Softwarová ochrana dat v počítačových sítích

Data protection in computer networks

Jan Mucha

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Jan MUCHA**
Osobní číslo:	**A09247**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Softwarová ochrana dat v počítačových sítích**

Zásady pro vypracování:

1. **Uveďte metody a techniky používaných v současnosti útočníky k průnikům do počítačové sítě.**
2. **Rozeberte principy a postupy pro zabezpečení počítačů a lokálních sítí proti útokům z internetu.**
3. **V praktické části prozkoumejte zabezpečení vybraných nejpoužívanějších operačních systémů.**
4. **Otestujte zabezpečení těchto systémů pomocí simulovaných útoků popř. pomocí nějakého testovacího software.**
5. **Vyhodnoťte provedené testy a formulujte doporučení, které by měl uživatel dodržet pro co nejlepší zabezpečení systému.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Ludvík, Miroslav a Bohumír Štědroň. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.**
2. **McClure, S., J. Scambery a K. George. Hacking bez záhad. Praha: Grada, 2007. ISBN 978-80-247-1502-5.**
3. **Kabelová, Alena a Libor Dostálek. Velký průvodce protokoly TCP/IP a systémem DNS. Brno. Computer Press, 2008. ISBN 978-80-251-2236-5.**
4. **McClure, S., J. Scambray a K. George. Hacking bez tajemství. 2. Aktualizované vydání. Praha: Computer Press, 2002. ISBN 80-7226-644-6**
5. **Dostálek, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. Praha: Computer Press, 2001. ISBN 80-7226-513-X.**

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

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Cílem mé práce je poskytnout čtenáři pohled na problematiku softwarové ochrany dat v počítačových sítích se zaměřením na rozebrání základních druhů útoků hackerů a také popsat, jak se proti těmto útokům bránit. Dále pak osvětluje čtenáři některé základní principy zabezpečení systému.

V praktické části je proveden průzkum zabezpečení nejpoužívanějších operačních systémů a otestování těchto systémů. Cílem bylo předvést uživateli PC, jak je jeho systém zabezpečen a rovněž doporučit kroky pro co nejlepší zabezpečení systémů se zaměřením na šifrování a zálohování dat.

Klíčová slova: bezpečnost, útoky, operační systémy, šifrování, zálohování dat

ABSTRACT

The aim of this thesis is to give a perspective to reader on the issue of software protection of data in computer networks with a focus on analyse the basic types of hacker attacks and also describe how to defend against these attacks. Further it illuminates to the reader some basic principles of system security.

In the practical part is carried out a survey about popular operating systems security and testing of these systems, the aim was to show to PC user how is his system secured and also recommended steps for the best system securing with focusing on encryption and data backup.

Keywords: security, attacks, operating systems, encryption, data backup

Poděkování

Rád bych poděkoval Ing. Jiřímu Vojtěškovi, Ph.D. za jeho rady, vstřícnost a ochotu. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi od nich dostávalo během tvorby této práce i celého studia.

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 jsem seznámen 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

V dnešní době je problematika úniku dat z cizího počítače velice aktuální, protože útoků, které vedou hackeři proti systémům či celým počítačovým sítím, je stále více. V oboru informačních technologií je tato problematika velmi rozsáhlá a není možné v práci uvést všechny metody a techniky, které v dnešní době používají hackeři. Cílem je představit nejzákladnější a nejběžnější druhy hackerských útoků, se kterými se může setkat běžný uživatel PC.

V běžném životě jsou si lidé vědomi nebezpečí, které jim hrozí z klasických krádeží, ale v případě krádeží vedených prostřednictvím počítače nebo počítačových sítí, to tak už nebývá. Je spousta uživatelů PC, kteří nemají ani ponětí o nějakých metodách hackerů, které jim mohou způsobit poškození systému či ztrátu dat, případně nějaké finanční škody, jak je toho v případě phishingu a pharmingu. Tito uživatelé by měli práci věnovat větší pozornost, aby se dozvěděli více o možnostech, jak se do systému nabourávají hackeři a jak v mnohých případech využívají vaší nepozornosti k proniknutí do osobních počítačů či sítí.

Práce popisuje základní druhy útoků, které provádí hackeři jako první při nabourávání se do systémů, zejména se jedná o vyhledávání stop, respektive určení počítačů, které by mohli napadnout a dále pak skenování portů a identifikace služeb, které má uživatel na počítači. Je důležité si uvědomit, že hacker se pomocí těchto kroků dostává stále více do vašeho systému. Uživatel, který je o těchto možnostech informovaný, se bude mnohem lépe bránit než ten, který o související problematice zdaleka nic netuší.

Na Internetu si dnes můžeme přečíst, že existuje celá řada programů a aplikací, které bychom měli znát v souvislosti se zabezpečením našeho počítače proti útokům ze sítě Internetu. Je však nelehký úkol si vybrat ty správné bezpečnostní aplikace, protože výběr těchto produktů je tak rozsáhlý, že by se daly studovat celé dny. V mé práci se můžete dozvědět, jak svůj počítač vybavit základním ochranným softwarem a důsledkem toho se zorientovat v této oblasti.

Dále pak mezi dnes často rozebíranou problematiku patří šifrování a zálohování dat, což představuje další kroky, které by měli uživatelé znát, aby tak předešli neoprávněnému přístupu k vlastním datům či samotné ztrátě dat. Z tohoto důvodu jsem se také na tyto dvě témata zaměřil a to zvláště na šifrování v operačním systému Windows 7, kde jsem popsal jeho základní principy a možnosti jeho nasazení. Se šifrováním je úzce spojené samotné

zálohování dat, což je dnes také velmi populární, protože ztráta důležitých či důvěryhodných dat představuje pro uživatele nemalý problém.

I. TEORETICKÁ ČÁST

1 METODY A TECHNIKY HACKERŮ

V první části své práce se zaměřím na metody a techniky, které se týkají průniku, tedy jakéhosi celkového narušení počítačových sítí. Cílem je tyto postupy představit, nikoli dát přesný návod, jak je v praxi provést. Patří sem zejména vyhledávání stop, dále pak skenování portů a mnoho dalších, které si představíme následovně.

1.1 Vyhledávání stop

Vyhledávání stop je činnost zaměřená na získávání informací o přítomnosti organizace v Internetu. Pomocí kombinace utilit, technik a databází, které jsou veřejnosti přístupné, může hacker zjistit informace o adresách zařízení připojených do sítě Internetu, doménových jménech, přidělených IP adresách a dalších. Technik je celá řada. V největší míře se používají techniky zaměřené na získávání informací o firemních sítích, tedy intranetu. Dále pak informace získané z Internetu, o vzdálených přístupech vnitřních sítí a extranetu.[1]

Hledání stop je velmi důležité, protože nám osvětlí jakýsi obraz o zabezpečení celé společnosti. Bez chybějících dat si nikdy nevytvoříme ucelený obrázek o systému, který je v dané síti použit. To pak může mít za následek, že během útoku narazíme na technologie a systémy se kterými jsme nepočítali. Celou práci při vyhledávání stop si shrneme do čtyř bodů:

1. Krok Určení sféry zájmu

Nejprve se musíme rozmyslet, o jaké informace máme vlastně zájem. Budeme se pokoušet získat informace o celé organizaci, pobočce nebo omezíme svoji činnost na osobní počítač zaměstnance. Internet v dnešní době představuje obrovské množství veřejně přístupných zdrojů, které se dají využít při získávání informací o organizaci a jejich zaměstnancích. V dnešní době můžeme na stránkách Internetu najít informace, které se týkají:

- Lokalit, ve kterých se organizace nacházejí.
- Telefonních čísel.
- Kontaktních osob a jejich e-mailových adres.
- Bezpečnostní politiky a informace o použitelných bezpečnostních mechanismech.
- Odkazů na další webové servery související s organizací.

2. Krok Mapování sítě

Mapování sítě představuje činnost, kdy se hacker snaží identifikovat domény a k nim síťové adresy organizací, do jejichž sítí chtějí proniknout. Doména nám v podstatě říká, kde organizaci v síti Internetu najdeme. Můžeme říci, že doména organizaci reprezentuje. Existuje několik registrátorů domén a celá řada whois databází, kde jsou domény uloženy. To samozřejmě komplikuje práci hackera, jelikož musí nejprve zjistit, v jaké whois databázi se doména nachází. Seznam registrátorů je dostupný z www.internic.net.[1]

Na serveru www.nic.cz nalezneme informace o doménách, které náleží do domény cz. Dalším zdrojem informací je server www.allwhois.com. Do whois databází je možné zadávat několik typů dotazů:

- Registrátor – zobrazí informace o subjektu, který prováděl registraci údajů do databáze, a o příslušných whois serverech.
- Organizace – zobrazí informace o příslušné organizaci.
- Doména – zobrazí informace o příslušné doméně.
- Kontakt – zobrazí informace o osobě odpovědné za uvedené informace, obvykle administrátorovi sítě.

3. Krok Zkoumání DNS

V případě, že se podaří útočníkovi vypátrat všechny domény, které si organizace zaregistrovala, může zaútočit na informace uložené v DNS. DNS je distribuovaná databáze, která překládá doménové názvy na IP adresy a naopak. IP adresy se špatně pamatují, proto vznikla doménová jména, která jsou uložena v systému DNS. Je tedy o mnoho jednodušší si zapamatovat doménové jméno, prohlížeč zajistí spojení s požadovaným serverem a zobrazí stránku. Pokud je DNS databáze špatně nastavena, je možné, že hackeři do ní mohou proniknout.

Jednou z největších chyb při konfiguraci DNS je povolení přenosu zóny na libovolný počítač v Internetu. Informace o zóně jsou přenášeny z primárního jmenného serveru (primary nameserver) na sekundární (secondary nameserver) kvůli zajištění redundance dat. Redundance je nutná v případě výpadku primárního jmenného serveru, kdy jeho funkce přebírá sekundární. Přenosy zóny by měly být povoleny pouze sekundárnímu serveru. Mnoho DNS serverů umožňuje tyto přenosy na libovolný počítač.

Tento druh nastavení je zvláště nebezpečný v případě, kdy DNS servery obsahují užitečné informace o intranetu podniku. Je pak snadné přečíst informace o zóně, které se týkají přehledu serverů ve vnitřní síti. Z těchto informací se dají vyčíst i jména počítačů, což nahrává do karet hackerovi, který může odhadovat, k čemu slouží konkrétní servery a jaké aplikace jsou na nich používány.

4. Krok Průzkum sítě

Pokud by se útočníkovi povedlo zjistit adresy sítí organizace, můžem se pokusit určit její síťovou topologii a potenciální přístupové cesty. K jednomu serveru může existovat několik přístupových cest, přes směrovače s několika síťovými zařízeními. Navíc může mít každé zařízení jiná pravidla ACL, které kontrolují přístup do připojených sítí.

ACL (Access Control List) tvoří seznam pravidel, které řídí přístup k nějakému objektu. Většinou se používají u aktivních prvků sítě. Můžou být také použity v operačním systému pro řízení přístupu k souboru. Pokud někdo žádá o přístup k souboru, nejprve se zkontroluje v pravidlech ACL, zda je tato operace povolena.

1.2 Skenování

Z předchozích technik útoků na počítačové sítě jsme zjistili bloky IP adres přidělené organizaci, jména zaměstnanců, telefonní čísla, adresy DNS serverů a adresy poštovních serverů. Při skenování se pomocí různých metod, jako je skenování portů, ping a automatizované lokalizování severů pokusí hacker zjistit, na kterých IP adresách se nacházejí funkční systémy dostupné z Internetu.[1]

V případě, že výpis zóny obsahuje IP adresu, není pro hackera ještě úplně přesně řečeno, zda je tato IP adresa dostupná z Internetu. Je zapotřebí otestovat systém, do kterého chce proniknout. Zvláště tedy skenovat porty a zjistit, na kterých portech systém naslouchá, tj. jaké na nich provozuje aplikace. Je tu možnost, že ve výpisu zóny nalezneme spoustu systémů, které se nacházejí ve vnitřních (privátních) sítích. Tyto adresy se zpravidla v Internetu netestují, protože je velmi obtížné na ně nasměrovat testovací pakety.

IP adresy privátních sítí jsou zejména 10.10.10.0, 172.17.16.0 a 192.168.0.0. Můžeme je najít v RFC 1918, což je standard pro přidělování privátních IP adres. Je to v podstatě dokument, který přesně definuje, které IP adresy jsou pro tyto sítě vyhrazeny.

1.2.1 Skenování portů

Skenování portů patří mezi průzkumné techniky na Internetu. Je velmi populární. Tuto techniku využívá například i vyhledávač Google. Zařadil jsem ji do své páce, jelikož bývá také velmi často využívána hackery jako prostředek k následnému průlomu do počítačové sítě. Takovéto skenování může v některých případech přispět k pádu či přetížení celé počítačové sítě.

Existuje celá řada programů, tzv. skenerů portů, které se zabývají skenováním portů. Nejjednodušším způsobem je otevřít TCP spojení na všech portech cílového systému. Nutností pro skenování portů je znát IP adresu PC, u kterého chtějí hackeři porty oskenovat. Některé programy umožňují zadat i doménové jméno, které je ale přiděleno IP adrese.

Při skenování je nejvíc nebezpečné, že hacker zjistí službu, která přes daný port běží. Podle toho se zařídí a směřuje svůj útok přes zjištěnou službu. Z toho vyplývá, že každý otevřený port představuje riziko. Také se často stává, že na osobních počítačích uživatelů běží služby na portech, o kterých sami uživatelé ani neví, že je mají. Mohli si je stáhnout z nezabezpečených webů při surfování na Internetu nebo je nainstalovali nedopatřením.

Tyto otevřené porty pak napomáhají hackerům, jelikož k získání přístupu zkouší předdefinované kombinace jmen a hesel k dané službě. Některé skenery portů umí také vyhledávat porty, které jsou typické pro trojské koně. Opět představují jakousi bránu pro hackery k průniku do sítě.[1]

1.3 Firewall

V dnešní době je většina počítačových sítí chráněna pomocí firewallu. Firewall je zařízení, které nám odděluje naši firemní síť od sítě Internetu. Slouží pro detekování škodlivých programů a aplikací, které k nám ze sítě Internetu proudí. Nelze ovšem říci, že zabezpečení sítě firewallem je 100% ochranou, protože spousta firewallů je špatně nastavena a nakonfigurována. Tato zařízení představují pro hackery vstup do zabezpečené sítě.

Pokud je ovšem firewall dobře nakonfigurován, jeho prolomení je velmi obtížné. Z těchto důvodů se hackeři zaměřují spíše na jiné mechanismy proniknutí do sítě, jako jsou například modemová připojení. Vzhledem k možnému riziku prolomení firewallu si dále

popíšeme základní techniky používané k detekci firewallu a ke zjištění jeho konfigurace.[1]

1.3.1 Identifikace Firewallu

Většina firewallů zanechává svojí přítomností v síti jednoznačnou elektronickou stopu. V takovém případě může útočník poměrně snadno zjistit typ, verzi a konfigurační pravidla téměř každého firewallu. Tato identifikace je velmi důležitá, protože na základě těchto údajů si může útočník vytvořit představu o slabých místech zařízení a metodách jejich využití k průniku do sítě.

Nejjednodušší způsob, jak identifikovat firewall je přímé skenování portů. Pro toto skenování se například používá program Nmap. Je to program určený k prozkoumávání sítí nebo k bezpečnostním auditům. Je to freeware navržený k rychlému skenování počítačových sítí nebo osobních počítačů. Funguje téměř na všech operačních systémech jako je Linux, Windows, Mac OS X, OpenBSD atd. V zásadě tuto metodu používají začátečníci. Existuje mnoho složitějších metod, jako je například použití distribuovaných skenů.

V případě, že chcete skenování portů na firewallu zakázat, musíte tyto porty zablokovat na směrovačích nacházejících se v síti před firewallem. Pokud se o administraci směrovačů stará poskytovatel připojení k Internetu, musíte ho kontaktovat a zažádat o zablokování příslušných portů.

Pokud přímé skenování není účinné, může se hacker pokusit identifikovat firewall pomocí skenování serverů skrytých za ním. Následnou analýzou výsledků lze odhalit firewall, ale i pravidla, která jsou na firewallu definována. Pokud skenujeme počítač programem Nmap, získáme informace o portech. Zjistíme, které porty jsou otevřené, zavřené a blokované. Tyto informace nám opět vypovídají o konfiguraci firewallu umístěném mezi námi a cílovým počítačem.[1]

1.4 Vzdálené připojení přes síť Internetu

Vhledem ke stále větší globalizaci dochází k tomu, že spousta firem je roztroušena po celém světě a často se stává, že personál, který se stará o počítačové sítě, není na místě přítomen. Právě z těchto důvodů se používá software pro vzdálený přístup.

1.4.1 Vzdálený přístup

Vzdálený přístup je program, který nám umožňuje vstoupit do vzdáleného počítače a vyřešit vzniklý problém nebo jen asistovat uživateli PC s náročnějším technickým úkolem. Bohužel některé tyto programy jsou špatně nakonfigurovány a obsahují tak slabé místa, což vede k jejich zneužití. Často bývají zneužívány hackery, kteří tyto programy využívají k připojení na systém, a tak získají mnoho citlivých informací, v horším případě mohou použít napadený počítač k útoku na celou síť.[1]

Každý síťový program očekává příchozí spojení na specifických otevřených portech. Počet a čísla portů závisí na použitém programu. Se znalostí těchto portů a pomocí skeneru portů může hacker odhalit počítače, na kterých je spuštěn program pro vzdálený přístup. Pokud útočníci objeví počítač, který má program pro vzdálený přístup, určitě se na něj pokusí získat přístup. V základním nastavení bohužel téměř všechny aplikace pro vzdálený přístup umožňují připojení bez zadání jména a hesla.

Pokud se hacker dostane do sítě pomocí vzdáleného přístupu, může využít spousty slabých míst k tomu, aby se později mohl vrátit. Některé starší produkty nešifrují jména a hesla, takže je útočník může poměrně snadno získat ze souborů, obrazovek nebo ze sítě.

Existují i další bezpečnostní díry, kterým je nutno věnovat pozornost, jedná se zejména o:

Nešifrovaná jména a hesla

Některé programy, které se používají pro vzdálený přístup, nešifrují jména a hesla. Toto opět velmi usnadňuje práci hackera, který se mnohem snáze dostane do programu a nemusí se zabývat prolomením hesla, které by jeho činnost přinejmenším zpomalilo.

Špatně skrytá hesla

Další programy, které řadíme do programů vzdáleného přístupu, sice hesla šifrují, ovšem jedná se o šifrování velmi slabé. Ve většině případů se jedná o pouhou substituci, kdy si stačí zapamatovat abecedu a heslo neodolá.

Odhalená hesla

U většiny programů při zadávání hesla se pouze zobrazují hvězdičky. Bohužel jsou programy, které pouze heslo za těmito symboly schovávají, ale už ho nešifrují. Jako příklad uvedu program pcAnywhere. PcAnywhere je program pro získání vzdáleného přístupu k

PC pomocí mnoha podporovaných protokolů a zařízení. K získání hesla používají hackeři dalších programů, které umí položit objekt na pole s heslem a heslo odhalit.

Přepsání profilů

V případě, že útočník získá oprávnění administrátora, může do systému zkopírovat své vlastní profily a získat tak přístup do systému pod svým vlastním heslem. Pokud máte software pro vzdálený přístup, který používá k ukládání autorizačních informací o spojení zvláštní soubory, je patrně náchylný k tomuto útoku.

1.4.2 Útoky přes VNC

VNC (Virtual Network Computing) je program, který umožňuje vzdáleně pracovat na počítačích připojených do sítě Internetu. Jeho výhodou je, že je nezávislý na platformě. Můžeme se tedy z operačního systému Windows připojit na Linux či jiný operační systém. VNC obsahuje také mnoho dalších funkcí. Bohužel program, který obsahuje tolik funkcí, bude mít i mnoho nedostatků. Samozřejmě, že bývá také vyhledáván hackery.

Jedním z útoků, které provádí hackeři je možnost získání hesla programem Revelation. Také se stává, že hackeři tajně nainstalují VNC do počítače uživatele a zajistí automatický start tohoto programu, který jim pak umožní se k počítači připojit. Existuje celá řada vážnějších útoků na VNC.

Zejména se jedná o útok hrubou silou na hesla programu VNC. VNC umožňuje jednoduchý způsob útoku hrubou silou, který může vést k odhalení hesla. Hackeři k tomu používají tzv. záplatu rfbproto.c. Jedná se o upravenou verzi programu, pomocí které může hacker provést útok na server. Vytvořený modifikovaný klient vncviewer vyzkouší všechna hesla, která má útočník ve svém slovníku a odhalí tak platné heslo. Také se může hacker přihlásit k serveru a získat tak kontrolu nad systémem.

Další útok, který hrozí u VNC, je analýza síťového spojení. Největším úskalím je, že pokud nainstalujeme VNC v základním nastavení, tak veškerá komunikace mezi klientem a serverem probíhá nešifrovaně. Protože je zdrojový kód programu volně k dispozici, není složité vytvořit specializovaný VNC sniffer, kterým může útočník například odchytávat hesla použitá během VNC relace k připojení na další servery.[1]

Naštěstí existuje celá řada metod, které slouží k zašifrování komunikace mezi VNC klientem a serverem. Jednou z metod je použití SSH tunelu. SSH znamená Secure SHell a

slouží k připojení na vzdálený počítač, který danou službu podporuje. Protokol SSH používá zabezpečený kanál pro komunikaci. Tento kanál lze také použít pro přenos jiných dat. Jedná se tedy o spojení SSH tunel, nebo také SSH tunelování, což představuje komunikaci mezi jednotlivými porty dvou počítačů. Dále pak existuje několik záplat, které umožňují použít knihovnu SSLeay k šifrované komunikaci na principu veřejného klíče. Lze také omezit přístup k VNC serveru na definované IP adresy.

1.5 DoS útoky

Další útoky, které často provádějí hackeři, jsou útoky typu DoS. DoS útoky jsou prováděny hackery proti serveru (resp. celé síti) připojenému k Internetu. Cílem tohoto útoku je ochromení provozu serveru na základě zvýšení počtu přicházejících požadavků na obsloužení. Typickým příkladem DoS útoku, který provádí hacker je spuštění programu, který posílá na server nesmyslná data a ty ho pak zahltí.[2]

Po zahlcení serveru daty již není schopen reagovat na požadavky uživatelů. Hacker tedy v konečném důsledku používá DoS útoky k úplnému zhroucení a zhavarování serveru. Tyto útoky se v současné době stále hackery provádí, proto jim budu věnovat v práci pozornost.

Útoky typu DoS (Denial of Servise) jsou vážným problémem libovolného systému nebo sítě. Také se nazývají útoky odmítnutí služby. Můžeme najít velké množství nástrojů, pomocí kterých lze DoS útoky provádět. Je tedy důležité si uvést teorie, které slouží pro pochopení 4 základních DoS útoků.

Obsazení přenosové kapacity linky

Je to pravděpodobně jeden z nejúčinnějších a zároveň nejskrytějších DoS útoků. Útočník tímto útokem může zablokovat přístup do sítě. Útok je možné vést v lokální síti, ale častějším způsobem je útok vzdálený. Existují dva druhy tohoto útoku:

- Útočníci mohou zahltit síť v případě, že sami vlastní linku o větší kapacitě. Většinou se tento útok neprovozuje v sítích s pomalými linkami.
- Ke zvýšení svých aktivit používají hackeři větší množství serverů. Útočníci ovládnou další systémy a začnou do cílové stanice generovat velké množství dat z každého serveru. Často se k těmto útokům používá protokol ICMP.

Protokol ICMP (Internet Control Message Protocol) je určen k signalizaci problémů v TCP/IP síti. Protokol zajišťuje přenos důležitých informací mezi klíčovými komponenty sítě, jako jsou například směrovače a koncové stanice. Mezi důležité informace patří např.:

- Signalizace přetížení sítě.
- Nedostupnost sítě, koncové stanice a komunikačního portu.
- Indikace určitých chyb v záhlaví IP paketu.
- Oznámení příliš dlouhé doby existence paketu v síti.
- Informace o dostupných směrovačích připojených do LAN sítě.

Přivlastnění systémových zdrojů

Tento útok se opět pokouší o zahlcení linky, ale jeho hlavním cílem je spotřebování systémových zdrojů cílového počítače. Tyká se to hlavně zdrojů, které představují diskový prostor, operační paměť, procesorový čas a jiné. Útok má za následek, že ostatní uživatelé, ale i operační systém mohou být od těchto zdrojů odříznuti, což vede ke zhroucení operačního systému, zahlcení souborových systémů a k tzv. tuhnutí procesů.[1]

Chyby v programech

Chyby v programech vyvolávají neobvyklé situace v aplikacích, operačním systému, které navozuje útočník. Takováto situace může vzniknout zadáním neočekávaných argumentů nebo datových vstupů. V případě počítačových sítí se jedná o nestandardní pakety, které mohou způsobit zhroucení jádra operačního systému nebo síťového subsystému. V případě aplikací, které očekávají nějaká data na vstup, může útočník zahltit pomocí dlouhých řetězců a způsobit tak jejich zhroucení. Pokud aplikace používá vyrovnávací paměť o konstantní délce, může útočník dosáhnout její přeplnění a následné zhroucení aplikace.

Útoky na DNS a systémy směrování paketů

Tyto útoky se používají pro ohrožení směrování paketů. Provádí se pomocí směrovacích tabulek, které mohou způsobit znepřístupnění služeb systémům nebo sítím. Celá řada směrovacích protokolů používá nedostatečnou autentizaci, proto může útočník změnit směrovací tabulky a přesměrovat datový tok do své sítě. Těmto sítím se říká černá díra, tedy sítě, které ve skutečnosti neexistují.

Útoky na DNS spočívají v umístění nesprávné informace do cache nameserveru. Ten pak poskytuje falešné informace klientovi a je nasměrován do černé díry nebo na jiný server, než je ten oficiální.

Mezi další druhy útoků DoS řadíme také Záplavové DoS útoky, jejichž hlavním smyslem je linku zahltit tak velkým množstvím dat, že dojde ke zhroucení normálního provozu linky. Nedílnou součástí útoků, které řadíme do kategorie DoS, jsou tzv. Reflektivní DoS útoky. Jejich hlavním smyslem je použití dat z více počítačů, které opět slouží k zahlcení linky oběti.

1.6 Exploit

K dalším technikám, jak proniknout do sítě patří části kódu, kterým se říká anglicky exploits. Exploity jsou programy, které využívají bezpečnostních děr v operačních systémech, prohlížečích a dalším softwaru. Využívají je hackeři ke spuštění dalšího škodlivého softwaru bez vědomí uživatele.

Nebezpečí spočívá v tom, že hacker vlivem spouštění dalších škodlivých kódů zahltí uživatelovo PC a vytvoří z něj skladiště a úložiště dalšího škodlivého softwaru.

Většina hackerů vlastní celé sady těchto exploitů, pomocí kterých se pak snaží proniknout do sítě. Na Internetu se těmto nebezpečným kódům věnuje spousta webových stránek, není tedy nijak složité je díky rozsáhlým schopnostem Googlu vypátrat. Daleko složitějším úkolem je vypátrání potenciálních cílů hackerů. Je spousta webových aplikací, které používají přímo hledání Googlu a jsou navržena tak, aby vypátrala potenciální cíle.

Hlavní otázkou je, jak tyto exploity v Googlu vypátrat. Používá se několik způsobů. Jedna z možností je sledovat přípony souboru zdrojového kódu a hledat konkrétní obsah uvnitř kódu. Pro tento úkol se nám Google hodí velimi dobře. Je to z toho důvodu, že spousta exploitů je napsána v jazyce C, kdy se jako přípona souboru používá .c.

Dalším způsobem, jak vypátrat exploity je zaměřit se na běžně používané řetězce ve zdrojovém kódu. Další variantou je sledovat běžné odkazy na vkládané nebo hlavičkové soubory. Programy v C obsahují standardně knihovní funkce pro vstupní a výstupní operace, které jsou odkazovány uvnitř zdrojového kódu pomocí příkazu include. Například dotaz „#include <stdio.h> exploit“ by vypátral zdrojový kód C, který obsahuje slovo exploit, bez ohledu na to, jakou má soubor příponu.

Pomocí technik traverzování se dají odhalit další nástroje a zbraně. Existuje řada způsobů, jak odhalit zdrojový kód pomocí běžných řetězců kódu. Ukázka, jak vypadá kód exploitů uvádím níže, viz Tabulka 1. [5]

Jazyk	Přípona	Ukázka řetězce
Asp.net(C#)	Aspx	"<%@Page Language="C#""inherits
Asp.net(VB)	Aspx	"<%@Page Language="vb""inherits
Asp.net(VB)	Aspx	"<%@Page Language="JScript"
C	C	"#include<stdio.h>"
C#	Cs	"using System;" class
C++	Cpp	"#include "stdafx.h""
Java	J,JAV	class public static
JavaScript	JS	"<script language="JavaScript">"

Tabulka 1 Ukázka řetězce kódu exploitů

Pátrání po zranitelných cílech

Hackeři používají nejčastěji tři způsoby pro pátrání po zranitelných cílech:

- Útočníci mohou pátrat po potenciálních cílech tak, že se soustředí na řetězce, které jsou přítomné v nainstalovaných demonstračních aplikacích poskytnutých výrobcem softwaru.
- Útočníci si mohou stáhnout a také nainstalovat nějaký zranitelný produkt, aby vypátrali konkrétní řetězce, které aplikace zobrazuje.
- Bez ohledu na to, jak se řetězce získají, dají se snadno převést na dotaz Googlu, čímž se velmi krátí čas, který má obránce na to, aby web zabezpečil poté, co vešla ve známost jeho zranitelnost.

1.7 Útoky hackerů

V této kapitole se dozvíme něco o dalších útocích, které hackeři provádí proti uživatelům Internetu. Takovýchto druhů útoků můžeme najít celou řadu, proto jsem se snažil vybrat ty nejznámější.

1.7.1 Clickjacking

Clickjacking představuje nebezpečí hrozící ze sítě Internetu pro všechny uživatele, kteří používají jeden z druhů Internetových prohlížečů. Tento útok není žádnou novinkou, hovořilo se o něm již před několika lety.

Uživatel, který se přihlásí na stránku, na které hackeři použili Clickjacking se může proklikat na další stránku Internetu a to zcela nevědomky. Může pak koupit něco přes e-shop, přidat či smazat článek z redakčního systému, zavázat se k nějaké objednávce služeb či zboží atd.

Největší nebezpečí spočívá ve funkci jazyka HTML, který umožňuje vkládat obsah z jiných webových stránek. Nebezpečí představuje pro uživatele oklamání Clickjackingem, který ho donutí klepnout na zdánlivě neškodný internetový odkaz, obrázek či tlačítko, které spustí neočekávanou akci. Existuje více druhů Clicjackingů. Některé druhy používají tzv. iFrames, které vás donutí kliknout na jedno konkrétní místo a jiné naopak překrývají celé stránky. Další druhy pak vyžadují pomoc Javascriptu.[6]

1.7.2 Phishing

Je podvodná technika hackerů, která se snaží pomocí e-mailu získat osobní anebo finanční informace uživatele. Ve většině případů se jedná o informace o platebních kartách, jejich pinech, dále různé přihlašovací údaje podobných služeb nebo jen informace o organizacích, které se zabývají manipulací s penězi. V těchto případech je možné zneužít jejich služeb. Mezi základní znaky phishingového e-mailu patří:

- Vyvolává dojem, že byl odeslán organizací, která se snaží ze svých klientů vylákat důvěrné informace. Tohoto je docíleno zfalšováním adresy uživatele a grafickou podobou e-mailu.
- Zpráva může obsahovat text o provedení nějakého dotazníku, neprovedení platby, výzvy k napsání osobních údajů atd.
- Obsahuje odkaz, který na první pohled vypadá jako odkaz, který odkazuje na stránky organizace. Ve skutečnosti odkazuje na podvodné stránky.

Pokud uživatel otevře odkaz, připojí se na stránky, které vypadají jako stránky banky či jiné organizace. Na stránce je připraven formulář pro vyplnění osobních údajů a dalších

kontaktů. Jedná se zejména o PIN k platební kartě, přihlašovací údaje ke službám a podobně.[7]

1.7.3 Pharming

Je nebezpečnější než Phishing. Pracuje na základě překladu jména serveru na odpovídající IP adresu. Útočí na DNS (Domain Name System). V případě, že uživatel ve svém Internetovém prohlížeči zadá adresu, dojde k překladu na odpovídající IP adresu. Dochází však k překladu na podvrženou, tedy falešnou IP adresu. Právě v tomto překladu na jinou Internetovou adresu je největší nebezpečí, protože podvržená stránka vypadá jako originál. Uživatel, který nic netuší, zadá přihlašovací údaje a tím je odešle útočníkovi.[8]

1.7.4 DNS spoofing

Tento útok představuje zfalšování IP dresy v paketu, který se k nám vrací jako odpověď na žádost o překlad doménového jména na IP adresu. Útok je možné provést i mimo lokální sítě, tedy přesměrovat jej na několik tisíc uživatelů.

Součástí operačních systémů je DNS Resolver, který slouží k překladu doménových jmen. DNS Resolver je sada volání, které se používají při práci s DNS protokolem. Jeho úkolem je pokládat dotazy na DNS server, který máme nastaven v nastavení sítě. Odpovědi se ukládají v lokální DNS Cache pro další potřebu.[9]

1.7.5 Tabnabbing

Tabnabbing je něco podobného jako Phishing. Jedná se o útok hackera, který vychází opět z nepozornosti uživatele. Typický příklad pro Tabnabbing je procházení internetového prohlížeče za účelem hledání informace, výrobku či jen tak surfování po Internetu. Při otevírá spousty záložek (tabech) se nakonec ve většině případů stane, že jich má uživatel otevřených několik a ztrácí kontrolu. Když je nakonec zavírá, tak se v jedné otevře přihlašovací stránka k vašemu e-mailu. Nic netušící uživatel zadá přihlašovací informace do stránky, která vypadá úplně přesně, jak stránka jeho e-mailu. V tomto případě má už údaje útočník.

Většinou se jedná o stránky, které jsou napadené skriptovým trojanem nebo pozměněné pomocí permanentních XSRF a to tak, že spouští Tabnabbingový skript. Pokud se na stránku díváte, není na ní nic podezřelého. Pokud se ale přepnete do jiné záložky, po

určitém čase se změní zpravidla na stránku, kde se přihlašujete k vašemu e-mailu, tedy například centrum, seznam či gmail atd. V tomto případě se sice url změní, ale nepozorný uživatel si toho nevšimne. Po odeslání údajů si útočník vše uloží a přesměruje uživatele na jeho skutečný e-mail. Tímto způsobem získává osobní přihlašovací údaje oběti k e-mailu.[10]

1.7.6 Sniffing

Sniffing patří mezi další hackerské techniky, kterou hackeři používají k ukládání a čtení TCP paketů. Většinou se používá při diagnostice sítě, zjištění používaných služeb a odposlechu datové komunikace. K odposlechu komunikace využívají hackeři několik způsobů. K prvnímu způsobu patří odposlech datové komunikace uvedením síťového hardwaru do promiskuitního modu. Tento způsob nám umožní odposlechnutí a uložení všech příchozích nebo vyfiltrovaných dat. Tento způsob sniffingu se využívá u počítačových sítí, které mají síťové prvky, jakou jsou switch a router. Tato zařízení rozesílají pakety do celé sítě a o data se stará pouze PC, pro které byla data určena.

Dalším způsobem je umístění snifferu mezi dva počítače, nebo servery, mezi kterými probíhá komunikace. Sniffer je program, který monitoruje síťový provoz a je schopen odchytit přenášenou informaci. Existuje celá řada programů, které hackeři používají k tomuto účelu. Mezi nejznámější programy patří Netcat a další nástroje jako je třeba Core Impact. U sniffingu je také velmi nebezpečné, že se dá použít pro odposlouchávání firemní komunikace, kterou pak hacker může použít proti firmě a zpeněžit ji u konkurenční firmy.[11]

1.8 Škodlivé programy

V této kapitole přejdu k popsání jednotlivých škodlivých programů, které nám mohou útočníci prostředním Internetu poslat. Škodlivé programy obecně nazýváme viry. Jedná se o kódy, který se rekurzivně šíří pomocí své změněné kopie, nebo se šíří přímo samy. Viry na počítačích infikují soubory, či systémové prvky, nebo pozměňují odkazy na tyto objekty. Poté, co převezmou kontrolu, se v dalších generacích opět množí. Níže uvádím příklady virů:[12]

Boot viry

Jedny z nejstarší počítačových virů napadaly tzv. boot sektory disků. První takový virus vnikl v roce 1986 a byl vytvořen dvěma pákistánskými bratry na počítači IBM PC. V současné době se tato technika nepoužívá a je také velmi zastaralá. Nicméně tuto techniku uvádím, protože je velmi nebezpečná a hlavně z důvodu, že dokáže infikovat počítač bez ohledu na typ operačního systému, kterým počítač disponuje. Boot viry se zaměřují na startování osobních počítačů, jelikož většina počítačů neobsahuje operační systém v paměti ROM a je tedy nutné ho nahrát například z disku nebo z lokální sítě.

Dříve nebylo nastaveno, odkud se mají operační systémy zavádět. Počítač se tedy pokusil bootovat operační systém z disketové mechaniky, čímž vytvořil příležitost pro aktivaci viru před startem operačního systému.

Souborové viry

Tyto viry napadají spustitelné soubory, tedy programy operačního systému MS-DOS. Napadají soubory s příponou .exe, .bat, .com, .bin, .sys a jiné. Ve většině případů pracují tak, že v programu přepíší část jeho kódu, případně připojí k programu část svého kódu, čímž změní jeho velikost a chování.

Makroviry

Jsou viry, které napadají makra především v aplikacích MS Office. Makra jsou malé programy, které se používají při práci s textovými editory, například pro vkládání textu, atd. Viry využívají makra ke svému šíření a mohou způsobit zvláštní chování počítače, jako je například spouštění některých aplikací, dále pak napadají soubory v počítači či mohou odesílat uživatelovi důvěrné informace.

Polymorfní viry

Fungují na změně vlastního kódu do vysokého počtu odlišných instancí. Tím zajistí, že v napadeném souboru nelze najít typické sekvence kódu. Prvním známým polymorfním virem byl vir 1260, kterého vytvořil pan Mark Washburn ve Spojených Státech v roce 1990. Virus byl založený na zajímavé technice, která používala k dekódování těla viru dva posunující se klíče.

Počítačoví červi

Počítačovým červem označujeme síťový vir, tedy vir, který se v první řadě šíří sítěmi. V nejčastějších případech se na vzdáleném počítači spouští bez vědomí a zásahů uživatele. Dalším případem jsou červi, kteří se rozesílají pomocí e-mailů a naopak potřebují uživatele, aby je spustil otevřením e-mailu. Většinou se jedná o samostatný program, který nepotřebuje hostitele. Někteří červi používají pro své rozšifrování metodu šíření infekcemi souborů, což nám ukazuje, že můžeme červy považovat za podtřídu počítačových virů.

Logické bomby

Logická bomba je výraz pro naprogramovanou chybu běžného programu. Aplikace se například po určitém množství spuštění může sama smazat z disku jako součást schématu ochrany před kopírováním nebo mohou být naprogramovány další druhy škodlivého kódu, které se provedou po případném kopírování.

Kód logické bomby je často ukryt mezi zdrojovými kódy daného programu. Častým případem skrytého kódu jsou velikonoční vajíčka (easter eggs). Programátoři je vytváří proto, aby v nich uvedli údaje o všech členech týmu, pracujících na vývoji nějakého produktu. Tato vajíčka nejsou v zásadě nijak škodlivá a vůbec uživatele neohrožují. Ovšem v mnohých případech mohou zbytečně zabírat prostor na disku.

Trojští koně

Trojský kůň je program, který se snaží uživatele něčím zaujmout a vytvářet dojem užitečnosti. Cílem je, aby uživatel tento program spustil na svém počítači. V jiných případech hackeři přidávají k běžným programům nějakou dodatečnou funkčnost, jako kamufláž svých aktivit, aby pak mohli lépe vypátrat daný systém a používat jej.

Mezi další škodlivé programy řadíme například Dialery, jejichž hlavním úkolem je přinutit uživatele, aby platil za použití telefonních linek se speciálním cenovým tarifem. Dále můžu uvést Stahovače, což jsou programy, které instalují nové programové položky na cíl útoku a způsobují stahování škodlivého obsahu z webových stránek. Do škodlivých programů dále řadíme Floodery a Rootkity. Floodery se používají hackery pro útoky na síťové počítačové systémy a pomocí těchto programů se generuje nadměrný síťový provoz, což vede k DoS útoku. Rootkity jsou speciální sady hackerských pomůcek, které se využívají poté, co hacker získá přístup k systému (včetně administrátorských práv).

2 ZABEZPEČENÍ POČÍTAČŮ A LOKÁLNÍCH SÍTÍ

V předchozích kapitolách jsem popsal nejrůznější metody a techniky hackerů, které používají hackeři k nabourání osobních počítačů nebo počítačových sítí. Dále se chci zaměřit na to, jak je možné se proti činnosti hackerů bránit. Zejména se zaměřím na ochranu počítačové sítě. Dříve, než přejdu k samotné ochraně počítačové sítě, popíšu protokoly, které tvoří základ komunikace v počítačových sítích.

2.1 Protokoly

Protokoly slouží ke vzájemné komunikaci v počítačové síti. Základní skupinu protokolů označujeme jako TCP/IP. Tato skupina vytváří základ mezisíťové komunikace a je zároveň základem komunikace na Internetu. Některé protokoly ze skupiny TCP/IP potom také zajišťují zabezpečený přenos dat.[13]

FTP protokol

FTP (File Transfer Protocol) je protokol ze skupiny protokolů TCP/IP. Je určen pro přenos souborů mezi počítači, ale dá se také využít při odesílání webových stránek, při vytváření webu či při umisťování fotografií na server.

Protokol používá dva kanály typu klient/server. Pomocí příkazového kanálu posílá uživatel požadavek na server, například na výpis nějaké složky či stažení souboru. Server tento požadavek vždycky očekává na portu 21. Dále pak protokol používá datový kanál, kterým se přenáší požadovaná data. U datového kanálu je zvláštnost, že se může role serveru a klienta obrátit. Právě proto se rozeznávají dva režimy komunikace u protokolu FTP, a to aktivní a pasivní.

Aktivní a pasivní režim komunikace je určen podle toho, kdo při spojení otevírá datový kanál. V případě, že datový kanál otevírá server, jde o režim komunikace aktivní, pokud datový kanál otevře klient, jedná se o režim komunikace pasivní. V aktivním režimu komunikace musí klient sdělit serveru svou IP adresu a port, na kterém bude očekávat příchod dat ze serveru. Při komunikaci pasivní, musí nejprve klient požádat příkazem PASV server, aby přešel do pasivního režimu komunikace. Pokud vše proběhne v pořádku, server pošle přes řídící kanál odpověď s uvedením IP adresy a portu, kde bude datové spojení realizováno.

Bezpečnostní problém nastává při připojování protokolu FTP, protože přihlašovací údaje, tedy jméno a heslo jsou přenášeny v textové podobě, je tedy možné je odchytit. Toto může mít za následek, že přenášená data mohou být zcizena nebo upravena. Často se objevují zprávy o tom, že se hackeři nabourali k serverům, protože získali, nebo tedy spíše zachytili nešifrované FTP heslo. [13]

Bezpečnost u protokolu FTP je řešena pomocí bezpečnostních protokolů přidružených k základnímu protokolu FTP. Mezi ně patří zejména protokol FTPS (File Transfer Protocol Security), který představuje šifrovaný komunikační protokol pro přenos dat. Pro využití této služby je potřeba mít na PC nainstalovaný klient s podporou FTPS. Dále sem řadíme protokol SCP (Secure Copy Protocol), který slouží k bezpečnému přenosu souborů mezi dvěma počítači propojenými počítačovou sítí pomocí protokolu SSH (Secure Shell). Protokol SSH se používá pro bezpečnou komunikaci mezi dvěma počítači v síti Internetu s tím ale, že zajišťuje autentizaci obou účastníků, šifrování přenášených dat atd. Opět je nutné mít na svém počítači při využívání této služby nainstalovaný klient s podporou SCP.

HTTP protokol

Protokol HTTP (Hypertext Transfer Protocol) je nejpoužívanějším protokolem na Internetu. Slouží pro vyhledávání informací na Internetu, dále pak k přenosu hypertextových dokumentů a obrázků.

Základ komunikace u protokolu HTTP je opět komunikace klient/server. V zásadě to funguje tak, že uživatel zapíše do okna prohlížeče požadovanou internetovou adresu, kterou chce prohlížet. Poté klient z identifikátoru objektu zjistí jméno serveru, které přeloží pomocí DNS na IP-adresu. Po získání IP-adresy, klient naváže spojení se serverem pomocí protokolu TCP.

Jedná se o komunikaci, která se skládá z dotazu a odpovědi. Relace mezi klientem a serverem je tvořena vždy pouze dotazem a odpovědí na tento dotaz. Starší verze protokolu HTTP navazovaly spojení protokolem TCP pouze na jednu relaci, a to dotaz – odpověď.

Riziko u protokolu HTTP představuje přenos dat, kdy data jsou přenášena jako obyčejný text. Lze je tedy opět jednoduše zachytit a zneužít je pro vlastní účely. Existuje protokol HTTPS (Hypertext Transfer Protocol Secure), který tento problém řeší. HTTPS je nadstavbou protokolu HTTP, nejedná se tedy o zvláštní protokol. Přenos dat probíhá

v rámci protokolu HTTP, ale s tím rozdílem, že data se nepřenášejí jako obyčejný text, ale jsou šifrována pomocí SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security).

SSL protokol najdeme mezi protokoly TCP/IP a HTTP. Je to Internetový protokol používaný pro servery a klienty. Umožňuje bezpečnou datovou komunikaci mezi SSL-serverem a SSL-prohlížečem. Pod pojmem bezpečná datová komunikace se rozumí ověření serveru, šifrování a datová integrita. TLS je také kryptografický protokol, který je nástupce protokolu SSL. Oba protokoly jsou si velmi podobné a mají za úkol zabraňovat při komunikaci odposlouchávání a falšování zpráv. TLS zvláště zajišťuje autentizaci serveru, což představuje velmi důležitý bezpečnostní fakt při komunikaci, protože druhá strana, tedy klient, si může být jistý, že komunikuje opravdu s tím pravým serverem.

Šifrování dat představuje ochranu proti sledování paketů, případně odposlouchávání komunikace mezi dvěma uzli sítě.

Poštovní protokoly SMTP, POP a IMAP

Posílání e-mailových zpráv v síti Internet zajišťuje protokol SMTP a software typu MTA (Message Transfer Agent), což je poštovní server. Jsou dvě možnosti ukládání e-mailových zpráv, a to buď na straně serveru, nebo na straně klienta. V případě, že uživatel má na svém počítači nainstalovaného e-mailového klienta, přistupuje k e-mailovým zprávám bez použití webového rozhraní. K tomuto účelu se používají protokoly POP a IMAP. Uživatelé, kteří e-mailového klienta nemají nainstalovaného na svém počítači, přistupují ke svým zprávám přes webové rozhraní k poštovním serverům, kde jsou jejich zprávy uloženy. Tento způsob využívají bezplatné e-mailové služby, jako je seznam, gmail, centrum atd.

SMTP

Součástí protokolů TCP/IP je i řešení elektronické pošty, která je založená na přenosovém protokolu SMTP. Podle protokolu SMTP (Simple Mail Transfer Protocol) je pak pojmenována celá koncepce a nazývá se „SMTP pošta“.[14]

Ze začátku tato služba byla určena čistě pro přenos krátkých textových zpráv, které byly psané v tzv. ASCII kódu, což je kód, který obsahuje znaky znázorněné v sedmi bitech. V současnosti je požadavek ale i na přenos jiných věcí, než jsou jenom krátké textové zprávy psané výhradně pomocí ASCII znaků. U protokolu SMTP je to vyřešeno tak, že všechno, co není čisté ASCII, se jednoduše přetransformuje tak, aby to mělo tvar čistého

ASCII textu. Na druhé straně dochází pak k opačné transformaci, která vše vrátí do původního stavu.

Jednou z velkých nevýhod, která představuje bezpečnostní riziko u protokolu SMTP je, že se nekontroluje žádné uživatelské jméno a heslo, není tedy standardně zajištěna autentizace přístupu. Existuje samozřejmě možnost, jak tento problém řešit. Jednou z možností je použití protokolu SASL (Simple Authentication and Security Layer), který nám definuje autentizaci pomocí hesla. Toto heslo je posíláno opět v otevřené podobě, je tedy vhodné celý přenos zašifrovat například pomocí funkce MD5, kdy se pak po síti neposílá heslo, ale jen kontrolní součet spočítaný právě metodou MD5 z hesla a z dohodnutého řetězce.[15]

Další variantou pro zašifrování celého spojení je opět využít protokolu SSL, který je popsán výše. U poštovního serveru to funguje tak, že všechny údaje, které se vyměňují mezi poštovním klientem a serverem jsou šifrovány s digitálním ověřením, takže je zajištěno, aby nikdo nemohl ukrást vaše přihlašovací údaje k e-mailu.

Co se týče dalšího zabezpečení odchozí pošty, je také možnost nastavení serveru odchozí pošty pouze v rámci vnitřní sítě. Je však pořád nebezpečí, že některý z uživatelů může poslat e-mail pod falešnou identitou, bude se tedy vydávat za někoho jiného. Tento druh zabezpečení využívá naše škola.

POP3

Post Office Protocol verze 3 je Internetový protokol, který slouží pro vyzvedávání e-mailů z poštovních schránek. Klient navazuje spojení na TCP port 110 serveru. Po navázání spojení čeká server na autentizaci uživatele, který tedy probíhá pomocí přihlašovacího jména a hesla. Pokud je vše v pořádku, komunikace přechází do takzvaného transakčního stavu, kdy klient může pracovat se zprávami ve své poštovní schránce na serveru.

Klient si stáhne ze serveru zprávy, které může číst již bez nutnosti internetového připojení. Klient si může vybrat zprávy, které chce přečíst, ostatní zprávy zůstávají uloženy na serveru. Nevýhodou protokolu POP3 jsou nešifrované přihlašovací mechanismy, které přestavují bezpečnostní riziko. S vývojem protokolu POP3 se kvůli těmto bezpečnostním chybám začalo pracovat na autentizaci a ověřování neoprávněného přístupu k cizí poštovní schránce. Jednou z autentizačních metod je APOP, který využívá hashovací funkci MD5, která se využívá pro zabezpečený přenos hesla od klienta na server. Je zde také možnost celou komunikaci šifrovat použitím SSL.

IMAP

Internet Message Access Protocol verze 4 je protokol, který se používá pro vzdálený přístup k e-mailové schránce. Na rozdíl od protokolu POP3 vyžaduje trvalé připojení k síti Internetu, ovšem na druhé straně uživateli nabízí možnosti vzdálené správy, jako je např. přesouvání zpráv, práce se složkami a další. Na počítač se stahují jen nezbytné informace, samotné zprávy a složky, které jsou uložené na poštovním severu, takže se stahují jen záhlaví určitých zpráv a jejich obsah jenom tehdy, když si je chce uživatel přečíst. Protokol také umožňuje připojení více klientů. [16]

IMAP je mnohem komplikovanější protokol a jeho implementace je složitější a náchylnější k chybám než implementace POP3. V případě, že ukládací a vyhledávací algoritmy na serveru nejsou bezpečně implementovány, prohledávání velké schránky může zatěžovat server a IMAP klienti mohou také způsobit zpoždění při vytváření nových zpráv u pomalejších připojení. Výhody oproti POP3 má IMAP následují:

- Dovoluje současně připojení více uživatelů k jedné schránce.
- Umožňuje vidět provedené změny ostatními klienty.
- IMAP klienti mohou pracovat se složkami na serveru a přenášet zprávy mezi schránkami.
- Dovoluje klientům udržovat přehled o zprávách, zda byly přečteny, smazány atd.

K dalším zabezpečením e-mailových zpráv patří nástroje S/MIME a PGP. Jeden z nejznámějších nástrojů je PGP (Pretty Good Privacy). Autorem PGP je pan Phil Zimmerman, který vytvořil tento nástroj pro šifrování elektronické pošty prostřednictvím šifrovacího procesu veřejným klíčem. S/MIME (Secure/Multipurpose Mail Extensions) je standard pro šifrování s veřejným klíčem a podepsáním MIME dat. Používání MIME je ve spojení s certifikační autoritou. Oba protokoly jsou postaveny na algoritmech společnosti RSA Data Security, Inc.

2.2 Ochrana počítačových sítí

Hlavním a tím nejdůležitějším úkolem ochrany počítačové sítě je zabezpečit, lépe řečeno kontrolovat přístup na síť a zajistit utajení dat. Zvláště při přenosu jsou data velmi zranitelná a často bývají vystavena útokům hackerů. Je tedy hlavní otázkou, jakým

způsobem mezi sebou komunikovat, jak vyměňovat informace a současně přitom kontrolovat přístup na síť tak, aby komunikace probíhala zabezpečeně.[17]

V této kapitole chci uvést některé metody, které se používají k oddělení lokální sítě od sítě Internetu. Ještě předtím ale přikládám tabulku, ve které jsou požadavky na bezpečnost a jejich řešení v současnosti, viz Tabulka 2.

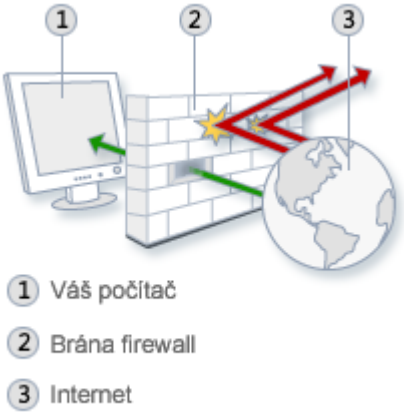
Požadavek na bezpečnost	Možné řešení	Realizace	Výsledek
Ochrana důvěryhodných dat	Zašifrování	Symetrické a asymetrické šifrování	Zakódování dat
Odhalení falešné identity	Ověření pravosti	Digitální potvrzení	Ověření identity
Zajištění nedoknutelnosti dat	Ověření pravosti	Digitální potvrzení	Ověření identity
Znemožnit neoprávněný přístup	Systém firewall	Firewally, VPN, hesla	Filtry (odmítnutí nebo vypuštění)

Tabulka 2 Požadavky na bezpečnost sítě

Kvalitní bezpečnostní systém je takový, který používá naráz všechny technologie uvedené výše v tabulce. Kombinace těchto různých technologií zajistí efektivnost bezpečnostního systému. Některé nástroje uvedené v této kapitole jsou popsány již v předchozí části práce. Nicméně ve výše uvedeném textu se jednalo o to, jak tyto nástroje používají hackeři ke své činnosti. Zde si rozebereme některé funkce těchto nástrojů, které nám pomohou zabezpečit síť právě proti hackerům a jiným útokům ze sítě Internetu.

2.3 Ochrana pomocí systému Firewall

Každá počítačová síť připojená do sítě Internetu by měla mít systém firewall. Je to jeden z hlavních ochranných nástrojů, které slouží jako obrana sítě proti hackerům a dalším útokům. Firewall je software nebo hardware, jehož hlavním úkolem je kontrolovat všechny informace přicházející ze sítě Internetu a na základě nastavených pravidel uživatele, tyto informace buď přijmout, tedy je pustit do PC, nebo je zamítnout. Grafické znázornění systému firewall je níže, viz Obrázek 1.



Obrázek 1 Brána firewall

Firewall můžeme umístit mezi intranet a Internet, nebo může fungovat mezi síťovými podsystémy uvnitř intranetu. Odborníci na informační technologie uvádí, že samotný firewall není těžké zkonstruovat, ale potom ho správně řídit.

Firewall představuje víceúrovňovou ochranu počítačové sítě a ochranu specifických aplikací, jako jsou poštovní nebo souborové servery. Je tedy vhodné, aby se správci sítí snažili víceúrovňovou ochranu firemní sítě vytvořit. Právě k tomuto tématu níže popisuji další nástroje, které slouží pro správce sítí k zabezpečení sítě. Mezi ně patří zejména filtrování paketů, proxy server, nastražený server a vytvoření podsítě.[17]

Filtrování paketů

Zařízení, které se používá k filtraci paketů je ochranný směrovač (screening router). Ve většině případů bývá umístěn mezi sítěmi a vytváří tak ochranu mezi sítěmi a sítí Internetu. Jeho hlavním úkolem je filtrovat pakety, které jdou se sítě Internetu do intranetu. Směrovač dále těmto příchozím paketům buď povolí přístup, nebo jej zamítá. Rozhoduje se tak na základě porovnání informace v záhlaví paketu se stanovenými pravidly správce sítě.

Proxy server

O Proxy server jsme se bavili již v předchozích kapitolách. Teď se ale zaměřím na to, jak nám může Proxy server pomoci k ochranně počítačové sítě proti útokům hackerů. Podobně jako směrovač může také Proxy server kontrolovat příchozí datový provoz. Kontrolují pravidla, která stanovuje administrátor a teprve poté, povolují další provoz dat. Proxy

serverů je několik druhů. Máme například mail Proxy server pro ochranu mail serveru, nebo FTP Proxy server, který hlídá FTP server.

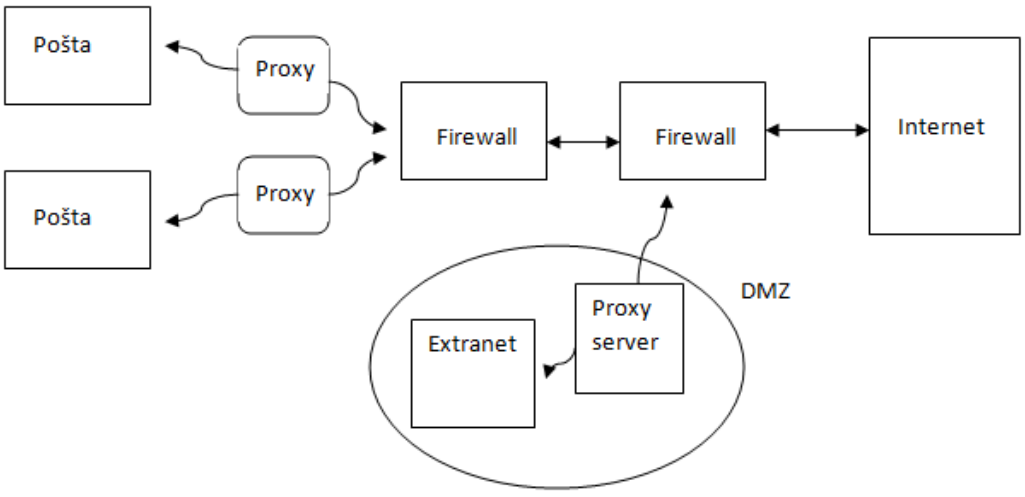
Proxy servery také kontrolují obsah paketů a buď je přijmou, nebo zamítnou. Pokud by Proxy server našel v žádosti příkaz, u kterého má administrátor nastaveno nepouštět žádný takový soubor obsahující tento příkaz, tak ho Proxy server zamítne.

Nastražený server

Nastražený server je takový „obětní beránek“, který představuje úmyslně nastražený server proti útočníkům. Většinou bývá umístěný izolovaně, nebo se v síti umístí před systémem firewall. Důležité je, že by měl obsahovat informace pouze na jedno použití. Tyto servery se používají hlavně z důvodu, že množství pozornosti, které servery přitahují, je indikátorem možné pozornosti, kterou může přitahovat Vaše vlastní síť. Ze zjištěných informací, které se provedou na serverech, může pak vycházet administrátor při realizaci ochranných opatřeních.

Podsíť (sub-net)

Jedná se o vyčleněnou oblast uvnitř chráněné oblasti. Obvykle bývá tato síť chráněna systémem firewall, složeného se směrovače a Proxy serveru. Tento typ sítě, která je vyčleněna od hlavní sítě se říká také Demilitarizovaná zóna (DMZ)[17]. Obvykle se používá k tomu, aby se zabránilo uživatelům firemní sítě navštěvovat ostatní části intranetu podniku, případně k ochraně vysoce důvěryhodných obchodních dat proti hackerům. Chráněná podsíť je zobrazena na obrázku, viz Obrázek 2.



Obrázek 2 Chráněná podsíť[17]

2.4 Autentizace dat

Pod pojmem autentizace si můžeme představit dva problémy. První problém spočívá v rozpoznání uživatele a druhý v ověření dat. Dále do této oblasti patří šifrování dat, použití hesel a digitálních podpisů.[17]

2.4.1 Řízení přístupu

Řízení přístupu představuje činnost, u které se musíme rozhodnout, na jaké úrovni budeme přístup blokovat. Jedná se zejména o oblasti operačního systému, adresáře, serveru a souboru. Přístup k souborům, řadičům, serverům, adresářům, jednotlivým souborům či částem souborů v počítačové síti může být povolen, nebo zamítnut.

První stupeň zabezpečení začíná v okamžiku, kdy se uživatel přihlásí na síť. Pokud vloží své uživatelské jméno a heslo, server zkontroluje, jaké přístupové povolení má uživatel povoleno. Je tedy puštěn do serverů, adresářů a souborů, které může navštívit. Pokud se odhlásí ze sítě, provede se řádný výstup a uzamkne se.

Další ochranu představuje databáze kontrolovaného přístupu ACD (Access Control Database). Databáze prověřuje síťové objekty a jejich vlastnosti. Tyto vlastnosti určují, jak se objekty budou chovat a kdo k nim bude mít přístup.

2.4.2 Heslo

Heslo patří mezi základní formu ověření identity uživatele. Administrátoři radí uživatelům, aby se vyhýbali druhům slov při vytvoření hesla, jako jsou jména jejich příbuzných, domácích mazlíčků. Bohužel existuje několik hesel, které jsou snadno zapamatovatelné a tedy i snadno rozluštitelné. Mezi hackery existuje několik programů, které se zabývají rozluštěním hesel. Například do těchto programů řadíme program password trap. Dále hackeři často používají metodu war dialer, která spočívá v tom, že se server bombarduje množstvím hesel a jedno z hesel bude možná to správné.

Kvalitní heslo musí obsahovat kombinaci písmen a číslic. Musí mít také požadovanou délku, příliš krátká hesla jsou často velmi rychle rozluštitelná. Někteří z uživatelů, kteří jsou v síti, nemají na svých osobních počítačích hesla do Windows a podobně. Opět je proniknutí do jejich operačního systému mnohem jednodušší.

2.4.3 Elektronický podpis

Elektronický podpis se používá jako jeden z hlavních nástrojů identifikace a autentizace osob v prostředí Internetu. Jde v podstatě o údaje v elektronické podobě, které se připojují k datové zprávě a slouží nám jako metoda určení identity podepsané osoby ve vztahu k datové zprávě.[18]

Můžeme ho využít zejména při přihlášení a odhlášení k nemocenskému pojištění, podání přehledu o příjmech a výdajích OSVČ, přiznání k DPH, komunikaci se státní správou, krajskými a městskými úřady, komunikaci se zdravotními pojišťovnami, žádosti o sociální dávky, podávání žádostí o dotace EU, podepisování faktur, podepisování PDF dokumentů nebo při podepisování e-mailů.

V České republice je elektronický podpis zakotven v zákoně číslo 227/2000 Sb., který upravuje v souladu s právem Evropských společenství, používaní elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

Elektronický podpis musí splňovat následující požadavky:

- Je jednoznačně spojen s podepisující se osobou.
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
- Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Elektronický podpis se používá s certifikáty, které zajišťují identitu člověka. Bezpečnost dat je zajištěna asymetrickým šifrováním, u kterého si uživatel vygeneruje dvojici klíčů pomocí běžně dostupných SW produktů. Pro šifrování se používá veřejný klíč a pro dešifrování pak klíč privátní (soukromý).

Certifikáty se rozdělují podle účelu a to na osobní, serverové, kvalifikované, kvalifikované systémové a komerční. Certifikáty vydává třetí strana, nazývá se „Certifikační autorita“. Mezi certifikační autority například patří CA Czechia, která vydává osobní a komerční certifikáty, dále pak První certifikační autorita a.s., která vydává všechny typy certifikátů a

jako poslední ještě uvedu Českou poštu, která vydává kvalifikované a kvalifikované systémové certifikáty.

Postup pro zřízení certifikátu je u všech certifikačních autorit podobný, jako příklad uvedu zřízení certifikátů pro fyzické osoby. Nejprve si fyzická osoba musí připravit podklady pro uzavření smlouvy a vydání certifikátu, poté navštívit příslušné kontaktní místo certifikační autority, kde dojde k uzavření smlouvy, zavedení do jejich systému a vydání certifikátu.

Po vytvoření elektronické žádosti o vydání certifikátu vzniká pár klíčů – privátní a veřejný klíč. Pro správné používaní vašeho certifikátu musíte mít k dispozici jemu příslušný soukromý klíč, který slouží pro vytvoření vlastního elektronického podpisu. Je doporučeno provést zálohu tohoto privátního klíče a to proto, aby po vydání příslušného certifikátu nenastaly problémy s jeho používáním.[19]

V případě, že uživatel nepoužívá pouze PC, ale hardwarové řešení, jako je čipová karta nebo USB token, soukromý klíč je umístěn na tomto médiu a zálohu není třeba provádět.

Certifikační autority si za vydání elektronického podpisu účtují poplatek, většinou se cena pohybuje ve stovkách korun. Například co se týká kvalifikovaného osobního certifikátu, který vydává Česká pošta, částka za vydání certifikátu je 396 Kč. Tato částka je aktuální pro květen 2012, v budoucnu se může změnit.[20]

II. PRAKTICKÁ ČÁST

3 ZABEZPEČENÍ OPERAČNÍCH SYSTÉMŮ WINDOWS XP A WINDOWS 7

Úkolem v mé práci je prozkoumat zabezpečení vybraných nejpoužívanějších operačních systémů. Vybral jsem si operační systémy Windows 7 a Windows XP, protože patří mezi ty nejpoužívanější operační systémy. Rozdělil jsem tuto kapitolu na dvě části, aby bylo jasné, jaké jsou rozdíly mezi těmito systémy.

3.1 Operační systém Windows XP

Operační systém Windows XP patří mezi starší systémy, ale můžeme ho na osobních počítačích uživatelů ještě najít, zvláště také proto, že jeho nástupce, operační systém Windows Vista, byl v minulosti mnohokrát kritizován ze strany uživatelů PC. Windows XP byl společností Microsoft postupně vylepšován v podobě aktualizací, kterým se říká Servis Pack. Tyto balíčky jsou tři. Vybral jsem si verzi Windows XP se Servis Packem 3, tedy nejnovější verzi.[23]

Windows XP Service Pack 3

Service Pack 3 je poslední service pack. Obsahuje několik oprav, které se týkají také bezpečnosti systému. Mezi nové služby patří:

Network Access Protection (NAP)

Funkce pro ochranu síťového přístupu. Její hlavní úkol je kontrolovat systémy, které se připojují do hlídané sítě. Kontroluje stav klientova zabezpečení a požadavek administrátora.

Detekce Black Hole Routerů

Black hole je v překladu černá díra. Zajišťuje, že v ní mizí pakety. Konkrétně tedy pakety zahazuje, aniž by počítač vrátil ICMP odezvu. Takováto funkce pomáhá při detekci routerů a chrání uživatele před jejich působením. Pro detekci black hole routeru se používá příkaz PING se správnými parametry.

Microsoft Kernel Mode Cryptographic Module (KMCM)

Je to modul, ke kterému mohou přistupovat ovladače až na úrovni jádra a využívají jeho šifrovací algoritmy. Využívá se pro vyšší zabezpečení. Pomocí KMCM mohou například

administrátoři implementovat druhou – šifrovanou vrstvu zabezpečení nad NAP. Použitý algoritmus je 3DES, který je přístupný skrze jádro operačního systému.

Bezpečnostní prvky, které obsahuje systém, jsou zde na rozdíl od Windows 7 soustředěny do Centra zabezpečení, nikoli do Centra Akcí, viz Obrázek 3.

Obrázek 3 Centrum zabezpečení

Mezi hlavní bezpečnostní prvky u Windows XP patří:

Ochrana proti virům

Windows XP, stejně jako každý operační systém, musí být chráněn antivirovým programem. V okně „Centrum zabezpečení“ je možné zkontrolovat, jestli systém opravdu antivirový program má, nebo nikoli. Opět uživatel může sáhnout do skupiny placených nebo neplacených antivirových programů.

Brána firewall

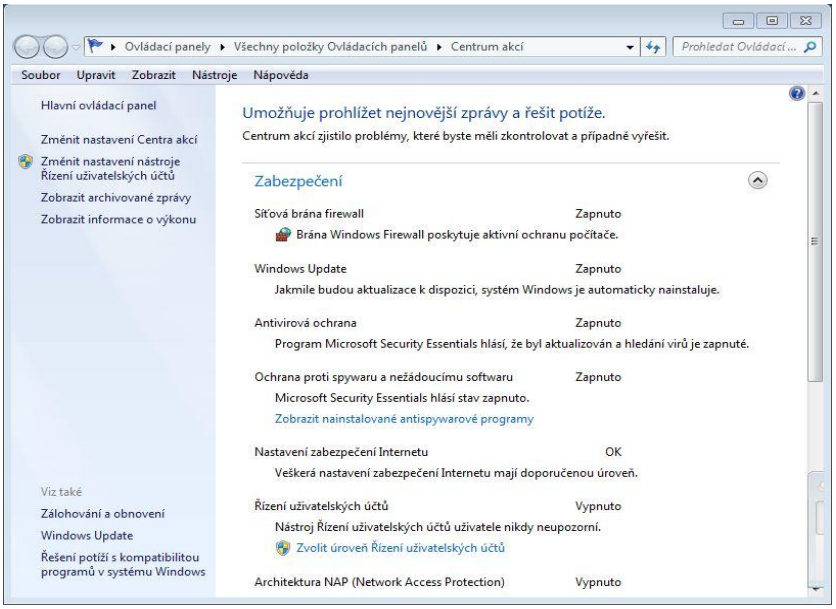
Operační systém Windows XP obsahuje bránu firewall již od Servis Packu 2, kde byla oproti Servisu Packu 1 zapnuta implicitně a v mnohém vylepšena, zvláště v oblasti kontroly odchozího provozu. Nástupem Servis Packu 3 se možnosti nastavení firewallu a činnost ještě zlepšuje.

Automatické aktualizace

Automatické aktualizace je možné sledovat v „Centru zabezpečení“. Aktualizace probíhají automaticky, ale je možné nastavit frekvenci pravidelných kontrol, případně je vypnout úplně, což ale společnost Microsoft nedoporučuje.

3.2 Operační systém Windows 7

Operační systém Windows 7 obsahuje celou řadu funkcí a nástrojů, které slouží k zabezpečení systému. Od předchozích operačních systémů, jako je Windows Vista a XP, se zabezpečení liší. Zejména se jedná o jednodušší rozhraní a funkcionalitu. Všechny funkce a nástroje, které se týkají bezpečnost v operačním systému Windows 7, najdeme v ovládacích panelech v *Centru Akcí*, viz Obrázek 4. Na její přítomnost nás upozorňuje bílá vlaječka v oznamovací oblasti, která nám sděluje, že Centrum Akcí plní svoji povinnost.



Obrázek 4 Centrum akcí

Mezi hlavní bezpečnostní prvky u Windows 7 patří:

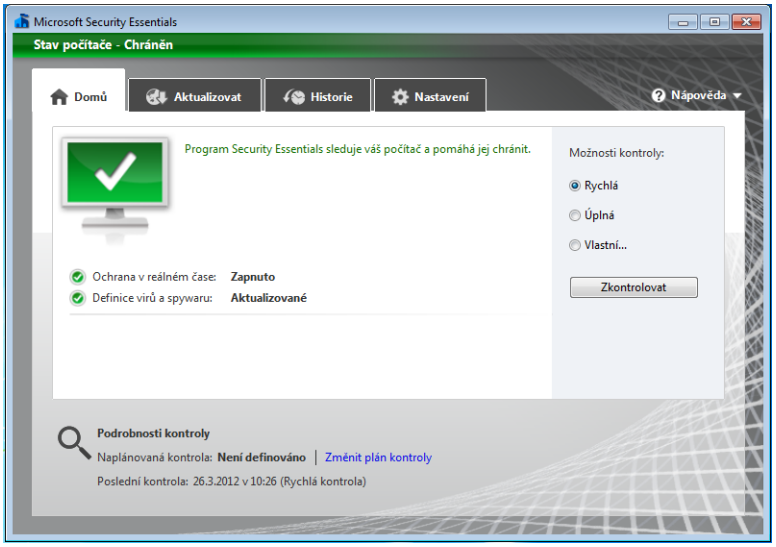
Brána Windows Firewall

Brána Windows Firewall je vylepšena o více přístupových profilů, je tedy možné být připojen a zároveň chráněn při připojení k více sítím. To zajišťuje, že správci mají mnohem větší kontrolu nad pravidly a dalším nastavením firewallu. Ve srovnání s bránou firewall v operačním systému Windows XP došlo k několika změnám:[24]

- Brána Windows Firewall podporuje sledování a řízení jak příchozího, tak odchozího síťového provozu.
- Nabízí více možností konfigurace a lze ji nastavovat i vzdáleně. Lze také konfigurovat protokol IPsec (Internet Protocol Security), což je mechanizmus pro autentizaci, šifrování a filtrování síťového provozu.
- Lze nastavit pravidla brány firewall i pro služby, účty a skupiny Active Directory, zdrojové a cílové IP adresy pro příchozí a odchozí provoz, přenosové protokoly jiné než TCP a UDP, atd.
- Používá tři profily. Jiný profil se použije při připojení do domény (doménový), jiný, pokud jste připojeni do sítě bez domény (privátní), a poslední při připojení k veřejné síti (veřejný).

Antivirový program

Antivirový program patří mezi hlavní bezpečnostní prvky systému. Zabraňuje proniknutí škodlivých programů do systému. Společnost Microsoft přímo nabízí svůj vlastní antivirový program, a to Microsoft Security Essentials, viz Obrázek 5. Můžete si samozřejmě nainstalovat vlastní antivirový program, nebo vyhledat na stránce w7io.com/1510, která obsahuje odkazy vedoucí k vydavatelům antivirového softwaru kompatibilního se systémem Windows 7. Tento odkaz lze nalézt v „Centru akcí“.



Obrázek 5 Microsoft Security Essentials

Nástroj řízení uživatelských účtů (UAC)

Tento nástroj snižuje nebezpečí, které hrozí, pokud uživatel pracuje na počítači jako správce a má přístup prakticky kamkoliv. Pro běžné užívání PC stačí používat standardní účet. Je tedy na správci, aby pro své uživatele vytvořil účty, které nemají oprávnění správce, ale standardního účtu.

Program Windows Defender

Windows Defender je antispywarový program. Jeho úkolem je monitorovat systém a zamezovat instalaci spywaru a také varovat uživatele v případě, že detekuje spyware. Kromě ochrany proti spywarovému chování programů, provádí Windows Defender i pravidelné kontroly souborů v počítači a hledá mezi nimi známý spyware.

Šifrování dat

Windows 7 obsahuje nástroj BitLocker Drive Encryption, který slouží pro šifrování pevného disku. Z důvodu krádeže počítače nabízí Windows 7 tento nástroj pro zašifrování pevného disku. Tato funkce je k dispozici pouze v edicích Enterprise a Ultimate. Pro zašifrování vyměnitelných disků se používá funkce BitLockerToGo.

Přesměrování dat

Aplikace, které se pokoušejí zapisovat do chráněné systémové složky, jsou přesměrovány do úložiště virtuálních souborů. V případě aplikací, které se pokouší zapsat do společných systémových oblastí registru, jsou přesměrovány do virtuálních klíčů, které můžeme najít v části registru příslušného uživatele. Tato funkce zabraňuje škodlivým aplikacím v zápisu do oblastí, kde by mohly způsobit havárii celého systému.

Rodičovská kontrola

Rodičovská kontrola je nástroj, který pomáhá rodičům vést své děti při používáním Internetu, her a dalších programů.

Přídavná bezpečnost na 64bitových počítačích

Na těchto verzích systému je možné nainstalovat pouze digitálně podepsané ovladače zařízení. Tento nástroj se nazývá PatchGuard, jeho hlavním úkolem je chránit jádro, aby nedošlo k jeho modifikaci.

Ochrana proti přetečení zásobníku

Technika ASLR (Address Space Layout Randomization) zajišťuje, že při každém spuštění systému Windows se načte systémový kód do jiných paměťových oblastí. Tato změna blokuje útoky od hackerů, které se snaží volat systémové funkce, které se nacházejí ve známých oblastech. Funkce ASLR je jedním z výsledků přijetí konceptu Security Development Life Cycle, což představuje proces, který má za cíl minimalizovat chyby v programovém kódu.

Architektura NAP (Network Access Protection)

Architektura NAP je platforma, kterou využívají správci sítě k zabezpečení podnikové sítě. Ochrana spočívá v tom, že pokud se chce někdo připojit k podnikové síti, která využívá architektury NAP, bude jeho počítač nejprve zkontrolován, zda obsahuje požadovaný software, potřebné nastavení a jestli má tyto položky aktuální.

3.3 Doporučení pro zabezpečení systému

Každý kvalitně zabezpečený operační systém musí mít nainstalovaný antivirový program. Bez této ochrany je počítač připojený do sítě Internetu velmi zranitelný proti škodlivým programům. V současné době máme na trhu antivirové programy placené a neplacené. Záleží na uživateli, kterou skupinu antivirových programů si vybere. Do placených antivirových programů patří například *ESET NOD32 Antivirus-Verze 5*, *ESET SMART Security 5* a další. Mezi neplacené antivirové programy patří například *Microsoft Security Essentials* a *AVG Anti-Virus Free 2012*.

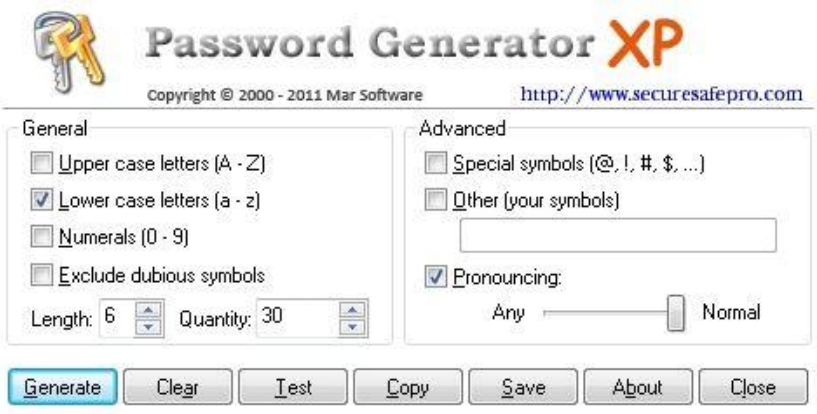
Mezi další prvky, které tvoří nedílnou součást operačního systému, je systém Firewall. Je to zařízení, které odděluje dvě sítě a řídí jejich provoz pomocí definování různých pravidel. Operační systémy Windows obsahují systém firewall od verze Windows XP Service Pack 2. Poté se s každou novou verzí operačního systému tato ochrana zkvalitňuje. Mezi známé firewally patří například *Comodo Internet Security, Windows 7 Firewall Cont*rol a *Privatefirewall*.

Dalším bezpečnostním krokem je rozdělení pevného disku. Při koupi nového disku je disk rozdělen na jediný diskový oddíl, protože toto rozdělení je výhodné pro výrobce disků z důvodu jednoduché manipulace s daty na disky, atd.

Pro uživatele toto rozdělení je ovšem nevhodné, protože máme na disku uloženy pohromadě programy, operační systém a data. Optimální rozdělení je mít odděleně operační systém a data, protože v případě havárie systému bychom instalovali jen operační systém. Všechno ostatní by zůstalo zachováno. Také je toto rozdělení vhodné pro zálohování dat, protože nemusíme zálohovat celý disk, pouze ten oddíl, kde máme data uložena.

Heslo do systému je opět dalším bezpečnostním prvkem, který by měl každý systém mít. Je spousta uživatelů, kteří se do systému po startu PC přihlašují automaticky, tedy bez hesla. Nastavení hesla je první krok, jak zabránit, aby se do vašeho systému nedostal cizí uživatel. Hesla by měla být kombinace velkých, malých písmen, čísel a interpunkce. Délka hesla by měla být minimálně 8 znaků, avšak čím více znaků, tím lépe. Někteří odborníci doporučují použít jako heslo frázi, která bude opět kombinací čísel, písmen a znaků.

K vytvoření kvalitního a bezpečného hesla, nám mohou pomoci programy, kterým se jmenují generátory hesel. Jsou to v podstatě programy, které patří mezi specializované nástroje pro práci s hesly a jejich detailním nastavením. Jejich úkolem je vygenerovat silné a bezpečné heslo, které můžeme použít jako heslo do systému nebo k ostatním službám. Jedním z takovýchto programů je Password Generator XP, který je rozdělen na dvě sekce. V první sekci si uživatel pomocí funkcí programu nastavuje, zda bude mít heslo velká či malá písmena, zda bude obsahovat číslice či vynechá od sebe hůře rozpoznatelné symboly, jakou bude mít délku hesla a kolik hesel se má takto vygenerovat. Druhá sekce je zaměřena na detailnější nastavení hesla, a to, jestli heslo bude obsahovat nějaké znaky nebo naše vlastní znaky, zda bude dobře nebo hůře vyslovitelné atd. Prostředí programu je zobrazeno na obrázku, viz Obrázek 6.



Obrázek 6 Generátor hesel

Co se týká dalšího kroku v zabezpečení systému, měli by se uživatelé zaměřit na správu uživatelských účtů a na přidělení práv k jednotlivým účtům. Na počítači by měl být jeden administrátor a ostatní uživatelé by měli mít nastavený svůj účet jako standardní. Je to z toho důvodu, aby neměli přístup do celého systému, ale jen tam, kde nemůžou smazat důležité složky, ovladače, programy a jiné součásti systému.

Také byste jako uživatelé měli zkontrolovat, zda pracujete v zabezpečeném Internetovém prohlížeči. Je spousta stránek, které využívají prvky ActiveX a také technologie Javascriptu, což je jazyk, který umožňuje provádět akce přímo z uživatelova prohlížeče. Tyto komponenty dělají webové stránky více lákavé pro uživatele, ale opět skrývají nebezpečí. Prvky ActiveX obsahují „prográmky“, které mohou mít v sobě škodlivý kód, který může infikovat počítač virem či jiným škodlivým softwarem. Co se týká Javascriptu, zde je nebezpečí podobné, a to takové, že může poškodit data na webu, může se pomocí něj provést krádež přihlašovacích údajů či odcizení účtů, případně také provést bankovní operace.

K zabezpečení používá Internet Explorer bezpečnostní zóny, které nám slouží k rozdělení webových serverů do čtyř kategorií podle jejich důvěryhodnosti. Jejich názvy jsou Internet, Místní intranet, Důvěryhodné servery a Servery s omezeným přístupem. Aplikace Internet Explorer aplikuje na každou zónu nastavení zabezpečení podle druhu serverů, které do zóny patří.

3.4 Otestování operačních systémů

Ve své praktické části se zaměřím na testování operačních systémů Windows XP a Windows 7. Cílem je porovnat, jaký je rozdíl v zabezpečení těchto systémů ihned po jejich instalaci a formulovat doporučení, jak nejlépe tyto operační systémy zabezpečit proti útokům z Internetu. Níže uvádím kapitolu, ve které podrobně popisuji testovací software, který jsem si vybral. Každý provedený test bude slovně ohodnocen, proč jsou výsledky takové a co je zapotřebí udělat, aby byl počítač co nejlépe zabezpečen.

3.4.1 Testovací software

Jeden z mých úkolů v rámci bakalářské práce byl výběr testovacího softwaru, pomocí kterého budu operační systémy testovat. Vybral jsem si PC Security Test 2011, protože je

to bezplatný program pro Windows, který kontroluje zabezpečení počítače před viry, spywarem a hackery. Program simuluje viry, spyware a hacking útoky. Dohlíží na reakce vašeho ochranného softwaru. Simulují se různé druhy útoků na váš počítač a vyhodnocuje se jejich odezva. Po ukončení testu vám nabídne tipy na zvýšení bezpečnosti počítače.

3.4.2 Provedený test

V rámci programu PC Security Test se dá vybrat několik druhů testů, které testují PC proti útokům. Já jsem si vybral „*Všeobecný test kompletního zabezpečení počítače*“, protože si myslím, že je to jediný test ze všech nabízených, který testuje PC na všechny možné útoky. Tento test se skládá ze čtyř kroků. V prvním kroku je provedena série fiktivních útoků virů, spywaru a hackerů na váš počítač. Druhý krok se skládá z vyhodnocení reakce vašich bezpečnostních programů. Například antivir by měl zareagovat nějakým hlášením. Poté, co je reakce vašich bezpečnostních programů vyhodnocena, zobrazí vám PC Security Test hlášení s nabídkou tipů. Čtvrtým krokem je pak samozřejmě odstranění všech souborů, které program použil k simulaci útoků.

Simulace útoku probíhá tak, že jsou kontrolovány otevřené porty, provedeno skenování portů, přidána položka do seznamu automatického spuštění aplikací, je spuštěn testovací soubor EICAR, provedena simulovaná infekce souboru neznámým virem a pokus o spuštění viru v paměti. Kontrola ochrany přes spywarem opět spustí falešného útočníka, přidá špehovací komponentu do Internet Exploreru a pokusí se provést změnu domovské stránky.

EICAR je testovací soubor, který slouží pro uživatele a správce PC, aby si mohli otestovat správnou funkci svého antivirového softwaru a nemuseli používat viry skutečné, což je nebezpečné.

3.4.3 Testy operačního systému Windows XP a Windows 7

V této kapitole již přecházím k samotnému otestování operačních systémů pomocí testovacího softwaru, který je popsán výše. Nejprve otestuji operační systém Windows 7 a pak Windows XP. Pro lepší přehlednost jsem vytvořil tabulky, kde jsou všechny testy pojmenovány a seřazeny. Program také vypočítá ochranný index u každého bloku testu.

Výsledky testů operačních systémů Windows XP a 7 ihned po instalaci, viz Tabulka 3 a Tabulka 4.

VIRUS: Antivirový ochranný test		Antivirový ochranný index
Přidaná položka do seznamu automatických aplikací	×	0%
Simulace souboru infikovaného známým virem	×	
Simulace souboru infikovaného neznámým virem	×	
Simulace virů běžících v paměti	×	
SPYWARE: Anti-spyware ochranný test		Anti-spyware ochranný index
Simulace spywaru běžícího v paměti	×	0%
Přidání špionážního komponentu k aplikaci IE	×	
Simulace nevyžádané úvodní stránky v IE	×	
HACKING: Antihackerový ochranný test		Antihackerový ochranný index
Detekce otevřených portů	✓	50%
Simulace internetového útoku (skenování portů)	✓	
Simulace škodlivého programu otevírajícího port	×	

Tabulka 3 Výsledky testu pro Windows XP – čistý systém

VIRUS: Antivirový ochranný test		Antivirový ochranný index
Přidaná položka do seznamu automatických aplikací	×	0%
Simulace souboru infikovaného známým virem	×	
Simulace souboru infikovaného neznámým virem	×	
Simulace virů běžících v paměti	×	
SPYWARE: Anti-spyware ochranný test		Anti-spyware ochranný index
Simulace spywaru běžícího v paměti	×	25%
Přidání špionážního komponentu k aplikaci IE	✓	
Simulace nevyžádané úvodní stránky v IE	×	
HACKING: Antihackerový ochranný test		Antihackerový ochranný index
Detekce otevřených portů	✓	50%
Simulace internetového útoku (skenování portů)	✓	
Simulace škodlivého programu otevírajícího port	×	

Tabulka 4 Výsledky testu pro Windows 7 – čistý systém

V prvním bloku testovací software zjistil nulové zabezpečení počítače proti virům, protože počítač ihned po instalaci neměl nainstalovaný antivirový program, nemohl se tedy proti virům žádným způsobem bránit. Je zde dobře vidět, jak je počítač proti virům jednoduše napadnutelný, pokud uživatel nemá nainstalovaný antivirový program.

Druhý blok testu byl zaměřen na spyware. Na počítači byl vypnut firewall v centru zabezpečení a žádný jiný firewall nainstalovaný nebyl. V tomto případě již samotný systém zareagoval pouze v případě útoku spywarem z webového prohlížeče. Opět je zde vidět, že

systém firewall je nedílnou součástí operačního systému, protože bez něj je systém zvláště na útoky pomocí spyware velmi zranitelný.

Co se týká třetího bloku testů na detekci portů, dva ze tří testů byly hodnoceny kladně, protože při čisté instalaci operačního systému nejsou nainstalované služby, jako je třeba FTP server a další. Právě z těchto důvodů služby, které běží na těchto portech či programy, které porty otevírají, nebyly detekovány.

Výsledky testu pro Windows XP a 7 s nainstalovaným firewallem PC Tools Firewall Plus a antivirovým programem Microsoft Security Essentials jsou uvedeny v tabulkách, viz Tabulka 5 a Tabulka 6.

VIRUS: Antivirový ochranný test		Antivirový ochranný index
Přidaná položka do seznamu automatických aplikací	✓	100%
Simulace souboru infikovaného známým virem	✓	
Simulace souboru infikovaného neznámým virem	✓	
Simulace virů běžících v paměti	✓	
SPYWARE: Anti-spyware ochranný test		Anti-spyware ochranný index
Simulace spywaru běžícího v paměti	×	0%
Přidání špionážního komponentu k aplikaci IE	×	
Simulace nevyžádané úvodní stránky v IE	×	
HACKING: Antihackerový ochranný test		Antihackerový ochranný index
Detekce otevřených portů	✓	50%
Simulace internetového útoku (skenování portů)	✓	
Simulace škodlivého programu otevírajícího port	×	

Tabulka 5 Výsledky testu pro Windows XP s nainstalovaným firewallem a antivirem

VIRUS: Antivirový ochranný test		Antivirový ochranný index
Přidaná položka do seznamu automatických aplikací	×	75%
Simulace souboru infikovaného známým virem	✓	
Simulace souboru infikovaného neznámým virem	✓	
Simulace virů běžících v paměti	✓	
SPYWARE: Anti-spyware ochranný test		Anti-spyware ochranný index
Simulace spywaru běžícího v paměti	×	25%
Přidání špionážního komponentu k aplikaci IE	✓	
Simulace nevyžádané úvodní stránky v IE	×	
HACKING: Antihackerový ochranný test		Antihackerový ochranný index
Detekce otevřených portů	✓	100%
Simulace internetového útoku (skenování portů)	✓	
Simulace škodlivého programu otevírajícího port	✓	

Tabulka 6 Výsledky testu pro Windows 7 s nainstalovaným firewallem a antivirem

Na rozdíl od prvních dvou tabulek je v prvních blocích testu zřejmé, že antivirový program chrání počítač opravdu kvalitně proti útokům virů, protože testy na simulaci virů dopadli kladně. Nainstalování antivirového programu by mělo být na prvním místě z bezpečnostních kroků uživatele, zvláště v případě, pokud chce mít svůj počítač připojený do sítě Internetu. Je také velmi důležité provádět pravidelné aktualizace antivirového programu, protože antivirový program, který není aktualizovaný, náš systém nijak neochrání před škodlivým softwarem.

Bohužel druhý blok se mi nepodařilo úplně přesně otestovat z důvodu, že testy jsou prováděné na PC ve virtuálním stroji. Byla zapnuta brána firewall ve Windows a nainstalovaný firewall *PC Tools Firewall Plus* a i přesto, testy nedopadly dobře. Pokusil jsem se daný program povolit v bráně firewall, jak v počítači, tak ve virtuálním stroji, ale zřejmě tento test nelze provést přesně, proto jsou tyto výsledky nejasné.

Co se týká testů na skenování portů a útoky na porty z Internetu, v tomto případě je lépe zabezpečen operační systém Windows 7, u kterého vyšly všechny tři testy kladně.

3.5 Ochrana dat

Ochrana dat je další problematikou, kterou bychom měli řešit při zabezpečení systému. Již se několikrát stalo, že lidé přišli v několika sekundách o svá cenná data, nebo zjistili, že se jejich data dostala k osobám, ke kterým se dostat vůbec neměla. Nejprve bychom měli provést zašifrovaní dat a pak tedy samotné zálohování, protože zašifrování dat nám pomůže před neoprávněným jednáním cizího uživatele, ale nikoli před jejich smazáním či poškozením.

Tato kapitola je rozdělena pro přehlednost na dvě části, a to na šifrování a zálohování dat, což je popsáno níže:

3.5.1 Šifrování

Šifrování souborů a složek v operačním systému Windows představuje způsob jejich ochrany před nežádoucím přístupem a zneužitím. Velkou výhodou zašifrovaných dat je to, že pokud je někdo získá, nebude je schopen přečíst. Zašifrované soubory lze přečíst pouze v případě, že se k počítači přihlásíte na svůj účet, tedy jako administrátor. Nikdo další k nim nebude mít přístup.[23]

Operační systémy Windows obsahují standardně šifrování EFS pro soubory a složky a pak funkci BitLocker pro zašifrování pevného disku, která je dostupná od operačního systému Windows Vista a dále. Program BitLocker To Go je novinkou a je používán až v operačním systému Windows 7 v edicích Windows 7 Enterprise a Ultimate. Jednotlivé funkce pro šifrování jsou popsány níže:

Šifrování EFS (Encrypted File System)

Šifrovaný souborový systém EFS používá Windows 7 pro šifrování souborů a složek. V první řadě systém vytvoří náhodně vygenerovaný klíč (FEK), který slouží pro zašifrování dat. Data jsou zašifrována pomocí veřejného klíče. Pokud systém EFS používáte poprvé, Windows pro vás vytvoří certifikát, ve kterém je uložen veřejný a privátní klíč. Zašifrovaná data i vygenerovaný klíč FEK lze dešifrovat pomocí certifikátu a vašeho privátního klíče. Privátní klíč je dostupný až po přihlášení pomocí vašeho jména a hesla. Právo dešifrovat soubor či složku mají také určené osoby nebo osoby, které se podílí na obnově dat. Pokud by se ostatní uživatelé pokusili přistoupit k zašifrovaným datům, systém je pouze upozorní, že k této akci nemají oprávnění. Tedy, že se jedná o nepovelený přístup k souborům.

Pro pochopení principu práce se šifrováním je nutné porozumět jednotlivým krokům, které systém EFS během kódování a dekódování dat provádí.

Soukromý a veřejný klíč

Veřejný klíč je volně šířený všem osobám, se kterými se komunikuje. Privátní (soukromý) klíč má druhá strana. Ten by měl zůstat utajen. Spolupráce těchto klíčů je ve Windows základem šifrování. To, co zašifrujeme klíčem veřejným, můžeme dešifrovat pouze klíčem soukromým, a naopak. Jeden jediný klíč nelze použít k oběma akcím.

V prostředí EFS operačního systému Windows jsou klíče přidruženy k elektronickým certifikátům uživatele.

Šifrování složky

Jde v podstatě o přidělení objektu atribut E (Encrypt). Doporučuje se šifrovat celé složky, protože soubory vytvářené ve složce budou kódovány automaticky, což se týká také dočasných souborů. Lze samozřejmě šifrovat jednotlivé soubory. Předvedeme si „zašifrování celé složky“:

1. Složku zobrazte (v Průzkumníkovi nebo přes ikonu Tento počítač)
2. Klepněte pravým tlačítkem myši na ikonu Složka (nebo Soubor), kterou chcete zašifrovat, z místí nabídky vyberte příkaz Vlastnosti.
3. Na kartě Obecné stiskněte tlačítko Upřesnit. Najdete jej ve spodní části okna, které je věnováno atributům.
4. Aktivujte políčko Šifrovat obsah a zabezpečit tak data.
5. Pokud složka obsahuje další podsložky, objeví se okno Potvrdit změnu atributů.

Dešifrování složky

Chcete-li složku dešifrovat, postupujete podobně jako při jejím šifrování:

1. Klepněte pravým tlačítkem myši na zašifrovaný soubor nebo složku a z místní nabídky vyberte Vlastnosti.
2. Ve spodní části karty Obecné stiskněte tlačítko Upřesnit.
3. Zrušte zaškrtnutí políčka Šifrovat obsah a zabezpečit tak data.

Chování šifrovaných souborů

Jak se chovají zašifrované soubory, uvádím v tabulce níže, viz Tabulka 7.

Přihlášení pod jiným účtem.	Pokud budete otevírat zašifrovaný soubor, zobrazí se chybová zpráva "Přístup byl odepřen".
	Pokud se pokusíte dešifrovat zašifrovaný soubor zrušením zaškrtnutí atributu šifrování, zobrazí se zpráva"Přístup byl odepřen".
	Pokud máte oprávnění Změnit nebo Úplné řízení, můžete zašifrovaný soubor odstranit nebo přejmenovat.
Zkopírování nebo přesunutí nezašifrovaného souboru do zašifrované složky.	Kopie v zašifrované složce se zašifruje.
Přesunutí zašifrovaného souboru.	Pokud jej přesunete do jiné složky na stejném svazku, zůstane soubor zašifrován.
Přejmenování zašifrovaného souboru.	Soubor se přejmenuje a zůstane zašifrován.
Odstranění zašifrovaného souboru.	Pokud soubor odstraníte do koše, zůstane obnovený soubor zašifrován.
Vytvoření zálohy zašifrovaného souboru pomocí nástroje Zálohování.	Soubory zůstávají na záložním médiu zašifrovány.
Použití zašifrovaného souboru v jiném počítači.	V počítači musí být k dispozici soukromý klíč šifrovaného certifikátu.

Tabulka 7 Chování šifrovaných souborů

Certifikáty

Jedním z problémů EFS je možnost, že při výskytu chyby již nebude možné data dekódovat. To se může stát v případě, že:

- Po reinstalaci Windows již šifrované soubory nedekódujeme.
- V podobné situaci budeme při ztrátě certifikátu.
- Stejné nebezpečí hrozí při smazání účtu nebo poruše uživatelského profilu.

Ztracená data je možné obnovit, ale je potřebné pochopit činnost, odehrávající se během šifrování, a včas vytvořit agenta obnovení nebo zálohu certifikátu.

Konzola MMC Certifikáty

V certifikátech jsou uloženy klíče, jejichž prostřednictvím se šifrování provádí. Nejčastěji se pracujeme s certifikáty pro jednotlivé účty uživatelů, ale výjimkou není ani přiřazení certifikátu službě. Ke správě certifikátů používáme konzolu MMC, do níž přidáme snap-in modul Certifikáty. Konzole MMC (Microsoft Management Console) je nástroj pro práci s nástroji pro správu. Lze pomocí ní spravovat nástroje pro správu hardwaru, softwaru a síťových součástí systému Windows. Hlavní typ nástroje, který lze do konzoly přidat se nazývá modul snap-in.

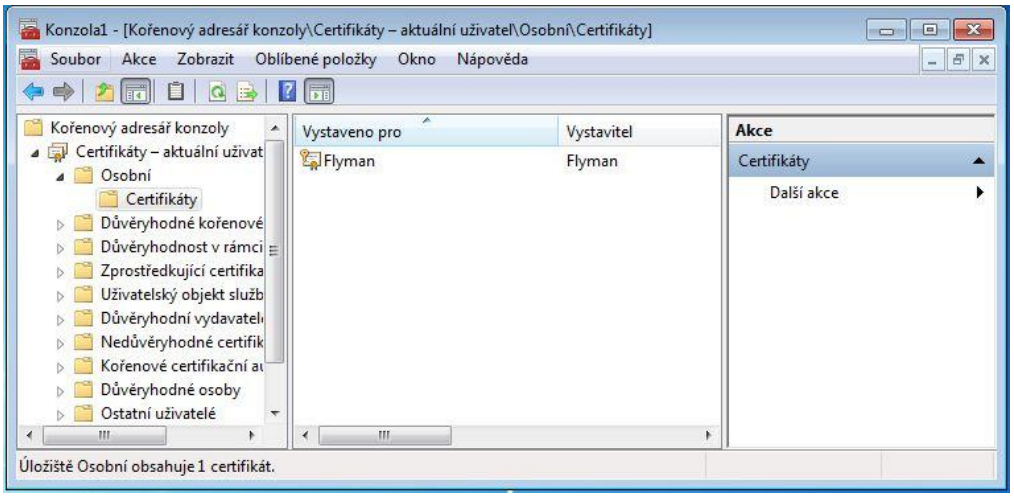
Postup:

1. Spusťte konzolu MMC.
2. V nabídce konzoly MMC zadejte příkaz Soubor - Přidat nebo odebrat modul snap-in.
3. Zobrazí se okno Přidat nebo odebrat samostatný modul snap-in. Zde je seznam modulů, použitelných v konzole MMC. Výše vidíte modul Certifikáty. Vyberte ho a stiskněte tlačítko Přidat.
4. Na obrazovce se objeví okno Modul snap-in Certifikáty. Nyní se musíte rozhodnout, jaké certifikáty budete spravovat.
5. Zaškrtnutím řádku Můj uživatelský účet budete spravovat certifikáty vlastního účtu, nainstalujte tedy modul Certifikáty- aktuální uživatel.

6. Účet služby je určen pro certifikáty služeb, v tomto případě instalujete modul s názvem Certifikáty - Služba (název_služby) v počítači název_počítače.
7. Účtem počítače můžete spravovat certifikáty, umístěné v určitém počítači, v okně konzoly uvidíte modul s názvem Certifikáty (název_počítače).
8. Rozhodnete-li se pro práci s Certifikáty Účtu počítače nebo Účtu služeb, budete muset ještě projít dalším oknem-Vybrat počítač. V něm zadáte, zda budete pracovat na místním počítači nebo na některém z počítačů v síti- na jiném počítači.
9. Po dokončení výběru modulu stiskněte v okně Přidat samostatný modul snap-in tlačítko Zavřít, v okně Přidat nebo Odebrat modul snap-in tlačítko OK a modul Certifikáty je konečně nainstalován.

Vytvoření certifikátu

Při prvním šifrování se automaticky vytvoří osobní certifikát uživatele. Jeho prostřednictvím je šifrování a dešifrování prováděno. Certifikát najdeme v konzole MMC Certifikáty, jeho jméno je shodné se jménem uživatelského účtu, k němuž jsme přihlášeni. Umístěn je ve složce Osobní/Certifikáty, viz Obrázek 7.



Obrázek 7 Umístění certifikátu v konzole MMC

Export Certifikátu

Certifikáty jsou vytvořeny vždy pro jednoho uživatele a aktuální instalaci operačního systému. Pokud se certifikáty naruší, jsou data nenávratně ztracena. Proto je velmi dobré certifikáty zálohovat- provést jejich export:

1. V Konzole MMC Certifikáty najděte svůj certifikát.
2. Klepněte na něj pravým tlačítkem myši, a v místní nabídce vyberte příkaz Všechny úkoly- Exportovat.
3. Spustíte Průvodce exportem Certifikátu.
4. Ve druhém okně průvodce rozhodujete, zda budete Exportovat privátní klíč. Jeho prostřednictvím jsou data dešifrována, proto zatrhněte možnost Ano, exportovat privátní klíč.
5. Třetí okno slouží pro definování formátu, v němž bude certifikát exportován. S naším certifikátem exportujete rovněž soukromý klíč, takže možnosti volby formátu jsou omezeny pouze na pfx. Důležitá volba Odstranit privátní klíč v případě úspěšného exportu. Pokud je zaškrtnete, bude certifikát z Windows odstraněn a vaše soubory nebude možné otevřít ani tehdy, když se přihlásíte z účtu, odkud byly zakódovány.
6. V následujícím okně vyplňte heslo, jímž je certifikát chráněn (budete jej muset vyplnit při zpětném importu).
7. V dalším okně zadejte umístění a jméno souboru s certifikátem (můžete si pomoci tlačítkem Procházet).
8. Poslední okno obsahuje souhrn nastavených zvolených parametrů.

Sdílení certifikátů

V jednom počítači může být nainstalováno více certifikátů, v principu pro každého uživatele jeden. Stačí, aby některý ze střídajících se uživatelů provedl šifrování dat, a certifikát je vytvořen. Přiřazení dalšího certifikátu provedeme následujícím způsobem:

1. V okně Upřesnit atributy (klepněte pravým tlačítkem myši na ikonu souboru, na kartě Obecné stiskněte tlačítko Upřesnit) stiskněte tlačítko Podrobnosti.
2. Otevřete okno Detaily šifrování, v jehož horní polovině vidíte uživatele, kteří mohou transparentně pracovat se zašifrovaným souborem.
3. Stiskněte tlačítko Přidat, zobrazíte okno Vybrat uživatele. V něm vidíte seznam uživatelských certifikátů, které můžete k souboru přiřadit.

4. Příslušný certifikát označíte a stiskněte tlačítko OK, tím ho přiřadíte k souboru (přesuňte ho do okna Detaily šifrování).
5. Z okna Detaily šifrování certifikát odstraníte tlačítkem Odebrat.

Agenti obnovení

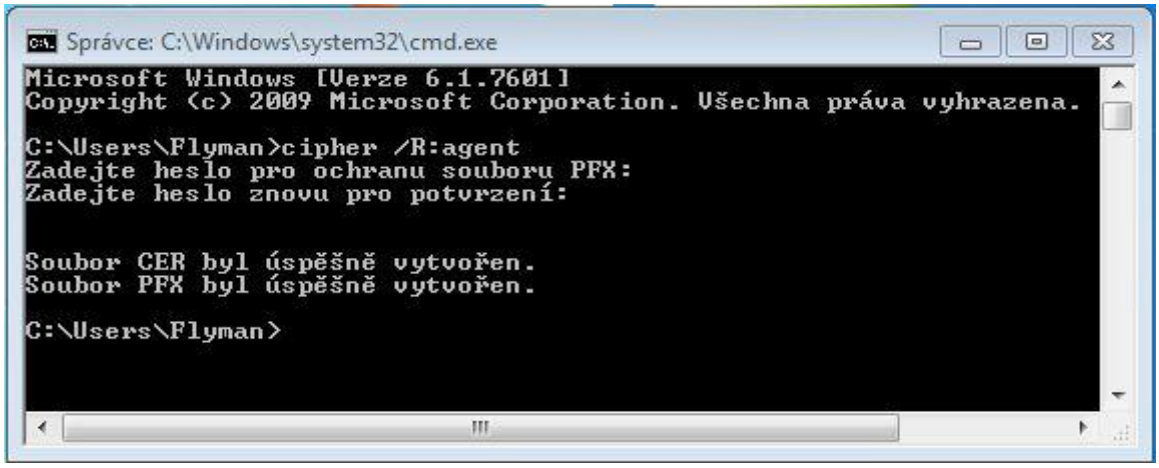
V podstatě jde o certifikát, který je přidružený k některému z uživatelských účtů. Můžeme pomocí něj data dekódovat. Na první pohled je agent pro data nebezpečný, protože přibude další certifikát pro dešifrování dat, ale pokud s ním pracujeme opatrně, je velmi prospěšný. Důvod pro použití agenta může být vyvolaný samostatným systémem - hardwarová porucha, resetování hesla, atd.

Generování certifikátu agenta obnovení

Certifikát agenta obnovení vygenerujeme následujícím způsobem:

1. Přihlaste se jako uživatel Administrátor.
2. Na příkazovém řádku zadejte příkaz cipher /R:název_souboru.
3. Po výzvě k zadání hesla zadejte heslo, které bude vytvořený soubor chránit.

Vygenerují se dva soubory – soubor PFX a CER se zadaným názvem, viz Obrázek 8.



Obrázek 8 Vytvoření agenta obnovení

Vytvoření agentů obnovení

Jakéhokoliv uživatele můžeme označit jako agent obnovení dat. Doporučuje se použít účet uživatele Administrátor.

Agenta obnovení dat vytvoříme následujícím způsobem:

1. Otevřete konzolu MMC. Dále pak přejděte do složky Certifikáty-aktuální uživatel/Osobní.
2. V nabídce Akce klepněte na příkaz Všechny úkoly a klepnutím na příkaz Importovat spusťte Průvodce importem certifikátu.
3. Zadejte cestu a název souboru s certifikátem šifrování (soubor PFX). Klepněte na tlačítko Další.
4. Zadejte heslo pro certifikát a poté zaškrtněte políčko Označit tento klíč jako exportovatelný. Pokračujte klepnutím na tlačítko Další.
5. Klepněte na políčko Automaticky vybrat úložiště certifikátů na základě typu certifikátu a poté klepněte na tlačítko Další. Klepněte na tlačítko Dokončit.
6. V konzole Místní nastavení zabezpečení (Secpol.msc) přejděte do složky Nastavení zabezpečení/Zásady veřejných klíčů/Šifrování systémů souborů.
7. V nabídce Akce klepněte na příkaz Přidat Agenta Obnovení dat. Poté klepněte na tlačítko Další.
8. Na stránce Vybrat agenty obnovení klepněte na tlačítko Procházet složky a poté přejděte do složky, která obsahuje CER, který jste dříve vytvořili. Vyberte soubor a klepněte na tlačítko Otevřít.
9. Klepněte na tlačítko Další a poté na tlačítko Dokončit.

Šifrování řádkovým příkazem (Cipher)

Šifrování souborů a složek se dá v operačním systému Windows provádět i přes příkazový řádek. K tomu nám slouží příkaz Cipher. Příkaz Cipher má řadu parametrů, mezi ty nejznámější patří /e, což je příkaz pro šifrování, dále pak /d, který složky a soubory dešifruje. Doporučuje se zašifrovat složku a také její obsah, tedy všechny soubory, které obsahuje. Základní využití řádkového příkazu je následující:

```
Cipher /e zkouška
```

Tímto příkazem jsme zašifrovali soubor či celou složku „zkouška“.

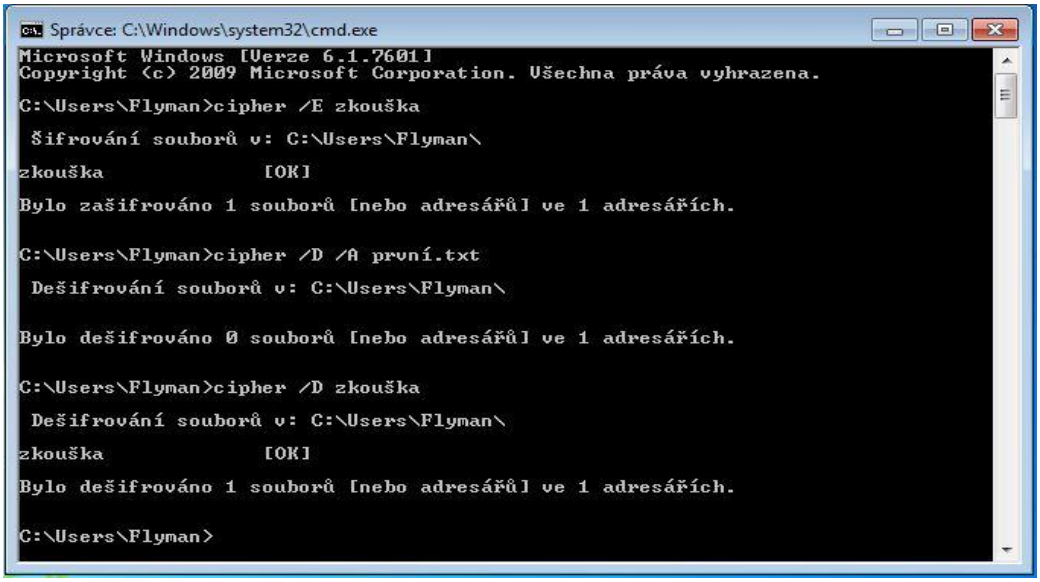
```
Cipher /d /a první.txt
```

A tento příkaz provede dešifrování souboru s názvem první.txt v aktuální složce.

```
Cipher /d zkouška
```

A nakonec takto dešifrujeme složku s názvem „zkouška“.

Pro znázornění příkazu přikládám ukázku šifrování v příkazovém řádku, viz Obrázek 9.



Obrázek 9 Příkaz Cipher

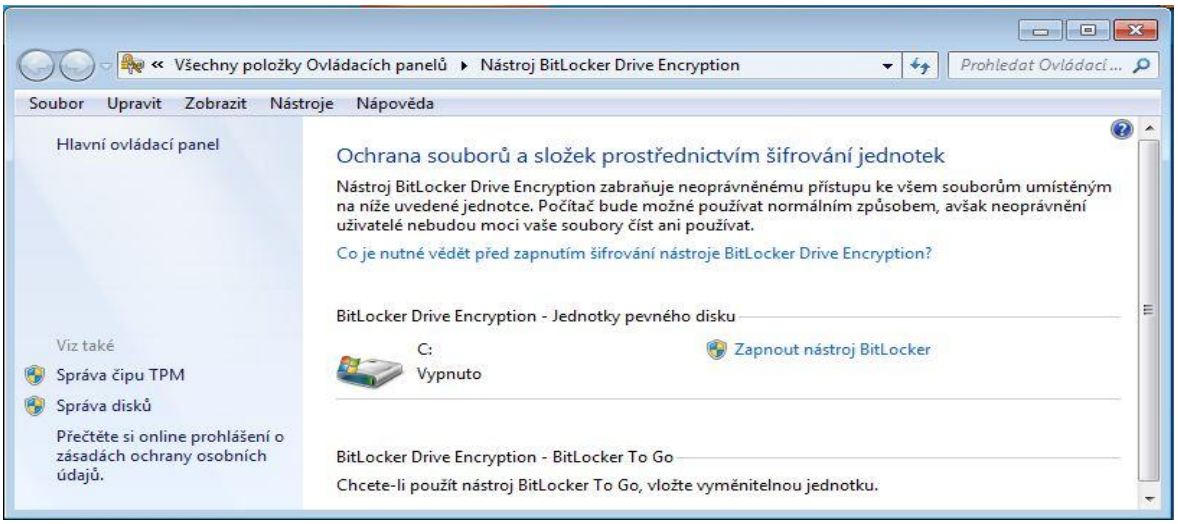
Parametry pro práci s příkazem Cipher jsou následující:

- `/B` – Zruší proces při zjištění chyby. Ve výchozím nastavení se pokračuje v běhu, i v případě zjištění chyb.
- `/C` – Zobrazí informace o zašifrovaném souboru.
- `/H` – Zobrazí soubory s atributy Skrytý nebo Systémový. Tyto soubory jsou výchozím nastavením vynechány.
- `/K` – Vytvoří nový certifikát a soukromý klíč pro použití se soubory EFS.
- `/R` – Vygeneruje klíč a certifikát agenta obnovení systému souborů EFS. Pak je zapíše do souboru typu PFX(obsahující certifikát a privátní klíč – bude chráněn heslem) a souboru CER (obsahující pouze certifikát).
- `/S` – Provede zadanou operaci i u všech podsložek.
- `/X` – Zálohuje zadanou operaci i u všech podsložek.
- `/REKEY` – Vytvoří nový certifikát a soukromý klíč pro použití se soubory EFS.
- `/ADDUSER` – Přidá důvěryhodné uživatele do zadaných zašifrovaných souborů.

Šifrování BitLocker

Hlavní rozdíl od šifrování EFS je, že BitLocker nám umožňuje zašifrovat celý oddíl, kdežto EFS pouze soubory. EFS nás ochrání před cizím uživatelem, BitLocker před neoprávněným systémem. Lze v podstatě říci, že pokud by nám někdo náš pevný disk z počítače neukradl, je pro nás tato funkce nepotřebná. Funkce BitLocker pracuje v reálném čase při práci s diskem a chrání systém před offline prolomením a zcizením dat z oddílů disku.

Bitlocker není při standardní instalaci v systému dostupný. Nejprve jej musíme aktivovat. Použijeme Ovládací panely – BitLocker, viz Obrázek 10.



Obrázek 10 Funkce BitLocker

BitLocker To Go

Jedná se o program, který funguje v počítačích se systémem Windows Vista a Windows XP a umožňuje otevírání a prohlížení obsahu přenosných jednotek, které jsou zašifrované pomocí nástroje BitLocker Drive Encryption ve Windows 7.

BitLocker To Go umožňuje uživatelům, kteří mají operační systém Windows 7 sdílení dat chráněných nástrojem BitLocker na přenosných jednotkách s kýmkoliv, kdo používá systém Windows 7, Windows Vista nebo Windows XP.

Aktivace BitLockerToGo

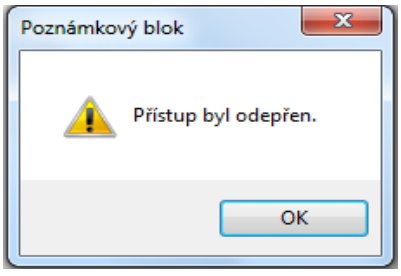
Je pravděpodobné, že základní Bitlocker pro interní disky ani nepoužijete a budete pracovat pouze s variantou BitLockerToGo:

1. Nejprve připojte flash disk nebo zařízení, které chcete šifrovat.
2. Pak přejděte do Start – Ovládací panely.
3. Zvolte ikonu šifrování BitLocker.
4. Zde uvidíte disky připravené pro zapnutí funkce BitLocker nebo BitLockerToGo.
5. Klepněte a povolte Zapnout BitLocker.
6. Spustí se průvodce pro zašifrování vašeho přenosného disku.

Neoprávněný přístup k souborům v zašifrované složce

V této kapitole si ukážeme, co se stane, pokud se pokusí někdo neoprávněně přistoupit k souborům v zašifrované složce. Abych tento test mohl předvést, vytvořil jsem si na svém počítači dalšího uživatele, který k této složce bude přistupovat. Nejprve jsem si vytvořil složku, do které jsem uložil soubor „první.txt“. Poté jsem ještě do složky překopíroval vlastní prezentaci, která je vytvořená v programu Microsoft Office PowerPoint 2007. Zašifrované soubory ve složce i celá složka jsou ve Windows 7 zeleně zabarveny, aby zašifrované soubory bylo možné rozlišit.

Nového uživatele jsem vytvořil v Ovládacích panelech v záložce Uživatelského účtu. V okně Spravovat změny uživatelského účtu jsem klikl na položku Spravovat jiný účet. V dalším okně jsem otevřel položku Vytvořit nový účet a vytvořil jsem vlastního uživatele, pomocí kterého jsem pak přistupoval k zašifrované složce. Dále přikládám screeny, aby bylo jasně vidět, co se stane po otevření složky neoprávněným uživatelem. Pokud neoprávněný uživatel přistoupí k zašifrovaným složkám, vyskočí okno, které ho upozorňuje, že jeho přístup byl odepřen, nebo že nemá právo pro zápis a čtení, případně že přistupuje k zašifrované složce. Přístup odepření souboru je na obrázku, viz Obrázek 11.



Obrázek 11 Přístup odepřen k textovému souboru

Program TrueCrypt

TrueCrypt je open-source pro šifrování diskových oddílů. Umožňuje šifrovat jak celé diskové oddíly (včetně systémového oddílu), tak i soubory a složky. Své služby nabízí uživatelům MS Windows, ale i těm, kteří používají Linux. Obě implementace jsou plně kompatibilní, takže není problém používat jeden šifrovaný flash disk v Linuxu i Windows.

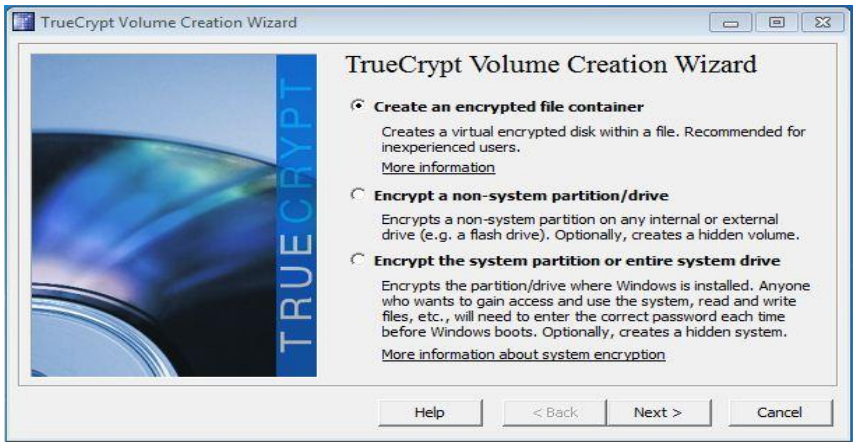
Program nabízí takzvané on-the-fly šifrování, což znamená, že veškeré procesy probíhají na pozadí a uživatel s daty pracuje, jako by byla na běžném disku. TrueCrypt je automaticky šifruje a dešifruje.

Velkou výhodou programu TrueCrypt je to, že vytvořený virtuální disk je v počítači vyobrazen na disku jakou obyčejný soubor, který si lze libovolně pojmenovat. Můžeme například tento soubor pojmenovat nějakým názvem s příponou .avi, čímž docílíme toho, že virtuální disk bude vypadat jako nějaký video soubor, což může útočníka přinejmenším zpomalit v případě, že by se naboural do uživatelova počítače.

Používá tři druhy algoritmů pro šifrování:

- AES-256.
- Serpent.
- Twofish.

V případě, že chce uživatel vytvořit zašifrovaný disk, musí v programu spustit průvodce pro vytvoření disku. Hlavní okno průvodce je vyobrazeno na obrázku, viz Obrázek 12.

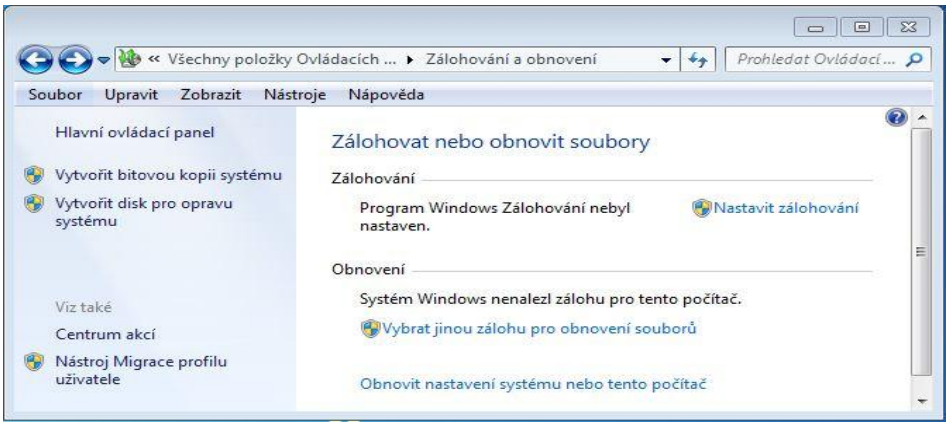


Obrázek 12 Průvodce pro vytvoření virtuálního disku

3.5.2 Zálohování dat

Zálohování dat představuje další krok k tomu, jak udržet váš systém ve stavu bezpečném. Ve většině případů jsou data potřeba chránit před nechtěným smazáním nebo chybou programu, před selháním diskového oddílu, před havárií celého systému, před havárií celého počítače, případně před lokální katastrofou, jako je požár nebo povodeň. Samotné zálohování dat představuje kopii dat uložených na jiném datovém nosiči, případně i místě. Záložní data se pak využívají v případě ztráty, poškození nebo jiné potřeby práce s daty uloženými v minulosti.[25]

Je několik způsobů, jak data zálohovat. Pro příklad uvedu operační systém Windows 7, ve kterém je přímo funkce pro zálohování dat. Tuto funkci můžeme najít v *Ovládacích panelech – Zálohování a obnovení*, pomocí ní můžeme zálohovat všechna data nebo určitá data na pevných discích i sdílených síťových složkách. Grafické znázornění funkce pro zálohování uvádím na obrázku, viz Obrázek 13.



Obrázek 13 Funkce pro zálohování a obnovu dat ve Windows 7

Další způsob zálohování dat je na externí a síťové disky, což představuje spolehlivý způsob ochrany dat před havárií celého počítače. Jinou možností je zálohovat data na CD nebo DVD, které nejsou ale příliš spolehlivé v otázce dlouhodobého uložení dat, protože spolehlivost zápisu je omezena dobou životnosti daného média. Může se stát, že CD či DVD, které dáte do mechaniky po letech, již nepůjde vůbec přečíst a data budou ztracena. Jsou na trhu sice výrobci, kteří uvádí životnost svých médií v desítkách let, ale jen v ideálních podmínkách, která jako uživatelé v domácnostech jen těžce vytvoříme.[26]

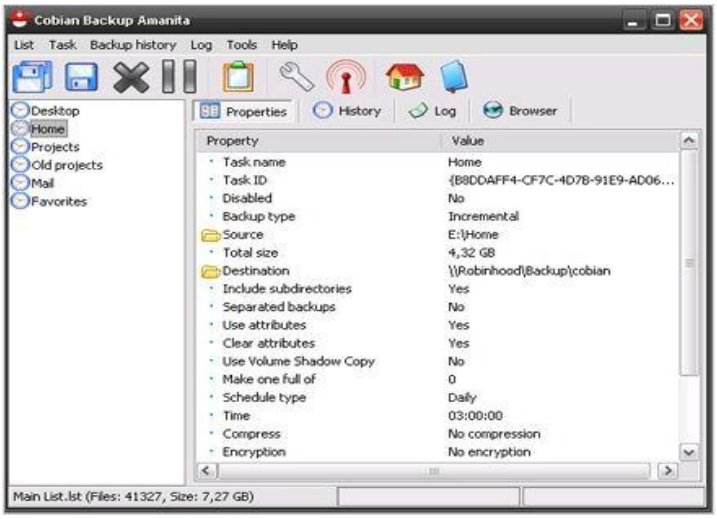
Běžný způsob zálohování dat ve firmách je zálohovat data na síťová úložiště, kdy jednotlivý uživatelé ukládají svá data do sdíleného úložiště na server nebo na síťové disky, o které se pak dále stará správce sítě, který data dále zálohuje a provádí údržbu.

Se stále rostoucí přenosovou rychlostí je také často využívaná možnost zálohy dat na FTP server. Velkou výhodou tohoto způsobu uložení dat je, že data mohou být uložena stovky kilometrů daleko od místa uložení zdrojových dat. V případě lokální havárie jsou data stále v bezpečí.

Mezi další možnosti zálohování dat patří také služby, které umožňují synchronizaci dat mezi více počítači. Funguje to tak, že si musí uživatel nainstalovat software a ten udržuje jeden adresář na disku, který je synchronizovaný proti serveru. Lze připojit více počítačů a všechny mají v jednom adresáři stejná data. Je výhodou, že pokud je počítač odpojený od služby, může pracovat uživatel lokálně na svém počítači, jakmile se připojí, tak se změny projeví i na serveru. K datům je tedy možné přistupovat z různých míst a počítačů, bez ohledu na to, na jakém počítači byly tyto změny provedeny. Mezi takové aplikace dnes patří například Dropbox, SkyDrive, případně Google Drive.

Z pohledu bezpečnosti představují tyto služby ale jisté riziko ztráty, případně zcizení dat, protože pokud hacker danou službu naboural, může vaše data ukrást. Uživatel si musí uvědomit, že pokud ukládá svá data do aplikace dané služby, musí také počítat s tím, že k nim může přistupovat třetí strana, tedy provozoval dané služby. Je tu samozřejmě možnost se proti těmto bezpečnostním rizikům bránit, a to například tím, že svá data, která ukládáte do aplikace, zašifrujete. Výše popisuji program TrueCrypt, který se pro tento účel hodí, je možné pomocí něj vytvořit virtuální disk, svá data do něj uložit a až teprve poté je nahrát do aplikací, které provádí synchronizaci dat. Uživatel, který by chtěl k datům přistoupit, tuto šanci nebude mít, protože data na virtuálním disku jsou zašifrovaná a lze do nich vstoupit jen pod heslem, které zná jen uživatel, nikoli třetí strana.

Existuje také celá řada programů, které se zálohováním dat zabývají. Jedním z takovýchto programů je *Cobian Backup*, což je program, který zálohuje soubory a adresáře jak na stejném, tak i na vzdáleném počítači. Program má spoustu funkcí a je také možné data zálohovat na FTP server. Grafické znázornění programu uvádím na obrázku, viz Obrázek 14.



Obrázek 14 Program pro zálohování dat – Cobian Backup

ZÁVĚR

Ve své práci jsem se pokusil vystihnout a popsat problematiku z oblasti bezpečnosti počítačových sítí. Věnoval jsem se nejen samotnému popisu jednotlivých metod a nástrojů hackerů, ale také jsem se snažil provést testy operačních systémů na zabezpečení, abych mohl lépe formulovat svá doporučení pro co nejlepší zabezpečení systému.

V teoretické části jsem se zaměřil na popis škodlivého softwaru, představil jsem čtenáři jeho základní formy, dále pak jsem uvedl nepřeberné množství útoků hackerů na počítačové sítě či na počítače uživatelů. Byl bych rád, kdyby tato práce sloužila i pro běžné uživatele, kteří by se po jejím přečtení mohli dozvědět více informací týkajících se hrozeb z prostředí Internetu. V praktické části jsem se snažil dát poznatky do souvislosti s navržením konkrétního řešení pro uživatele, tedy jaké bezpečnostní kroky by měl dodržet, případně provést, aby byl chráněn proti hackerům.

Při shánění materiálů pro tuto práci jsem byl sám velmi překvapen, kolik je možností a různých aplikací či jiných technik pro nabourání systému. Mezi důležitou část své práce řadím formulování doporučení pro co nejlépe zabezpečený systém. Uživatel tak může lehce zjistit nedostatky ve svém systému, případně se dozvědět něco nového o zabezpečení operačních systémů.

I ten nejlépe zabezpečený systém je potřeba ovládat uživatelem, který zná možná rizika a nástroje, jak se proti nebezpečnému softwaru bránit, případně jak ho rozpoznat, což je taky někdy velmi důležité. Nedílnou součástí dobře zabezpečeného systému je použít kombinaci šifrování a zálohování dat, což představuje jeden z možných kroků, jak svá data zachovat ve stavu bezpečném. Velkým přínosem do práce je představení programu TrueCrypt, o kterém většina lidí nemá ani ponětí. Pomocí něj můžeme svá data zašifrovat a v kombinaci se správným zálohováním můžeme tak vytvořit kvalitní systém ochrany dat jak pro běžného uživatele, tak i pro firemní účely.

Tato práce zahrnuje základní znalosti, jež by měl běžný uživatel o hackerských metodách znát, aby se mohl účinně bránit. Věřím, že pro čtenáře bude práce užitečná a dokáže se z ní poučit a zamyslet se nad problematikou týkající se nástrah hrozících z Internetu.

ZÁVĚR V ANGLIČTINĚ

In my thesis I try to represent and describe the issue of computer networks security. I devoted myself not only to description of different methods and implements of hackers, but I have also tried to test the operating systems for securiting, to better formulation of my recommendations for the best system security.

In the theorethical part, I focused on the description of the malware, I have introduced readers its basic forms, and then I have presented inexhaustible amount of hacker attacks on computer network ort he computers of users. I would be glad,if this thesis served also for ordinary users, who would after reading it could learn more about infromation of the threats from the Internet. In practical part I have tried to put pieces of knowledge into connection with concept of specific solution for the user, so which safety steps he should follow, or if necessary to carry out to be protected against hackers.

When searching for materials for this thesis, I was very surprised how many different options and applications, or other techniques for the hacking to system exist. Among the important part of my thesis I consider formulating of recommendations for the best secured system. The user can appreciate, where his system has shortages, or he can learn something new about the operation systems security.

Even the best secured system is needed to control by a user, who knows the risks and methods, how to defend against dangerous software or how to recognise it, which is also sometimes very important. In this thesis I have outlined possibilities of encryption and data backup, I have tried to describe all the wals to keep your data safe. A great contribution to the thesis is the introduction of the TrueCrypt program, which most people do not even know it exist. With it we can encrypt our data and in combination with the right backing up we can create a quality system of data protection for both normal users and also for corporate purposes.

This thesis includes basic knowledge of chat should a regular user know about hacking methods, in order to effective defending themselves. I hope that this thesis will be beneficial for the reader and that he will learn from it and reflex on the issue of threats from the Internet.

SEZNAM POUŽITÉ LITERATURY

[1] SCAMBRAY, Joel, Stuart MCCLURE a George KURTZ. *Hacking bez tajemství, 2. aktualizované vydání*. Praha: Computer Press, 2002. ISBN 80-7226-644-6.

[2] Lupa.cz. HALLER, Martin. *Denial of Service (DoS) útoky: záplavové typy* [online]. 12.9.2006 [cit. 2012-03-08]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/

[3] Lupa.cz. HALLER, Martin. *Denial of Service (DoS) útoky: záplavové typy* [online]. 12.9.2006 [cit. 2012-03-08]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/

[4] Lupa.cz. HALLER, Martin. *Denial of Service útoky: reflektivní a zesilující typy* [online]. 17.10.2006 [cit. 2012-03-09]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/

[5] LONG, Johnny. *Google Hacking*. Brno: Zoner Press, 2005. ISBN 80-86815-31-5

[6] Zdroják.cz. HASSMAN. *Clickjacking: nebezpečí číhající na uživatele webových aplikací* [online]. 8.10.2008 [cit. 2012-03-28]. Dostupné z: http://zdrojak.root.cz/zpravicky/clickjacking-nebezpeci-pro-uzivatele/

[7] HOAX.cz. DŽUBÁK, Josef. *PHISHING* [online]. 2000 [cit. 2012-03-08]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[8] Lupa.cz. *Rybaření střídá pharming* [online]. 1998 [cit. 2012-03-08]. Dostupné z: http://www.lupa.cz/clanky/rhybareni-strida-pharming/

[9] HALLER, Martin. Lupa.cz. *Odposloucháváme data na přepínaném Ethernetu (5.)*: *DNS Spoofing* [online]. 11.6.2006 [cit. 2012-03-08]. Dostupné z: http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-5

[10] Root.cz. MALÝ, Martin. *TabNabbing krade přihlašovací údaje nepozorným*: *Jak vypadá TabNabbing* [online]. 31.5.2010 [cit. 2012-03-08]. Dostupné z: http://www.root.cz/clanky/tabnabbing-krade-prihlasovaci-udaje-nepozornym/

[11] ROOT.CZ. KRČMÁŘ, Petr. *Jak se asi „hackovala" hesla z e-mailu Seznamu* [online]. 14.4.2006 [cit. 2012-03-28]. Dostupné z: http://www.root.cz/clanky/jak-se-asi-hackovala-hesla-z-e-mailu-seznamu/

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

[13] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP*: *Bezpečnost*. Praha: Computer Press, 2001. ISBN 80-7226-513-X

[14] PETERKA, Jiří. EArchiv.cz. *Elektronická pošta á la TCP/IP - část I.* [online]. 2011 [cit. 2012-04-20]. Dostupné z: http://www.earchiv.cz/a98/a804c200.php3

[15] RUDA, Miroslav. ÚVT MU. *Autentizace v protokolu elektronické pošty SMTP* [online]. 14.11.2011 [cit. 2012-04-20]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/175.html

[16] Poštovní protokoly. *Home* [online]. 2012 [cit. 2012-04-18]. Dostupné z: http://home.zcu.cz/~bosekma/

[17] GREER, Tyson. *Intranety princip a praxe*. Brno: Computer Press, 1999. ISBN 80-7226-135-5

[18] Zákon o elektronickém podpisu. *Business center* [online]. 2012 [cit. 2012-05-02]. Dostupné z: http://business.center.cz/business/pravo/zakony/epodpis/cast1.aspx

[19] První certifikační autorita, a.s. *Záloha certifikátu včetně soukromého klíče* [online]. 2012 [cit. 2012-05-03]. Dostupné z: http://www.ica.cz/Zaloha-certifikatu.aspx

[20] Certifikační autorita PostSignum. *Ceny za vydávané certifikáty* [online]. 2012 [cit. 2012-05-03]. Dostupné z: http://www.postsignum.cz/certifikaty.html

[21] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*: *praktické rady a návody*. Praha: Grada Publishing, 2003. ISBN 80-247-0663-6.

[22] GREER, Tyson. *Intranety princip a praxe*. Brno: Computer Press, 1999. ISBN 80-7226-135-5

[23] BOTT, Ed a Carl SIECHERT. *Mistrovství v Microsoft Windows XP*. Praha: Computer Press, 2002. ISBN 80-7226-693-4

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

[25] Zálohování.net. *Před jakými hrozbami je potřeba data chránit* [online]. 4.3.2010 [cit. 2012-04-23]. Dostupné z: http://www.zalohovani.net/inpage/ochrana-dat-pred-hrozbami/

[26] Acronis. *Zálohování dat - jak vytvořit datovou zálohu* [online]. 2012 [cit. 2012-04-23]. Dostupné z: http://www.acronis.cz/kb/zalohovani-dat/

[27] CAFOUREK, Bohdan. *Windows 7*: *kompletní příručka*. Praha: Grada Publishing, 2010. ISBN 978-80-247-3209-1.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DNS Domain Name System

Systém pro překlad doménových jmen na IP adresy

ACL Access Control List

Pravidla pro řízení přístupu

TCP/IP Transmission Control Protocol / Internet Protocol

Sada protokolů pro komunikaci v počítačové síti

VNC Virtual Network Computing

Program, který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní

SSH Secure Shell

Zabezpečený komunikační protokol

SCP Secure Copy Protocol

Protokol pro bezpečný přenos souborů mezi dvěma počítači

FTP File Transfer Protocol

Komunikační protokol

FTPS File Transfer Protocol Secure

Zabezpečený protokol FTP

HTTP Hypertext Transfer Protocol

Protokol určený pro přenos hypertextových obrázků a dokumentů

HTTPS Hypertext Transfer Protocol Secure

Šifrovaná varianta Internetového protokolu HTTP

ICMP Internet Control Message Protocol

Protokol, který umožňuje sdílet informace o chybách a stavu sítě

HTML HyperText Markup Language

	Jazyk HTML pro tvorbu webových stránek
IMAP	Internet Message Access Protocol
	Internetový protokol určený pro vzdálený přístup k e-mailové schránce
POP	Post Office Protocol
	Internetový protokol určený pro stahování e-mailových zpráv
SMTP	Simple Mail Transfer Protocol
	Internetový protokol určený pro přenos zpráv elektronické pošty
TLS	Transport Layer Security
	Kryptografický protokol používaný pro zabezpečení Internetové komunikace
SSL	Secure Sockets Layer
	Protokol, který se používá pro šifrované spojení u protokolu HTTP
MTA	Message Transfer Agent
	Označení pro poštovní server
DoS	Denial of Service
	Útok odmítnutí služby
DMZ	Demilitarizovaná zóna
	Vyhrazená část sítě, která je zvláště zabezpečena
SASL	Simple Authentication and Security Layer
	Protokol, který umožňuje autentizaci pomocí hesla

Seznam obrázků

SEZNAM TABULEK