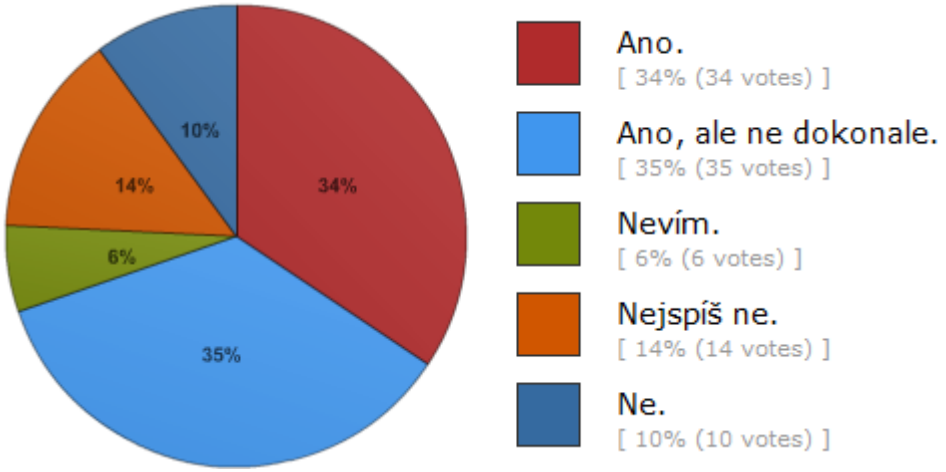
Další velká bezpečnostní chyba. Až třetina uživatelů se nijak nestará o to, aby jejich systém byl zabezpečen nejnovějšími aktualizacemi. Usnadňují tak cestu případným útočníkům.



Obrázek 8 – Graf odpovědí na otázku číslo 7

Otázka č. 8 – Dokážete si, dle svého názoru, zabezpečit počítač?

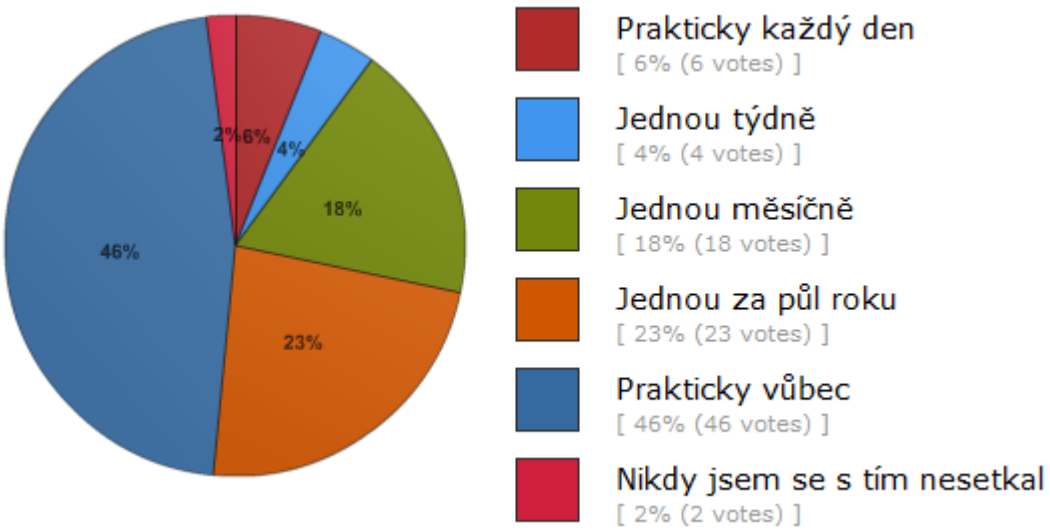
Otázka na schopnost zabezpečit si systém. Většina uživatelů si nějakým způsobem dokáže zabezpečit svůj systém, což je určitě pozitivní zjištění.



Obrázek 9 – Graf odpovědí na otázku číslo 8

Otázka č. 9 – Jak často se setkáváte s viry a jinými škodlivými programy?

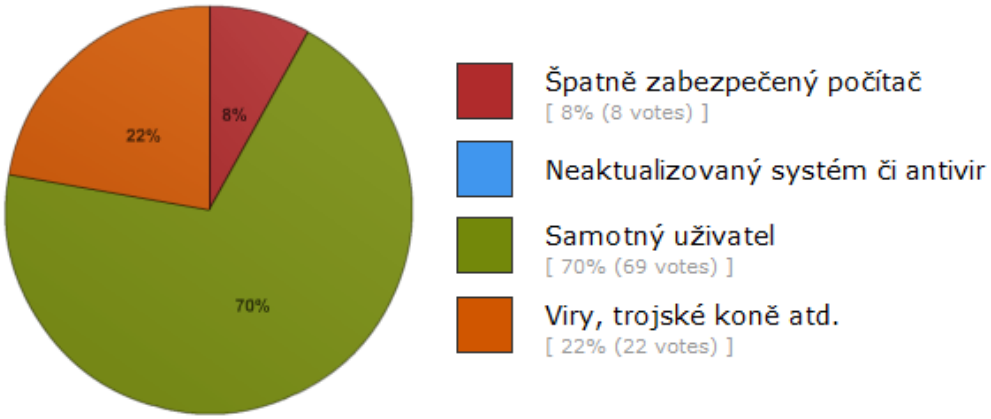
Dotaz na viry dopadl podle mého názoru s velmi překvapivými výsledky. Drtivá většina uživatelů se se škodlivým softwarem prakticky nesetkává. Což určitě neodpovídá jeho množství všude kolem.



Obrázek 10 – Graf odpovědí na otázku číslo 9

Otázka č. 10 – Co je podle vás z následujícího největší nebezpečí pro počítač?

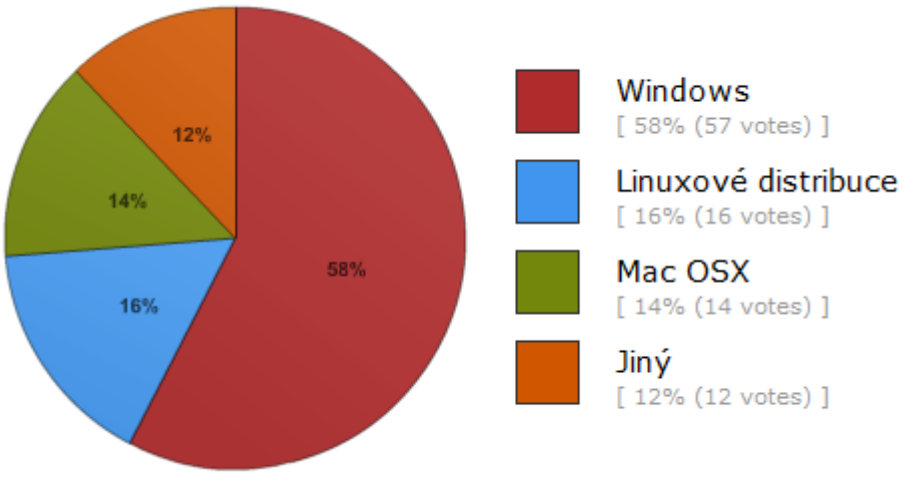
Většina dotázaných si správně uvědomuje, že největší podíl na bezpečném systému visí na samotném uživateli.



Obrázek 11 – Graf odpovědí na otázku číslo 10

Otázka č. 11 – Který operační systém je podle vás považován za nejméně bezpečný?

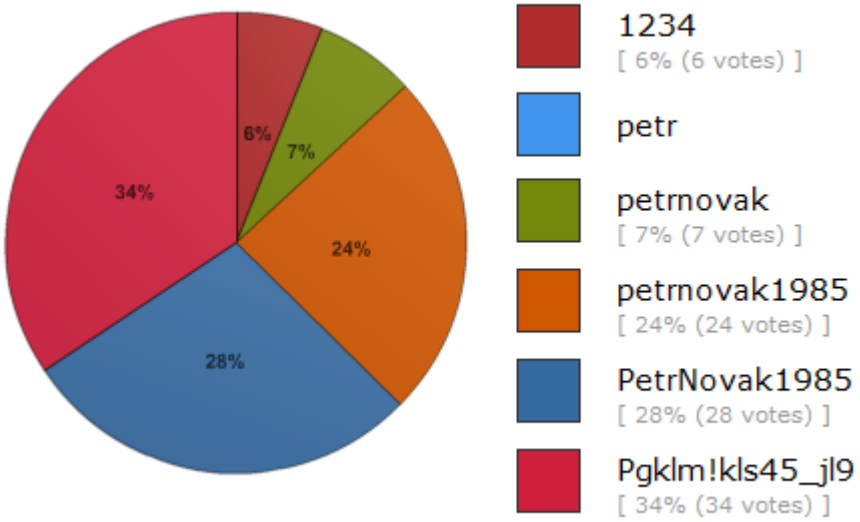
I v této otázce systémy Windows potvrdily svou pověst nejméně bezpečného operačního systému.



Obrázek 12 – Graf odpovědí na otázku číslo 11

Otázka č. 12 – Jakého typu používáte hesla?

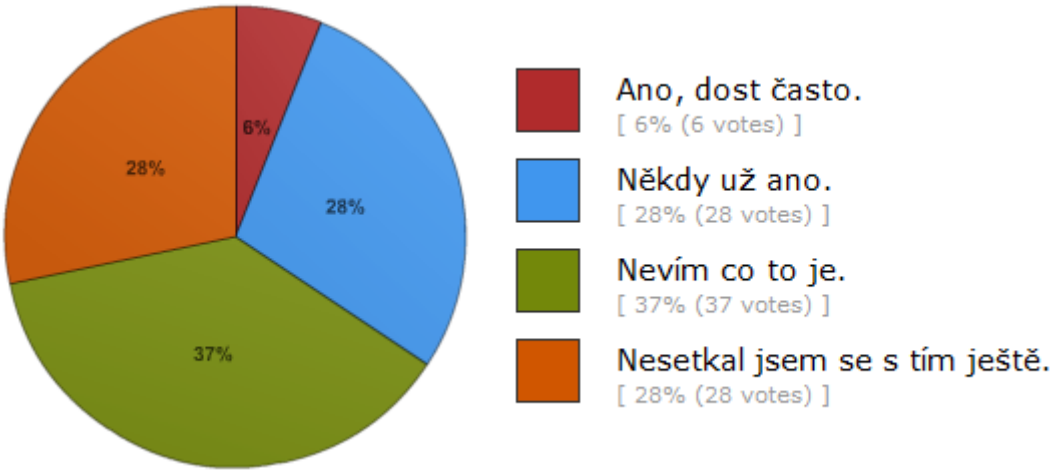
Možná největší zjištěné bezpečnostní pochybení. Pouze každý třetí uživatel používá hesla podle bezpečnostních zásad.



Obrázek 13 – Graf odpovědí na otázku číslo 12

Otázka č. 13 – Setkali jste se někdy se sociálním inženýrstvím?

Tato otázka přinesla zjištění, že více než třetina dotázaných neví, co vůbec znamená největší hrozba pro nejdůležitější článek zabezpečení počítače - samotného uživatele.



Obrázek 14 – Graf odpovědí na otázku číslo 13

Otázka č. 14 – Jste si vědomi možných rizik při používání sociálních sítí?

Další velké bezpečnostní pochybení na závěr. Polovina dotázaných si není vědoma nebo ignoruje velká bezpečnostní rizika spojená s používáním sociálních sítí.

Obrázek 15 – Graf odpovědí na otázku číslo 14

6 ZABEZPEČENÍ PŘI INSTALACI SYSTÉMU

Při instalaci systému Windows 7 jsou z bezpečnostního hlediska důležité tři věci:

1) Před instalací systému je velmi dobré si rozdělit pevný disk na více oddílů, pokud nepoužíváte více pevných disků, a systém instalovat na oddíl jemu vyhrazený, který nebude stejný, jako ten, na který budeme ukládat svá data. Toto uživatelé ocení hlavně v případě havárie systému, kdy přijdou „pouze“ o systém, ale data budou mít v pořádku na jiném oddíle.
2) Při formátování disku před instalací je z hlediska bezpečnosti lepší volit formát NTFS než FAT32. To platí především u systému Windows XP, jelikož v systému Windows 7 je již standardně NTFS. Použití NTFS nám zajistí vyšší bezpečnost při zabezpečení souborů a složek.
3) Před spuštěním systému si můžeme nastavit heslo v BIOSu, které po nás bude počítač při každém spuštění vyžadovat. Do BIOSu se obvykle dostaneme stisknutím klávesy *DEL* hned po startu počítače. Najdeme si kartu *BOOT* a následně *Security*, kde můžeme v kolonce *Change supervisior password* heslo nastavit. Názvy uvádím podle mé základní desky, u BIOSů jiných základních desek se názvy mohou mírně lišit.

6.1 Zabezpečení po instalaci systému

Systém po instalaci vyžaduje následující 2 základní bezpečnostní věci:

1) Vytvoření administrátorského účtu a nastavení jeho hesla

Vytvoření dostatečně silného a bezpečnostního hesla je základ všech bezpečnostních nastavení. Většina uživatelů hesla moc rádi nemají, a proto nepoužívají žádná, nebo velmi jednoduchá.

Zásady silného hesla:

- Nepoužívat slova, které lze najít v jakémkoliv slovníku.
- Nepoužívat jména domácích zvířat, příbuzných, osobní data (narozenin) a jiné, zvláště nepoužívat své vlastní jména, ať už reálná nebo přihlašovací.
- Zpravidla platí, že čím více „nesmyslné“ heslo, tím více bezpečnější.

- Mít heslo uchované pouze v hlavě a nikde si ho nezapisovat.
- Snažit se vytvořit si co nejsilnější heslo.
- Nepoužívat jednoduché kombinace typu „12345678“ nebo „qwertzuiop“.
- Neměli bychom používat stejné heslo na více důležitých místech.
- Heslo by mělo být požadováno u každého účtu.

Jak by mělo vypadat silné heslo:

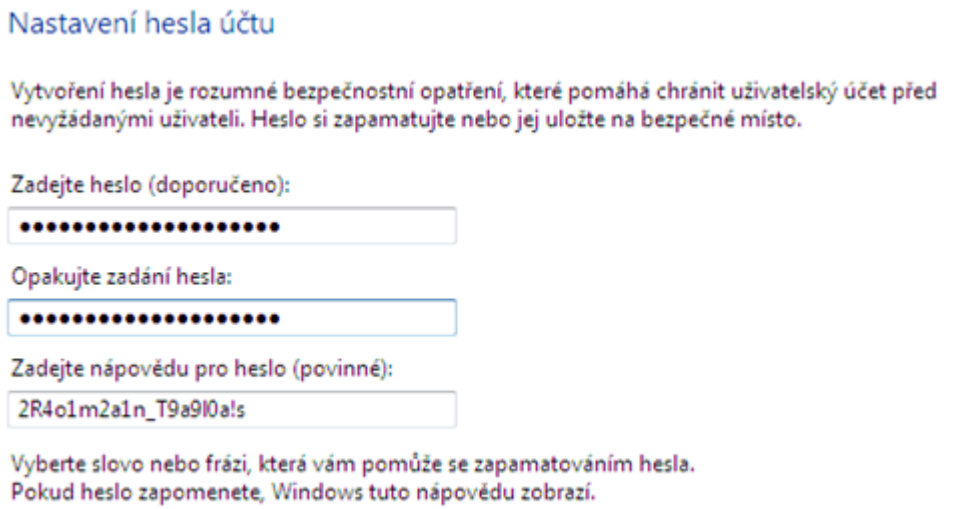
- Obsahovat minimálně 8 znaků, nejlépe ale 15 znaků a více.
- Obsahovat kombinaci malých a velkých písmen, číslic a speciálních symbolů (,._!“?$...).
- Mělo by se v pravidelných intervalech měnit.
- Nemělo by obsahovat v žádné formě naše uživatelské jméno a podobné údaje.
- Nesmí být s nikým sdíleno.

Složitá hesla se sice špatně prolamují, ale stejně tak i špatně pamatují. Proto je dobré používat nějaký efektivní systém. Nejčastěji se používá systém následující:

1) Vybereme si větu: „Skákal pes, přes oves, přes zelenou louku.“
2) Z počátečních písmen vytvoříme heslo: „Sp,po,pzl.“
3) Zvýšíme složitost hesla přidáním libovolných číslic a speciálních znaků:

   „1Sp!,5po?,9pzl.!“
4) Heslo otestujeme některým webovým nástrojem pro kontrolu síly hesla. Třeba přímo na stránkách Microsoftu na adrese http://www.microsoft.com/cze/athome/security/privacy/password_checker.mspx.

Výše uvedené je pouze příklad. Zde uvádím praktičtější způsob použití, když jsem použil mé jméno (Roman Talaš) a smyšlené datum narození (24. 12. 1990):



Obrázek 16 – Nastavení hesla účtu

Mnou vykombinované heslo je v čitelné podobě napsané v nápovědě pro heslo, kterou systém taky nabízí. Můžete si zde napsat něco, co vám v případě zapomenutí hesla pomůže při jeho vzpomínání. Pamatujte však, že když to pomůže vám, může to pomoci i útočníkům. Případně, pokud si nejste jisti svým zvoleným heslem, lze na Internetu najít spoustu nástrojů na vygenerování silného hesla. Jednoduchým a zároveň velmi dobrý nástroj najdeme například na stránkách http://www.generator-hesel.cz.

2) Vybrání typu sítě

Zde vyberte podle popisu typ sítě, ve které se zrovna nacházíte. Na výběr máte *Domácí, Pracovní* či *Veřejnou síť*. Slouží to k nastavení základní úrovně zabezpečení. Protože se s největší pravděpodobností v době instalací nacházíte ve svém domově, vyberte možnost *Domácí síť*.

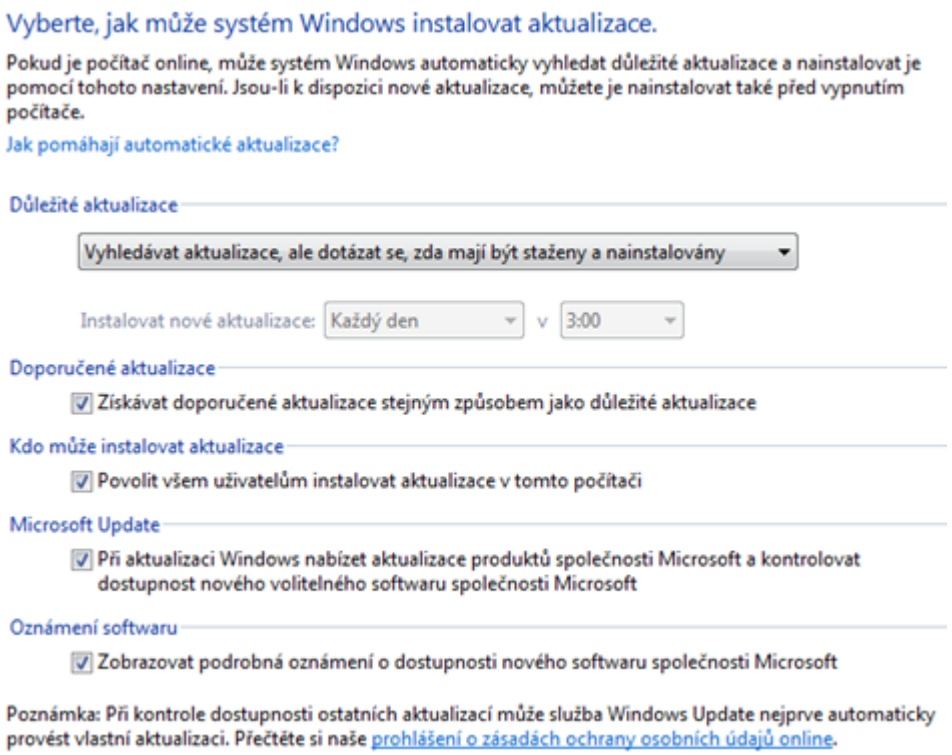
7 PRVNÍ BEZPEČNOSTNÍ KROKY PO NAINSTALOVÁNÍ SYSTÉMU

Než vůbec čerstvě nainstalovaný systém začnete používat a vůbec než vkročíte na Internet, musíte provést následující opatření. Všechny kroky lze provádět přes *Centrum akcí*, které lze nalézt zde: *Start* > *Ovládací panely* > *Systém a zabezpečení* > *Centrum Akcí*

Všechna upozornění *Centra akcí* lze vždy sledovat v pravém spodním rohu.

7.1 Aktualizace systému Windows 7

Zde si všimneme, že automatické aktualizace nejsou zapnuté, tudíž je příslušným tlačítkem zapneme, nebo ještě lépe zvolíme vlastní nastavení, podle svých vlastních potřeb. Nastavení si skutečně můžete zvolit podle vlastních potřeb. Pamatujte ovšem, že všechny *Důležité aktualizace* je NUTNÉ vždy instalovat a je taky velmi doporučováno instalovat všechny *Doporučené aktualizace*.



Obrázek 17 – Nastavení aktualizací

Po nastavení necháme systém vyhledat všechny aktualizace a poté je nainstalovat. Nemusíme se obávat instalovat všechny nalezené aktualizace. Služba Windows Update je poměrně inteligentní a bezpečná, a tak by žádná z aktualizací by neměla nijak vašemu

systému ublížit. Neaktualizovaný operační systém by opravdu nikdo mít neměl. Je doslova zbytečné takto otevírat útočníkům cestu do systému.

7.2 Antivirová ochrana

Jak už bylo řečeno dříve, systém nemá žádný integrovaný antivirový program. Občas se ale stane, že služba *Windows Update* nabídne instalaci software *Microsoft Security Essentials.* Pokud se tak však nestane, můžeme si jej stáhnout ze stránek Microsoftu na adrese http://www.microsoft.com/downloads/cs-cz/details.aspx?FamilyID=e1605e70-9649-4a87-8532-33d813687a7f, a poté jej nainstalovat. Po jednoduché instalaci nám software nahlásí neaktuální databázi, je nutné jej tedy *Aktualizovat.* Jaké jsou možnosti programu?

a) Kolonka *Domů* – Zde můžeme vidět, zda je software aktualizován, zda je náš systém momentálně chráněn, kdy byla provedena poslední kontrola a můžeme si naplánovat čas pravidelné kontroly počítače. Samozřejmostí je zde možnost okamžité kontroly a to buď *Rychlé* (inteligentním skenovacím mechanismem), *Úplné* (software proskenuje každý soubor) nebo *Vlastní,* kdy si uživatel zvolí, které části systému chce prověřit. Je dobré mít nastavenou co nejširší pravidelnou kontrolu alespoň jednou týdně.

b) Kolonka *Aktualizovat* – Tady najdeme pouze možnost aktualizace virové databáze a informace o poslední aktualizované databázi.

c) Kolonka *Historie* – Zde najdeme všechny nebezpečné položky, které jsme kdy v systému měli, roztříděné do kategorií *Všechny položky, Všechny položky v karanténě* a *Pouze povolené položky.*

d) Kolonka *Nastavení* - Zde najdeme všechny možnosti konfigurace programu:

e) *Naplánovaná kontrola* – Zde si nastavíme čas pravidelné kontroly systému a její podrobnosti, jako je např. procento využití výkonu procesoru. Jak už jsem řekl dříve, je dobré nastavit si pravidelnou kontrolu alespoň jednou týdně.

f) *Výchozí akce* – Zde si můžeme nastavit chování programu při nalezení potencionálního nebezpečí. Podle úrovně jednotlivých výstrah (nízká až závažná) zvolíme buď *Doporučenou akci,* tudíž necháme výběr na programu, *Odebrat soubor,* kdy dojde k odstranění souboru a nebo *Vložit do karantény,*

kdy se soubor přesune do prostoru, kde už s ním není možné pracovat. Zde bych z pohledu běžného uživatele nechal všude volbu *Doporučená akce*.

g) *Ochrana v reálném čase* – Zde si nastavíme, zda necháme software kontrolovat systém neustále, jaké druhy souborů má sledovat, zda příchozí nebo odchozí, a jestli taky monitorovat chování uživatele a případně ho upozornit na podezřelou aktivitu. V tomto případě je nutné nechat kontrolu v reálném čase zapnutou, stejně jako všech souborů či síťových připojení.

h) *Vyloučené soubory a umístění* – Zde si můžeme nastavit složky či soubory, které nechceme zahrnout do kontroly programu. Nedoporučuji si zde něco přidávat, nebezpečný software se může nacházet kdekoliv.

i) *Vyloučené typy souborů* – Zde si můžeme nastavit přípony od souborů, které nechceme zahrnout do kontroly programu. Opět nedoporučuji si zde něco přidávat, nebezpečný software se může nacházet kdekoliv.

j) *Vyloučené procesy* – Zde si můžeme nastavit všechny procesy, které nechceme zahrnout do kontroly programu. Znovu nedoporučuji si zde něco přidávat, nebezpečný software se může nacházet kdekoliv.

k) *Upřesnit* – Zde najdeme rozšířená nastavení, např. zda vytvářet při kontrolách *Bod obnovení* nebo jak dlouho uchovávat soubory v karanténě. Zdejší nastavení už je spíše na preferencích uživatele, ale rozhodně neuškodí pravidelně kontrolovat archivované soubory a vyměnitelné jednotky.

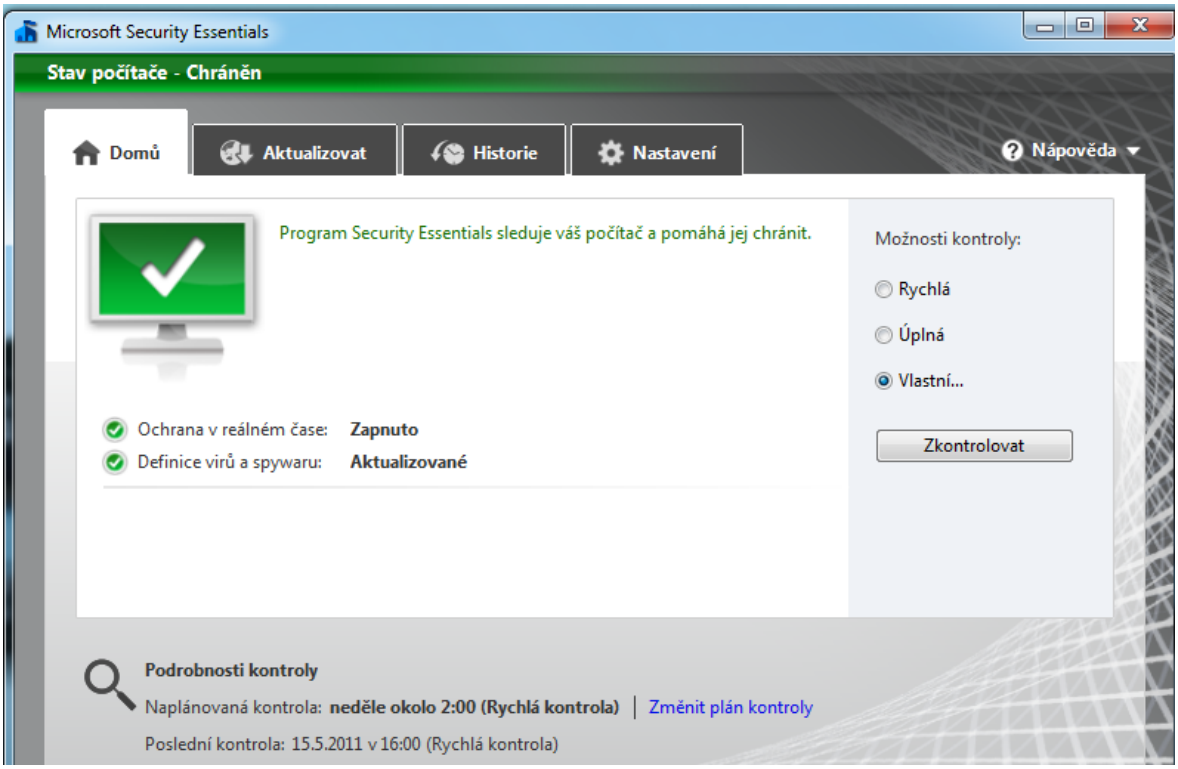
l) *Microsoft SpyNet* – Nastavení služby či spíše internetové komunity, která pomáhá uživatelům při reakcích na nalezená nebezpečí.

Obecné rady při nalezení škodlivého programu:

- Přečtěte si informace, kterým rozumíte z těch, které vám program nabízí.
- Hledejte na Internetu informace o vaší hrozbě a řiďte se podle důvěryhodných informací. Pozor, někdy se může stát, že za škodlivý bude prohlášen i plně důvěryhodný a bezpečně pracující program!

Program Microsoft Security Essentials je velmi dobrý antivirový software poskytovaný zdarma, jehož kvality dokazují i nezávislé srovnávací testy. Samozřejmě si můžete zvolit jakýkoliv jiný antivirový software, pokud uznáte, že jeho kvality jsou lepší a nevadí vám

případná investice do jeho koupě. Podle posledních testů v době psaní této práce byly jako nejlepší ohodnoceny programy následujících firem: F-Secure, Symantec, Avira, Kaspersky a ESET. Dají se však sehnat i velmi dobré antiviry v plné verzi zdarma. Takovým je například antivirus ClamWin.



Obrázek 18 – Prostředí programu Microsoft Security Essentials

7.3 Konfigurace brány Windows Firewall

Stejně jako předchozí aplikace, tak i bránu Windows Firewall nalezneme v *Centru akcí*. Tento program nabízí jednoduché rozhraní s přehledným ovládáním, které zvládne každý běžný uživatel. Veškeré položky menu aplikace najdeme v levém sloupci. Jsou jimi:

a) *Zapnout nebo vypnout bránu Windows Firewall* – Zde si můžeme jednoduše zvolit, zda chceme bránu Windows Firewall mít zapnutou, či nikoliv. V případě zapnutí můžeme ještě navolit možnost zablokování všech příchozích připojení a možnost upozornění pro uživatele nových blokovaných programů. Správně by se zde měla nechat brána Windows Firewall zapnutá v obou typech sítí, jak domácích, tak veřejných a blokování všech příchozích spojení povolit pouze v případě, pokud je váš počítač již napaden nebo chcete zvýšit bezpečnost na maximální úroveň.

b) *Povolení průchodu bránou Windows Firewall* – Zde nalezneme seznam všech povolených programů a funkcí systému, které mají povolený průchod skrz bránu Windows Firewall. Tady bychom měli mít zaškrtnuté pouze programy, které opravdu potřebujeme, jelikož každé další zaškrtnuté políčko znamená taky zvýšené nebezpečí. Dále si zde můžete přidat kterýkoliv program, který chcete nebo potřebujete. Nejčastěji se to dělá tak, že po spuštění konkrétního programu se vás systém zeptá na jeho nastavení a povolení přístupu.

Zde si ovšem vždy dobře přečtěte, co vám systém oznamuje a dejte si velký pozor zejména na následující fakta:

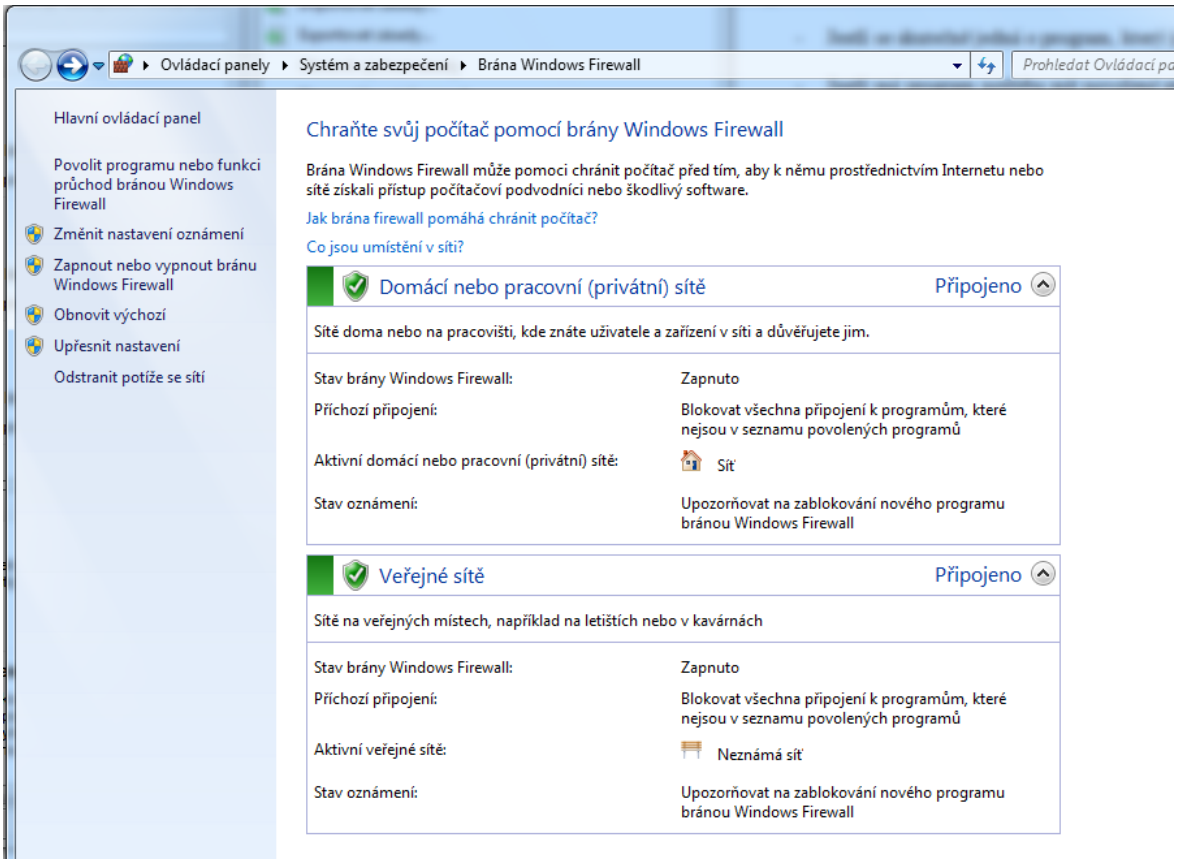
- Jestli se skutečně jedná o program, který jste spustili a nainstalovali
- Jestli má program potřebu mít povolené příchozí spojení
- Jestli může mít program vždy povolené spojení v momentálním typu sítě

Pokud si nejste u všech bodů jistí s kladnou odpovědí, přístup raději nepovolujte. Dále se můžou přidávat povolené programy přes tlačítko *Povolit jiný program*.

c) *Obnovení výchozích nastavení* – Zde se můžete kdykoliv vrátit k původnímu způsobu konfigurace, pokud bude cítit tu potřebu. Pamatujte však, že tím odstraníte všechna pravidla, která jste do té doby nastavili.

d) *Upřesnit nastavení* – Zde už najdeme ty nejpokročilejší nastavení a taky se zde dají konfigurovat brány Windows Firewall na vzdálených pracovních stanicích. Konkrétně se tu jedná o modul snap-in s předdefinovanou konzolí MMC. Přes všechna složitá nastavení zde nalezneme jednoduché a přehledné rozhraní. I přesto je ale tato konzole určena spíše zkušenějším uživatelům. A ti nejzkušenější můžou využít i příkazové řádky příkazem **netsh advfirewall**.

Přestože se brána Windows Firewall každou verzí hodně zlepšuje, pořád nedosahuje svého jména („ohnivá zeď“). Pokud tedy myslíte bezpečnost svého počítače vážně, mohli byste se poohlédnout po alternativách od jiných výrobců. Na druhou stranu kvalitní a profesionální firewall není vůbec levná záležitost. Opět se samozřejmě ale dají sehnat i neplacené varianty. Špičkou tady je firewall od firmy Comodo.



Obrázek 19 – Prostředí programu Windows Firewall

7.4 Windows Defender

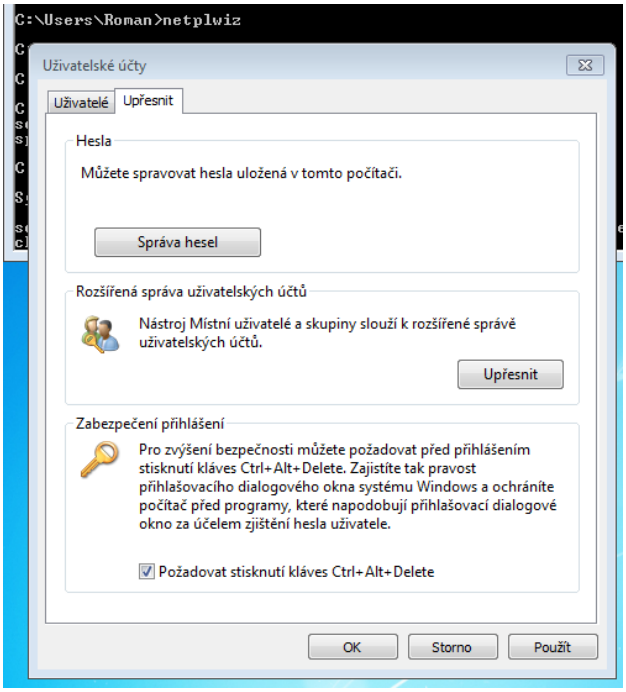
Windows Defender je v systému jako antispywarová ochrana. Pracuje tak, že software, u kterého je naprosto jasné, že se jedná o spyware, odstraní nebo přesune do karantény. Ostatní software, u kterého to tak jasné není, spadá do tzv. „šedé zóny“ a řada přichází na uživatele, které vybere akci, která se má se souborem provést.

Program běží jako služba, může jej tedy využívat každý uživatel počítače. Jinak je Windows Defender programem hodně podobným Microsoft Security Essentials. Není divu, vždyť z něho Microsoft Security Essentials vychází. V případě, že již máte nainstalovaný Microsoft Security Essentials, tak máte Windows Defender vypnutý a je dost možné, že vám zapnout nepůjde. Jelikož ale Microsoft Security Essentials má v sobě i antispywarovou ochranu, tak se nejedná o nic hrozného. Jinak zde není potřeba uvádět nějaká větší doporučení, jelikož jsou prakticky totožná s těma u Microsoft Security Essentials.

8 UŽIVATELSKÁ ZABEZPEČENÍ

Doposud jsme pracovali s administrátorským účtem vytvořeným hned na začátku instalace systému. Účet s tolika oprávněními je pro běžnou každodenní práci nepotřebný a zbytečně tak o něco zvyšuje možnosti útočníka při vstupu do systému. Proto je velmi dobré si vytvořit nový standardní účet, který budeme používat, bez administrátorských oprávnění. Práva tohoto účtu jsou nastavena tak, aby uživatele nijak neomezovala v běžné práci, a pokud i přesto budete chtít spustit nějaký program jako správce, můžete tak kdykoliv učinit přes kliknutí pravým tlačítkem a volbu *Spustit jako správce*. Nový účet vytvoříme následovně přes tento nástroj:

Start > *Ovládací panely* > *Uživatelské účty a zabezpečení rodiny* >*Uživatelské účty* > *Spravovat účty* > tlačítko *Vytvořit nový účet*.



Obrázek 20 – Nastavení zabezpečení přihlášení

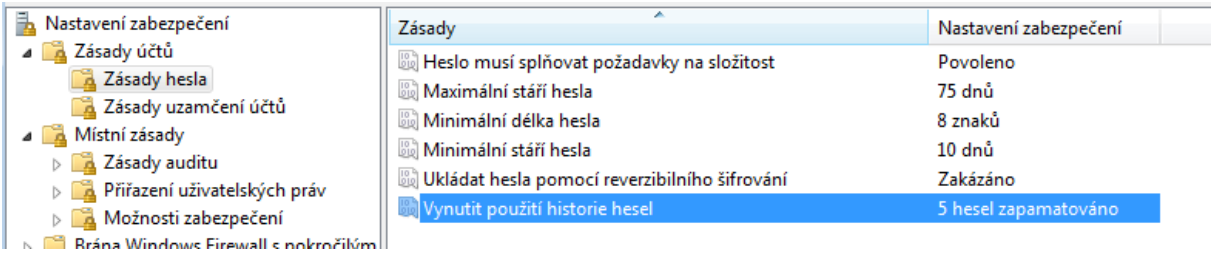
Poté na nově vytvořený účet klikneme a tlačítkem *Vytvořit heslo* k němu přidáme heslo podle již uvedených zásad. Každý účet musí být bezpodmínečně chráněn heslem. Abychom zvýšili bezpečnost jednotlivých účtů, přejdeme do pokročilejšího nastavení zadáním příkazu *netplwz* v příkazové řádce. Zde si opět můžeme vytvářet či odstraňovat účty, měnit hesla nebo organizovat účty do různých skupin. Nás bude zajímat karta *Upřesnit*. Na ní zaškrtneme možnost *Požadovat stisknutí kláves Ctrl+Alt+Del*, které chrání před programy napodobující přihlašovací okna s účelem sejmutí hesla uživatele.

Dále si můžete zapnout účet *Guest* neboli účet hosta, který můžete potřebovat, např. pokud k nám občas přijde na počítač nějaká návštěva, která při práci s ním nepotřebuje prakticky žádná oprávnění. Toto ale moc nedoporučuji. Lepší je si vytvořit zvláštní účet pro tyto příležitosti, ve kterém si nakonfigurujete všechna omezení podle svých představ.

Nyní stiskneme klávesy *WIN* + *R* pro spuštění služby *secpol.msc*, která spustí *Místní zásady zabezpečení* a kde nastavíme ta nejpodrobnější zabezpečení účtů. Zajímá nás následující:

a) *Zásady účtů >Zásady hesla*

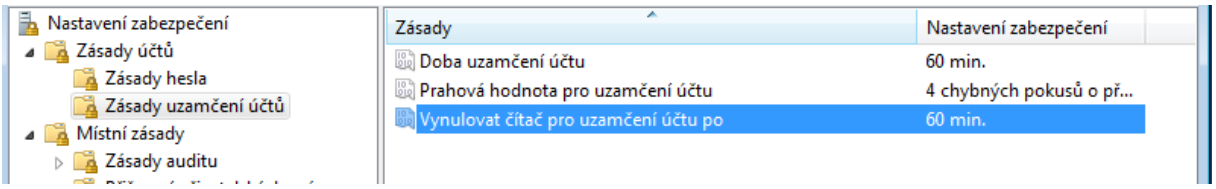
Zde zapneme funkci *Heslo musí splňovat požadavky na složitost*, což nám zajistí silná hesla u všech uživatelů. Dále nastavíme *Minimální stáří hesla* alespoň na několik dní, než si může uživatel změnit své heslo na nové, protože není zase dobré měnit heslo každou chvíli, a *Maximální stáří hesla*, které nám udává dobu, po které bude systém po uživateli vyžadovat změnu. Zde si nastavte dobu, kterou podle svého uvážení považujete za vhodnou, já osobně bych doporučil 3 měsíce. Funkci *Ukládat hesla pomocí reverzního šifrování* můžete nechat vypnutou, jelikož se v dnešní době jedná o prakticky již nepotřebnou technologii. V kolonce *Vynutit použití historie hesel* doporučuji nastavit alespoň hodnotu 5. Budeme tím mít zajištěno, že nové heslo uživatele bude odlišné od předchozích pěti. A nakonec poslední a možná nejdůležitější kolonka, kterou je *Minimální délka hesla*. Zde se musí nastavit hodnota alespoň 8 znaků, ovšem čím více, tím lépe.



Obrázek 21 – Nastavení zásad hesla

b) *Zásady účtů >Zásady uzamčení účtů*

Zde nastavíme především *Prahovou hodnotu pro uzamčení účtu*, která nám udává počet možných pokusu k přihlášení. Doporučuji nastavit hodnotu na 3 nebo 4 pokusy. Pokud v tomto počtu nebude uživatel schopen vložit správné heslo, bude mu účet zamknut. Po jakou dobu, to nastavíme v kolonce *Doba uzamčení účtu*.



Obrázek 22 – Nastavení zásad uzamčení účtů

c) *Místní zásady >Zásady auditu*

Tato sekce slouží k monitorování činností uživatelů a z hlediska bezpečnosti je dobrá k tomu, že můžeme vidět, co který uživatel prováděl v systému a kde tedy může hrozit nějaké nebezpečí. Můžeme sledovat používání oprávnění; přístupy k objektům, službám, procesům; přihlášení; správu účtů; systémové události nebo změny zásad zabezpečení.

d) *Místní zásady >Přiřazení uživatelských práv; Místní zásady > Možnosti zabezpečení*

Zde nalezneme velkou spoustu funkcí, kde každé z nich můžeme přiřadit skupinu uživatelů, která ji může provádět. Jelikož se jedná už o složitější nastavení systému určené hlavně pro zkušené uživatele, nebudu je tu rozebírat dopodrobna. Jako příklad uvedu funkci *Přístup k počítači přes síť*, kterou mají standardně povolenou všechny skupiny. Pokud nechceme u některé skupiny přístup přes síť, jednoduše ji z povolených skupin odstraníme.

Dále zde přes tuto službu ještě spoustu dalších různých nastavení, jako např. podrobná nastavení brány Windows Firewall nebo bezpečnostní zásady omezení při používání softwaru. Všechna tato nastavení jsou ale opět určena hlavně velmi zkušeným uživatelům.

8.1 Rodičovská kontrola

Rodičovská kontrola je funkce systému, která umožňuje kontrolovat činnost dětí na počítači, blokovat programy či webové stránky, které nesmějí používat či navštěvovat. Stejně tak ale může program dobře posloužit při omezování práv dospělých uživatelů.

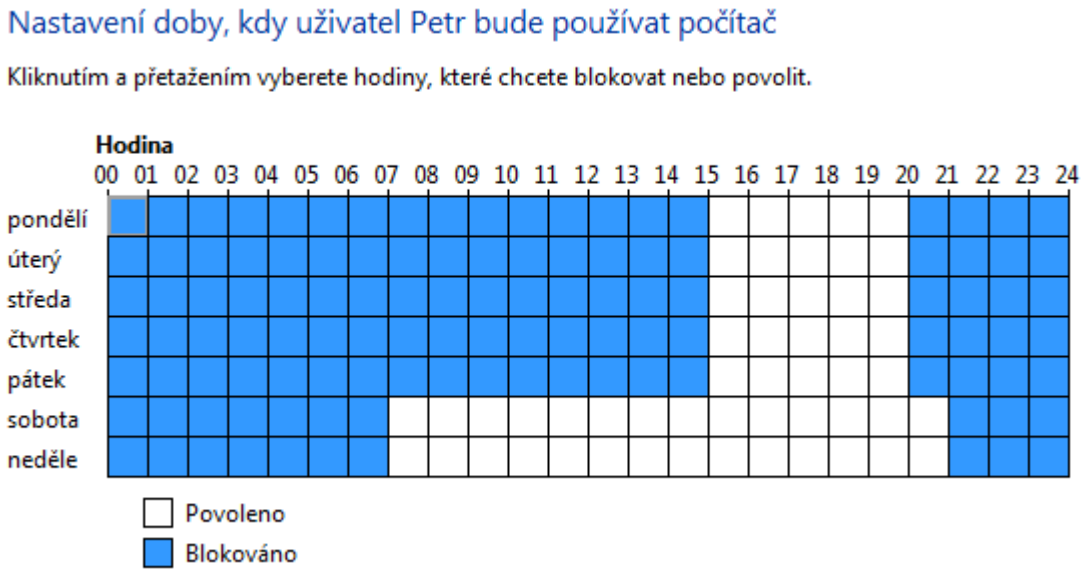
Nástroj otevřete následující cestou:

Ovládací panely >Uživatelské účty a zabezpečení rodiny>Rodičovská kontrola> Uživatelské ovládací prvky

Po výběru uživatelského účtu, který chceme kontrolovat, můžeme nastavit následující možnosti:

a) *Časové limity*

Zde si můžeme přesně nastavit, kterékoliv hodiny a kterýkoliv den může být uživatel přihlášen na počítači.



Obrázek 23 – Nastavení používání systému v rodičovské kontrole

b) *Hodnocení her*

Zde si nastavíme, zda uživatel může hrát hry. Pokud ano, tak jakého žánru a s jakým věkovým ohodnocením. Samozřejmě si lze nastavit ručně, které konkrétní hry uživatel hrát může a které ne.

c) *Omezení programů*

Zde si můžeme přes jednoduché nastavení vybrat zvolit všechny programy, které bude uživatel moci používat.

d) *Zablokování webových stránek*

Určitě nastane situace, kdy budete chtít některým uživatelům zablokovat přístup k určitým internetovým stránkám. Toto můžete nastavit i zde, kde je to ale spíš určené pro zabezpečení dětí a hlavně je vyžadován účet na službě Hotmail. Uvedení zablokování jiným způsobem je uvedeno v kapitole Internet Explorer.

8.2 Řízení uživatelských účtů (User Account Control)

Jedná se o nástroj systému, který slouží k varování před spouštěním určitého typu aplikací nebo při pokusu o nějaké změny v systému. Nejčastěji se setkáme s následujícími oznámeními:

- Žádost programu o povolení k činnosti
- Výzva k zadání pověření (pokud pracujeme pod standardním účtem a program vyžaduje oprávnění správce)
- Oznámení v červeném okně (Většinou značí ohrožení systému a aplikace, jejíž vydavatel je v počítači zablokován)
- Oznámení v oranžovém okně (Podepsaná aplikace, které ještě nebyla v systému vyjádřena důvěra)
- Oznámení v modrém okně (Aplikace, která je součástí systému Windows)
- Oznámení v šedém okně (Podepsaná aplikace, které je v systému vyjádřena důvěra)

Nastavení UAC můžeme provést zde:

Start > Ovládací panely > Uživatelské účty a zabezpečení rodiny > Uživatelské účty, kde vybereme možnost *Změnit nastavení nástroje řízení uživatelských účtů.* Máme na výběr ze 4 úrovní zabezpečení:

1) Nikdy uživatele neupozorňovat.
2) Upozorňovat uživatele pouze pokud se pokusím program provést změnu v systému.
3) Možnost podobná té uvedené výše, reaguje ale na více změn prováděných v systému.
4) Nejvyšší úroveň upozorňování. Nástroj dá uživateli vědět při každém pokusu nějakého programu provést změnu v systému, stejně tak jako při pokusu uživatele.

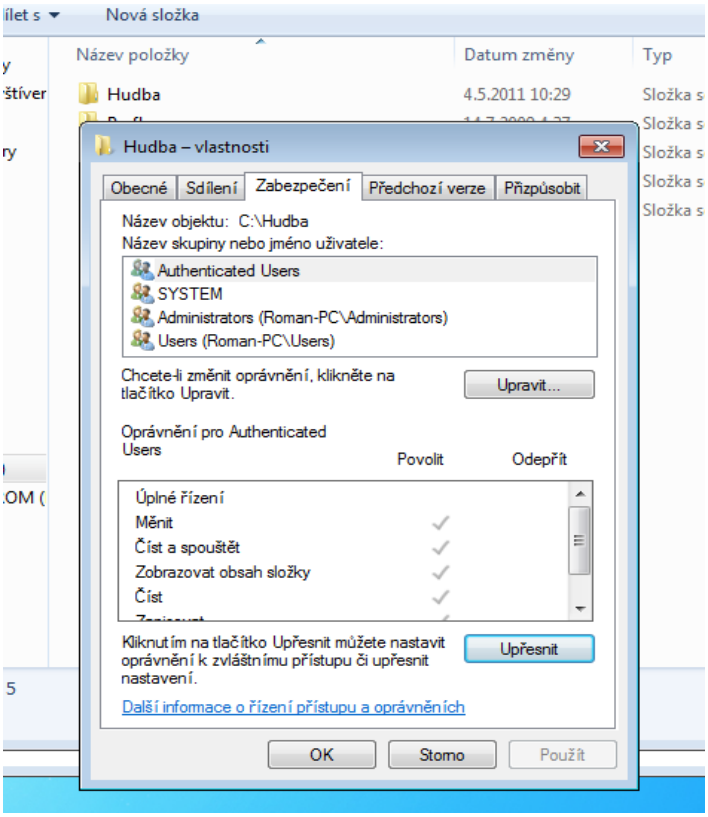
Zde nastavíme úroveň minimálně na třetí stupeň.

9 ZABEZPEČENÍ SOUBORŮ A SLOŽEK

U bezpečnosti souborů a složek nás zajímají především body uvedené v následujících podkapitolách.

9.1 Oprávnění

Může se stát, že k určitým složkám nebo souborům budeme chtít povolit přístup pouze určitým uživatelům, stejně jako možnost práce s nimi. Vše si můžeme jednoduše nastavit přes dialogové okno *Vlastnosti*, které najdeme po kliknutí pravým tlačítkem na požadovanou složku nebo soubor a najdeme si kartu *Zabezpečení*.



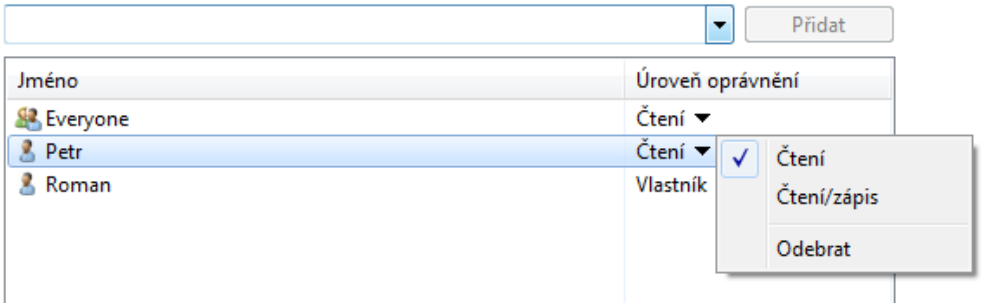
Obrázek 24 – Nastavení zabezpečení oprávnění přístupu do složek

Nyní vybereme skupinu uživatelů, jejíž oprávnění chceme měnit a klikneme na tlačítko *Upravit*. Teď už jenom jednoduchým zatržením políček ve sloupcích *Povolit* nebo *Odepřít* nastavíme atributy podle vlastních potřeb. Můžeme nastavit následující: *Úplné řízení, Měnit, Číst a spouštět, Zobrazovat obsah složky, Číst, Zapisovat a Oprávnění k zvláštnímu přístupu*.

Pokud bychom místa tlačítka *Upravit* klikli na tlačítko *Upřesnit,* vyskočí nám jiné dialogové okno s prakticky stejnými možnostmi, jenom se zde nachází více detailnějších atributů pro upřesnění oprávnění jednotlivých uživatelů. Dále si zde můžeme na dalších kartách nastavit auditování jednotlivé složky či soboru, nastavit jejich vlastníka nebo si přehledně zobrazit všechna oprávnění jednotlivých uživatelů.

9.2 Sdílení

Pokud budeme chtít nastavit složku či soubor jako sdílený v síti pro připojené počítače, musíme vše samozřejmě nastavit. Provedeme to pravým kliknutím na konkrétní složku nebo soubor a vyvoláním dialogového *Vlastnosti,* kde vybereme kartu *Sdílení*. Jako první klikneme na tlačítko *Sdílení…*, kde jednoduše přidáme uživatele nebo skupinu uživatelů, kteří sem budou mít přístup, a ještě nastavíme, zda dotyční budou mít pouze práva čtení nebo i zápisu. Po kliknutí na tlačítko *Sdílet* vše uložíme.



Obrázek 25 – Nastavení zabezpečení sdílení

V nově vyvolaném dialogovém oknu *Rozšířené možnosti sdílení* můžeme omezit maximální počet současně přistupujících uživatelů, v kolonce *Oprávnění* můžeme znovu poupravit pravomoc jednotlivých uživatelů a v kolonce *Mezipaměť* můžeme nastavit sdílení souborů v offline režimu.

9.3 Šifrování dat

Šifrování dat nám poslouží k tomu, aby se k důvěrným datům nikdo bez znalosti vašeho hesla nedostal a to ani v případě jejich odcizení. V systému Windows 7 máte v podstatě dvě možnosti zašifrování dat:

Systém EFS: Tento souborový systém zašifruje data tak, že se stanou čitelná pouze pro uživatele, kteří se přihlásí do systému pod vaším jménem a heslem. Použijeme jej tak, že

opět vyvoláme dialogové okno Vlastnosti dat, které chceme zašifrovat, a na kartě Obecné zvolíme Upřesnit a zaškrtneme položku Šifrovat obsah a zabezpečit tak data. Pro ostatní uživatele jsou sice data viditelná, ale nejdou nijak otevřít.

BitLocker, BitLocker To Go: Jedná se o velmi dobrý šifrovací nástroj, který je ale v plné verzi dostupný pouze pro uživatele, kteří používají verzi systému Ultimate nebo Enterprise. V ostatních verzích se uživatelé musejí spokojit se šifrováním vyměnitelných jednotek. Tento program použijeme tak, že klikneme pravým tlačítkem na disk, který chceme zašifrovat a vybereme možnost *Zapnout nástroj BitLocker*... Program nám dá na výběr, jakým způsobem budeme chtít soubory následně odemykat. Můžeme zvolit *Čipovou kartu*, *Heslo* nebo případně kombinaci obojího. Já zvolím heslo. Program vám dále nabídne možnost tisku tohoto obnovovacího hesla, případně jeho uložení do souboru. Poté již systém začne jednotku zašifrovávat a po dokončení šifrování budeme požádáni o zadání hesla, pokud budeme chtít zašifrovaná data používat. Dále můžeme odškrtnout možnost automatického odšifrování dat v případě našeho přihlášení na tomto počítači.

Pokud se budeme chtít věnovat šifrování důkladněji nebo jenom nemáme nejvyšší verzi systému, doporučuji použít výborný freeware nástroj TrueCrypt, který má široké možnosti šifrování.

9.4 Záloha dat

Pokud nechceme někdy přijít o svá data, určitě si hned nastavíme jejich zálohu. K tomu je v systému Windows 7 určen program *Windows Zálohování*. Dostaneme se k němu následující cestou:

Start > Ovládací panely >Systém a zabezpečení >Zálohování a obnovení

Nastavení zálohy spustím tlačítkem *Nastavit zálohování* a vybereme umístění, kam se bude záloha ukládat. Je dobré volit externí úložiště nebo síťové disky. Dále si nastavíme přístupové jméno a heslo k záložnímu souboru.

V dalším kroku zvolíme, zda si vybereme sami soubory k zálohování nebo necháme volbu na systému. Samozřejmě je lepší zvolit první možnost, ať máme vše pod kontrolou. Před uložením nastavení ještě můžeme změnit časový plán pravidelného zálohování. Nástroj poté provede první zálohu systému a dat.

10 NASTAVENÍ APLIKACE INTERNET EXPLORER

Internet Explorer je internetový prohlížeč společnosti Microsoft zařazený v systému Windows 7. Tedy abych byl přesnější, byl zařazený pouze v prvních vydaných verzích. Poté už musel Microsoft z důvodu nařízení vyšších institucí nabízet uživatelům všechny prohlížeče, aby si mohl každý sám vybrat. I přesto je Internet Explorer stále hojně používaný prohlížeč a proto uvedu jeho bezpečnostní zásady a nastavení.

S nastavením bezpečnosti začneme tak, že po spuštění aplikace přejdeme v panelu příkazů do kontextového menu *Nástroje > Možnosti Internetu,* kde uvidíme čtyři karty, které nás zajímají:

a) Karta *Obecné* – Zde nás zajímá pouze část věnující se historii procházených stránek. Rozhodně zaškrtneme políčko *Odstranit historii prohlížení při ukončení,* což nám zajistí smazanou historii naší aktivity na webu při každém vypnutí programu. Pokud bychom chtěli z nějakého důvodu historii prohlížení uchovávat, v dialogovém oknu *Nastavení* určíme počet dní, jak dlouho se má historie našich aktivit uchovávat.

b) Karta *Zabezpečení* – Karta, která nás zajímá nejvíce. Najdeme zde čtyři předdefinované zóny, u kterých můžeme měnit nastavení zabezpečení:

   Místní intranet: Určena pro servery v rámci firem a korporací, které jsou obvykle v souladu s vysokou důvěryhodností.

   Důvěryhodné servery: Jedná se o servery mimo bránu firewall, ke kterým uživatel chová velkou důvěru.

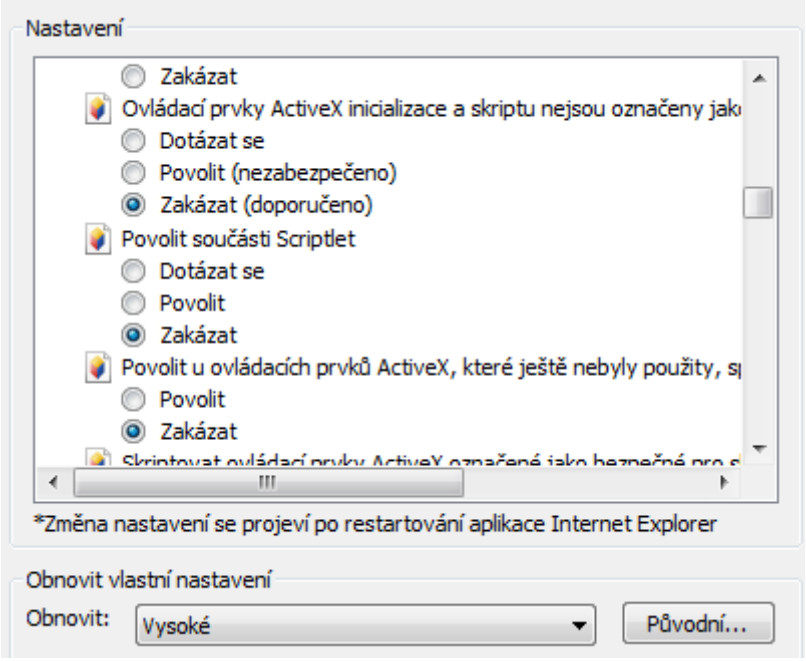
   Servery s omezeným přístupem: Servery, kterým uživatel značně nedůvěřuje.

   Internet: Všechny ostatní servery, které nespadají do předchozích zón.

   Vlastní: Zóna, kterou si uživatel nastaví sám podle vlastních pravidel.

   Do každé ze zón, kromě zóny Internet, můžeme přidat v dialogovém oknu *Servery* servery, které do dané zóny spadají, čímž ulehčíme aplikaci práci. Stejně tak můžeme u každé zóny *Povolit chráněný režim*, což je funkce, která znesnadňuje škodlivému softwaru přístup do počítače. Hlavním nastavením této karty je *Úroveň zabezpečení*, u které najdeme 3 volby úrovně: *Střední, Středně vysoká, Vysoká.* Nás zajímá především ochrana zóny Internet, kde bych doporučil nastavit úroveň

zabezpečení na hodnotu *Vysoká,* což může sice u některých stránek způsobit menší problémy s jejich zobrazením, ale není nad maximální bezpečnost. Dále si kdykoliv můžeme vytvořit *Vlastní úroveň zabezpečení*, v jehož dialogovém okně najdeme vyčerpávající možnosti přizpůsobení od možnosti *Stahovat písma* až po třeba možnost *Stahování nepodepsaných prvků ActiveX*. U většiny atributů si většinou můžete zvolit volbu *Povolit, Zakázat* nebo *Dotázat se* při každé příležitosti.



Obrázek 26 – Vlastní nastavení zóny zabezpečení v aplikaci Internet Explorer

c) Karta *Osobní údaje* – Hlavní část nastavení této karty se věnuje souborům cookies. Jejich zabezpečení můžeme nastavit v šesti úrovních, od úrovně *Povolit všechny soubory cookie* až po úroveň *Blokovat všechny soubory cookie*. Osobně doporučuji úroveň čtvrtou – *Vyšší*, která blokuje cookies, které nemají zaručenu ochranu osobních údajů a které mohou být použity bez našeho výslovného souhlasu. V dialogovém oknu *Sítě* můžeme aplikaci opět ulehčit práci a zadat weby, kde soubory cookies povolujeme nebo blokujeme.

   V druhé části karty najdeme nastavení *Blokování automaticky otevíraných oken.* Toto se týká spíše našeho klidnějšího brouzdání po webu než jeho zabezpečení, tudíž si to každý uživatel může nastavit dle libosti. Osobně však doporučuji většinu vyskakovacích oken blokovat.

d) Karta *Obsah* – Zde nás zajímají tři části karty. Tou první je *Poradce při zabezpečení obsahu*, který nejdříve povolíme. Na kartě *Hodnocení* pak můžeme u jednotlivých kategorií (např. nahota, násilí atd.) nastavit míru zobrazení, které jsme uživateli ochotni poskytnout. Na kartě *Schválené servery* můžeme nastavit konkrétní stránky, které může uživatel navštívit a které naopak ne. Na kartě *Obecné* nás zajímá především *Heslo správce*, které vytvoříme, a bude nám sloužit proti změně nastavení. Dále nastavíme, jestli v případě přístupu uživatele na zakázanou stránku bude nabídnuta možnost zadání hesla pro zobrazení obsahu stránky. Ošemetnou částí je povolení obsahu z nevyhodnocených stránek. Já osobně bych tuto možnost raději zakázal.

Druhou částí karty jsou *Certifikáty*. Zde můžeme povolit či zakázat různé vydavatele certifikátů, a jednotlivé certifikáty spravovat.

Poslední částí, která nás zajímá je *Automatické dokončování*. Zde nastavíme, která data si má prohlížeč archivovat a usnadňovat nám tak „práci“. Rozhodně ale vypneme funkci pro *Formuláře* a *Uživatelská jména a hesla.*

Přímo v panelu příkazů nalezneme kontextové menu *Zabezpečení.* Zde můžeme prohlížeč kdykoliv přepnout do módu *InPrivate*, což je funkce, která pomáhá uživatelům nezanechávat stopy po použití aplikace. Po jejím zapnutí aplikace přemění své nastavení tak, že soubory cookies a dočasné soubory, které jsou navíc zašifrovány, jsou po ukončení aplikace smazány, historie prohlížení stránek a formulářová data s hesly se neukládají vůbec. Druhou funkcí je filtr SmartScreen, který monitoruje všechny navštívené stránky a pomáhá uživateli rozpoznat, zda se nejedná o nějaký škodlivý web nebo jestli od něho nehrozí phisingový útok.

Nedávno byla vydána nová verze aplikace Internet Explorer, již s pořadovým číslem 9. Z bezpečnostního hlediska se toho prakticky moc nezměnilo, tudíž jsem výše uvedené popisoval pro rozšířenější verzi Internet Explorer 8. Jelikož Internet Explorer udělal v posledních dvou verzích z bezpečnostního hlediska velký pokrok, dá už se považovat za bezpečný prohlížeč. Pokud vám však z nějakého důvodu nevyhovuje, můžete použít jiný. Volba závisí především na osobních preferencích. Já osobně doporučuji Google Chrome, můžete však použít i ostatní ze zaběhlých prohlížečů jako je Mozilla Firefox, Opera nebo Safari.

11 OBECNÉ RADY K POUŽÍVÁNÍ INTERNETU

1) Než se vůbec poprvé připojíte na Internet, důkladně zkontrolujte následující:
   - Zda máte zaktualizovaný operační systém
   - Zda máme správně nakonfigurovaný firewall a aktualizovaný antivirový software
   - Zda máme důkladně a bezpečně nastaven internetový prohlížeč
   - Zda máme nastavený a zabezpečený poštovní program, pokud jej využíváme
   - Při používání internetového prohlížeče nevyužíváme účet administrátora, ale běžný uživatelský účet s omezenými právy
   - Zkontrolujte, že všechna důležitá data mají vypnuté sdílení přes Internet
   - Nastavte si bezpečnostní pravidla ohledně cookies, vypněte nepoužívané služby systémy a porty
   - Sledujeme informace o nejnovějších bezpečnostních hrozbách a momentálních rozšířených hoaxech
   - Než si projdete a splníte všechny předchozí body, tak se na Internet nepřipojujte!
2) Používání Internetu na místech, kde jsou po vás vyžadovány citlivé údaje:
   - Na Internetu nikdy, nikde a nikomu nedávejte důležité své osobní údaje, jako jsou např. přihlašovací jména a hesla
   - Pokud už to někde chcete udělat nebo je to po vás vyžadováno, dělejte to pouze na serverech, které využívají zabezpečeného šifrovaného připojení SSL, které poznáme podle toho, že začátek adresy se změní z *http* na *HTTPS*
   - Kontrolujte důvěryhodné servery a jejich certifikáty
   - Nevyřizujte důležité věci přes Internet, jako např. posílání citlivých souborů. Když už, tak to alespoň dělejte s použitím silného zašifrování.
   - Bankovní transakce a podobné věci řešte vždy pokud možno pouze přes počítač, ke kterému máte přístup pouze vy
   - Nikdy neposkytujte žádné nevyžádané informace navíc
3) Používání elektronické pošty:
   - Nikdy po vás nikdo nebude žádat přihlašovací jména, hesla, certifikáty

- Banky a podobné instituce po vás nikdy nebudou vyžadovat kontrolní přihlášení
- Nikdy neotvírejte odkazy, u kterých si nejste 100 % jisti a dávejte si velký pozor na podvržené adresy
- Nikdy si neinstalujte aktualizace systému, které vám přišli v e-mailu
- Nikdy neotvírejte soubory z příloh, zvláště typu *.exe,* pokud si opravdu nejste jisti, že zpráva pochází od uživatele, kterého znáte a zprávu očekáváte. Stejně tak nikdy nepřijímejte zprávy přes chatovací komunikační programy, pokud si nejste opravdu jisti.
- Ignorujte spam a nastavte si filtrace e-mailů
- Pokud už nějaká data posíláte elektronickou poštou, tak k nim vždycky uveďte textové vysvětlení a dobře je zabezpečte šifrováním. To samé očekávejte i od příchozí pošty.
- Zprávu, kterou nelze ověřit, smažte a nijak se jí nevěnujte
- Na podezřelé zprávy neodpovídejte
- Při posílání zpráv více uživatelům vepište jejich adresy do kolonky *Skrytá kopie*

4) Používání bezdrátové Wi-Fi sítě:
   - Wi-Fi síť si vždy zabezpečte silným přístupovým heslem
   - Změňte si název sítě SSID a zrušte vysílání jeho názvu
   - Použijte šifrování vysílání a pokud možno raději WPA nebo WPA2, než WEP
   - Pokud je to možné, používejte přístupovou metodu podle MAC adres. Díky nim si můžete přesně nastavit, který přístroj má přístup do vaší sítě
   - Zakažte dálkovou správu a aktualizujte firmware hardwaru
   - Pravidelně kontrolujte nastavení bezpečnosti a zranitelnost sítě
   - Nemějte přímé propojení sítě Wi-Fi se sítí LAN
   - Při použití veřejné sítě postupujte extrémně opatrně, tak jako by veškerou vaši činnost mohl kdokoliv vidět
5) Další obecné rady při použití Internetu:
   - Stahujte soubory pouze z bezpečných stránek a nikdy neinstalujte soubor, u něhož nemáte 100 % jistotu. Vždy si jej pro jistotu prověřte antivirem.
   - Vyhýbejte se stránkám s pochybným obsahem (warez, stránky s erotickým

obsahem)

- Používejte legální software. Cracky a podobný software jsou po e-mailové poště druhým nejčastějším přenašečem škodlivého softwaru
- Snažte se používat co nejvíce různých silných hesel pro různé služby
- Pro „neživotně“ důležité internetové služby si pořiďte zvláštní emailovou schránku
- Surfujte pokud možno anonymně
- Při použití cizího počítače mějte na paměti, že vaše činnost může být kdykoliv sledována
- Vyhýbejte se na Internetu podezřele příjemným nabídkám
- Snažte se o bezpečnostní osvětu i u svého okolí
- Vždycky platí pravidlo – „Důvěřuj, ale prověřuj“
- Pokud je to možné, používejte i *Virtuální privátní síť (VPN)* nebo virtualizovaná prostředí
- Po skončení používání Internetu po sobě „ukliďte“

Následující body platí v dnešní době při rozšíření sociálních sítí a podobných služeb ještě více:

- Přemýšlejte, zda na té či oné službě musíte opravdu být
- Nedejte na falešný pocit bezpečí
- Žádná služba není veřejným majetkem, tudíž nikdy nemůžete vědět, co se s vašimi daty může dít
- Hodně přemýšlejte, než něco na Internet zveřejníte
- Nekomunikujte s lidmi, které opravdu dobře neznáte
- V každé službě se nejdříve věnujte detailnímu nastavení bezpečnosti
- Nepoužívejte podobné služby, pokud nejste ve 100 % psychickém a fyzickém stavu (opilost, únava)
- Nikdy na Internet nepište to, co byste neřekli v reálném životě komukoliv

Hlavně vždy používejte zdravý rozum!

12 OBRANA PROTI SOCIÁLNÍMU INŽENÝRSTVÍ

Varovné příznaky útoku:

- Odmítnutí sdělit zpáteční číslo.
- Neobvyklá žádost.
- Ohánění se autoritou.
- Zdůrazňování naléhavosti záležitosti.
- Hrozba důsledky nevyhovění žádosti.
- Neochota volajícího odpovídat na dotazy.
- Zmiňování mnoha jmen.
- Komplimenty či pochlebování.
- Flirtování.

Obranné rady:

- Nikdy nedůvěřujte nikomu bez ověření totožnosti. Vždy kontrolujte totožnost protistrany, ať už nějakou průkaznou otázkou nebo prokázáním jasné identifikace, případně osobním setkáním. Musíte si být naprosto jisti, zda je osoba skutečně ta, za kterou se vydává a zda má vůbec právo na informace, jež požaduje.
- Nikdy nikomu nesdělujte heslo nebo jiné důvěrné informace. Heslo ani pod žádnou záminkou třeba na chvíli neměňte. Nikdy. Dále do počítače nikdy nezadávejte žádné příkazy, neinstalujte software nebo neměňte nijak nastavení počítače, pokud si nejste naprosto jisti totožností a účelem protistrany.
- Vyžadujte elektronické podpisy u e-mailů a nikdy neotvírejte jiné než očekávané přílohy, navíc proskenované antivirem.
- V případě nějaké žádosti ve firmě vždy kontaktujte svého nadřízeného pro schválení žádosti protistrany a kontrolujte její totožnost v podnikových seznamech.
- V případě telefonních hovorů vždy kontrolujte, zda pochází z místa udávání a zpětným zavoláním zjistěte, zda zobrazené číslo odpovídá osobě, která volá.

ZÁVĚR

V rámci bakalářské práce je ukázán širší pohled na počítačovou bezpečnost, zvláště na tu u operačních systémů Windows a uvedeno, proti čemu a jak se bránit. V teoretické části je hlavně nastíněn pohled širší veřejnosti na tuto problematiku, která je často hodně zanedbávána, a jaké důsledky to následně může přinést. Proto byl také vypracován internetový dotazník, který velmi dobře ukázal, jak se většina uživatelů k počítačové bezpečnosti staví, na co si dávají velký pozor a co zanedbávají.

Hlavní náplní práce je praktická část, ve které je sestaven podrobný návod, jak systém Windows 7 zabezpečit pomocí nástrojů dostupných přímo v systémové konfiguraci, nebo doplňky od Microsoftu volně stažitelnými z Internetu. Případně jsou doporučeny vhodné programy a software od jiných výrobců. Nejdůležitější částí ale jsou do hloubky rozebrané položky jednotlivých nastavení systému, která jsou základním kamenem dobře zabezpečeného počítače. Výstupem práce jsou taky rady, jak se chovat na síti Internet, která je v dnešní době zdrojem největšího nebezpečí. Část práce je taky věnována sociálnímu inženýrství, které se stále více rozmáhá a spousta lidí stále ani neví co to je, natož jak se mu bránit.

Samotný systém Windows, konkrétně jeho nejnovější verze s názvem „7“, která oproti minulým verzím přinesla spoustu bezpečnostních vylepšením, je pravděpodobně nejbezpečnější verzí vůbec v historii. Z nástrojů se musí vyzdvihnout hlavně Internet Explorer, který už nyní není jako dříve ten „nejméně bezpečnější prohlížeč“, jenž udělal v tomto směru velké kroky směrem vpřed, a pokud je uživatel zdravě opatrný, může ho s klidným svědomím používat. Windows Firewall se zase konečně dá považovat konkurenceschopný software, i když od kvalit placených profesionálních programů je stále na míle vzdálen. Antivirový nástroj Microsoft Security Essentials zase patří mezi přední freewarové nástroje v tomto oboru a proto je škoda, že není integrován přímo v systému. Alespoň je nabízen přes službu Windows Update, která je pro změnu nyní více přehledná a neobtěžuje už tak moc uživatele.

Celkově lze říci, že pokud bude běžný uživatel používat nejnovější verzi systému, samozřejmě pravidelně aktualizovanou a nastavenou tak, jak je uvedeno v práci a bude se na Internetu chovat podle uvedených rad, nemůže mít prakticky s bezpečností žádné problémy.

CONCLUSION

Within the scope of the bachelor's thesis there is shown a wider view of the computer's security, especially of the operating systems Windows, and there is stated how and against what to be protected. In the theoretical part there is mainly foreshadowed general public's view of these questions that are often widely neglected and what consequences it can bring. Therefore the internet inquiry was elaborated and it showed very well how most of users perceive the computer's security, what they are very careful of and what they neglect.

Main scope of this work is in practical part where there is elaborated a detailed manual how the system Windows 7 is to be secured by means of instruments approachable directly in system configuration or by supplements by Microsoft that are downloadable from the Internet for free. Eventually useful programs and software by other producers are recommended. But the most important part is in deeply analysed items of particular system set-ups that are the keystones of a well secured computer. Output of the work is also in advice how to use the Internet, which is the source of the biggest dangers nowadays. Part of the work is also attended to the social engineering that extends more and more and a lot of people neither know what it is nor how to defend against it.

The system Windows itself, particularly its newest version with the name „7" that brought plenty of security improvements in comparison with the older versions, is probably the safest version at all in its history. From the instruments there must be pointed out especially Internet Explorer that is not "the least secure browser" in these days as it was in the past. It took big steps forward in this respect and if the user is properly careful he can use it with clear consistence. Windows Firewall can be finally regarded as able-to-compete software although it does not reach by far the qualities of paid professional software. Antivirus instrument Microsoft Security Essentials is on the other hand ranked among the chief freeware instruments in this field and therefore it is a pity that it is not integrated directly in the system. At least it is offered through Windows Update, which is for a change more transparent now and it does not trouble the users so much.

Globally it can be said that if common user uses the newest system's version, of course regularly updated, set up in the way it is stated in the work and he uses the Internet according to the stated advice, he cannot have in effect any problems with security.

SEZNAM POUŽITÉ LITERATURY

[1] RYCHNOVSKÝ, Lukáš. Zpravodaj ÚVT MU [online]. 2005, 3.5.2011 [cit. 2011-05-07]. Počítačová bezpečnost. Dostupné z WWW: <http://www.ics.muni.cz/zpravodaj/articles/342.html>.

[2] BOTT, Ed ; SIECHERT, Carl . Mistrovství v zabezpečení MS Windows 2000 a XP : Nejpraktičtější a nejucelenější průvodce bezpečností Windows. Vydání první. Brno : Computer Press, a.s., 2004. 696 s. ISBN 80-722-6878-3.

[3] ZEMÁNEK, Jakub. Slabá místa Windows aneb jak se bránit hackerům. Kralice na Hané : Computer Media s.r.o., 2004. 156 s. ISBN 80-86686-11-6.

[4] ITPOINT 2008 [online]. 31.3.2008 [cit. 2011-05-18]. Bezpečnost počítače. Dostupné z WWW: <http://www.itpoint.cz/zprava-itpoint.asp?id=1908&ico=48429627>.

[5] NETMARKETSHARE [online]. 18.5.2011 [cit. 2011-05-18]. Top Operating System Share Trend. Dostupné z WWW: <http://marketshare.hitslink.com/os-market-share.aspx?qprid=9>.

[6] HOLČÍK, Tomáš . Živě.cz : O počítačích, IT a Internetu. [online]. 17.1.2004 [cit. 2011-05-16]. Stručná historie Windows. Dostupné z WWW: <http://www.zive.cz/clanky/strucna-historie-windows/sc-3-a-115491/default.aspx>.

[7] BOTT, Ed; SIECHERT, Carl; STINSON, Craig. Mistrovství v Microsoft Windows 7. Brno : Computer Press, 2010. 936 s. ISBN 978-80-251-2817-6.

[8] BOTT, Ed; SIECHERT, Carl. Mistrovství v Microsoft Windows XP. Brno : Computer Press, 2004. 608 s. ISBN 80-7226-980-1.

[9] DOČEKAL, Michal. Shadow Weblog : Blog linuxového nadšence [online]. 2.2.2009 [cit. 2011-05-07]. Bezpečnost: O můj počítač nikdo nestojí. Ale ne. Stojí. Dostupné z WWW: <http://www.shadow.cz/blog/512>.

[10] KAŠPAR, Jaromír . Silicon Hill [online]. Verze 37. 8.8.2006, 22.9.2006 [cit. 2011-05-07]. Zabezpečení Windows. Dostupné z WWW: <http://wiki.siliconhill.cz/Zabezpe%C4%8Den%C3%AD_Windows>.

[11] MIKLE, Ondrej . Živě.cz : O počítačích, IT a Internetu [online]. 25.11.2004 [cit. 2011-05-07]. Jak zabezpečit počítač s Windows XP. Dostupné z WWW: <http://www.zive.cz/clanky/jak-zabezpecit-pocitac-s-windows-xp/sc-3-a-120996/default.aspx>.

[12] MITNICK, Kevin; SIMON, William. Umění Klamu. Vyd. 1. Gliwice, Polsko : Helion S.A., 2002. 348 s. ISBN 83-7361-210-6.

[13] SOSINSKY, Barrie. Mistrovství - počítačové sítě : [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

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

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DDos	Distibuted Denial of Service
DDE	Dynamic Data Exchange
P2P	Peer To Peer
NTFS	New Technology File System
FAT32	File Allocation Table
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
AGP	Accelerated Graphics Port
DVD	Digital Versatile Disc
VPN	Virtual Private Network
EFS	Encrypting File System
SNMP	Simple Network Management Protocol
FTP	File Transfer Protocol
DNS	Domain Name System
IP	Internet Protocol
BIOS	Basic Input-Output System
MMC	Microsoft Management Console
SSL	Secure Sockets Layer
HTTPS	Hypertext Transfer Protocol Secure
SSID	Service Set Identifier
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
LAN	Local Area Network

SEZNAM OBRÁZKŮ