ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

Windows XP – bezpečnost

Bakalářská práce

PRAHA 2008 ©

Vedoucí práce: Ing. Václav Lohr

Autor práce: Jiří Dziedzic

PROHLÁŠENÍ

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité prameny a literaturu, které jsem při vypracování používal či z nich čerpal, uvádím v přiloženém seznamu literatury.

.....

Jiří Dziedzic

V Praze dne 6. 5. 2008

PODĚKOVÁNÍ

Děkuji Ing. Václavu Lohrovi za odborné vedení a pomoc při vypracování této bakalářské práce.

Windows XP - Bezpečnost

Souhrn

Tato bakalářská práce se zabývá zabezpečením počítačových operačních systémů, s důrazem na operační systém Microsoft Windows XP. V první části jsou rozebrány obecné zásady a principy zabezpečení operačních systémů, ve druhé pak jednotlivé komponenty správy zabezpečení Microsoft Windows XP. Třetí a poslední část se zabývá operačním systémem Microsoft Windows Vista, konkrétně změnami v systému zabezpečení proti Windows XP.

Klíčová slova: operační systém, zabezpečení, správa zabezpečení, Microsoft Windows XP, šifrování dat, uživatelský účet, uživatelská skupina

Windows XP - Security

Summary

This bachelor work deals with security of computer operating systems, emphatically with operating system Microsoft Windows XP. The first part of work analyses the general policies and principles of operating systems security, the second analyses single components of Microsoft Windows XP security control. The third and the last part considers the operating system Microsoft Windows Vista, concretely differences in security system compared to Windows XP.

Key words: operating system, security, security control, Microsoft Windows XP, data encryption, user account, user group

Obsah

1 Úvod

Počítače jsou jedním z největších přínosů v dějinách techniky. První počítače, jako jsou známé dnes, tedy všestranně využitelné, se objevily v roce 1990, kdy na trh přišel operační systém Windows 3.0 firmy Microsoft (MS), který je považován za první reálně použitelný operační systém s grafickým rozhraním. Brzy se stal velmi oblíbeným a počet počítačů v domácnostech a ve firmách (nejprve pouze v USA) se rázem zněkolikanásobil. V roce 1992 přišla na trh další důležitá verze systému Windows, a to verze 3.11. Její důležitost spočívala v implementaci síťového rozhraní do operačního systému a následnému rychlému rozšíření sítě Internet, ke kterému bylo v tomto roce připojeno již více než jeden milion uživatelů (v roce 1984 to byl pouhý jeden tisíc). Spolu s rozmachem používání počítačů pro (nejen) pracovní účely vyvstalo riziko zneužití dat v nich uložených, a proto se objevila snaha toto nebezpečí eliminovat. Tím byl položen základ fenoménu zvaného počítačová bezpečnost. Dnes je zabezpečení základním kamenem každého operačního systému.

2 Cíl a metodika práce

Tato práce se bude zabývat problematikou zabezpečení osobních počítačů, respektive bezpečností operačního systému, který je základním programovým vybavením každého počítače a umožňuje komunikaci mezi uživatelem a hardwarem a řídí činnost jednotlivých částí počítače.

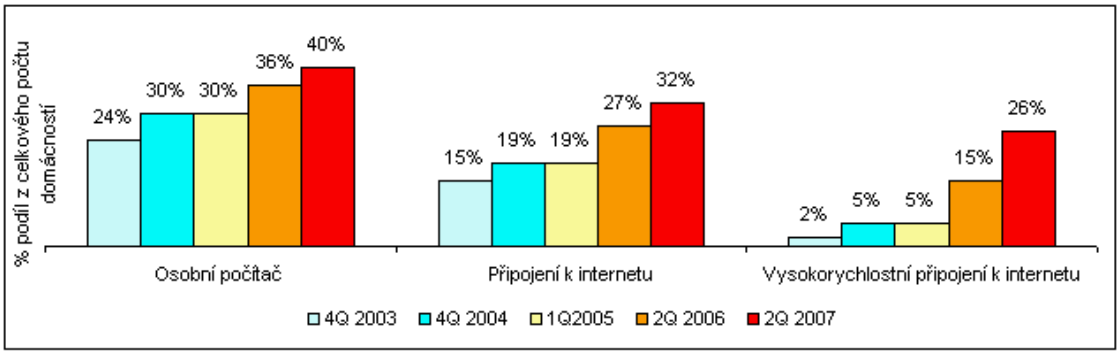
Teoretická část práce si klade za cíl objasnit uživateli počítače rizika práce s ním a možnosti, jak tato rizika minimalizovat, případně zcela eliminovat.

V praktické části se práce bude zabývat jednotlivými komponenty správy zabezpečení operačního systému MS Windows XP. Práce se bude snažit co možná nejlépe vysvětlit jejich význam, výhody či případné nevýhody a probrat jejich nastavení pro zajištění maximální bezpečnosti. Pro tuto část práce bude použita verze operačního systému MS Windows XP Professional, které oproti verzi Home obsahuje rozšířenou síťovou podporu a mnoho nástrojů pro ochranu dat a přístupu k nim, je tedy proto pro dané zkoumání vhodnější.

Třetí část zmiňuje změny v systému zabezpečení nově vydaného operačního systému Windows Vista, který má být podle slov představitelů firmy Microsoft nástupcem systému Windows XP.

3 Teorie bezpečnosti operačních systémů

Počítače se v současné době staly nedílnou lidského života. Přestože ve využívání informačních technologií Česká republika stále zaostává za státy západní Evropy, počet osob tyto technologie využívajících rychle stoupá. Podle údajů Českého statistického úřadu (ČSÚ) počet počítačů v domácnostech od roku 2003 strmě vzrostl a v současné době vlastní počítač již 40 % českých domácností (celkem 1,68 mil. domácností). Podobně je tomu u využívání nejrozšířenější informační technologie dneška, Internetu (Podle údajů Českého statistického úřadu používá Internet alespoň dvakrát týdně více než 45 % všech osob starších 18 let). Připojení k síti Internet dle ČSÚ vlastní v současné době 32 % všech českých domácností (1,36 mil.), 80 % z nich vlastní připojení vysokorychlostní (1,08 mil.). Tyto údaje zachycuje následující graf.



Obrázek .č. 1: Počet počítačů a internetových připojení v domácnostech v ČR [24]

Počet počítačů a počet připojení k síti Internet v domácnostech se během posledních čtyř let takřka zdvojnásobil, počet vysokorychlostních připojení v domácnostech je pak oproti roku 2003 více než desetinásobný.

S využíváním počítačů jako nástroje pro práci a komunikaci ovšem roste také riziko zneužití dat v nich uložených, případně napadení škodlivým softwarem, který má za úkol ohrozit stabilitu počítače jako takového.

3.1 Operační systém a struktura jeho zabezpečení

Operační systém (OS) je základní programové vybavení počítače, které řídí systémové prostředky a poskytuje uživateli prostředí, ve kterém provádí svou činnost. OS spravuje systémové procesy a řídí jejich činnost a komunikaci s hardwarem. Provádí také základní úkony, jako je kontrola a alokace operační paměti, vstupních a výstupních zařízení, síťových prostředků a správa souborů. OS musí obsahovat každý osobní počítač, bez něj by nebyla práce s ním možná. V současné době ovšem OS nalezneme na téměř každém elektronickém zařízení, jako jsou mobilní telefony, hudební přehrávače, herní konzole, digitální fotoaparáty a další.

Každý operační systém obsahuje určitou úroveň zabezpečení. Existují dvě základní úrovně zabezpečení, vnitřní a vnější.

Vnitřní bezpečnost si můžeme představit jako ochranu systémových prostředků před samotnými programy, které na počítači běží. Většina operačních systémů umožňuje programům (respektive procesům, které program tvoří) běh přímo na procesoru, základním problémem vnitřní bezpečnosti tedy je, jak zabránit programům v přístupu k systémovým prostředkům na stejné úrovni, na které pracuje operační systém (který je ve své podstatě také pouze program). Toto je u většiny OS (včetně MS Windows) realizováno přidělováním práv jednotlivým procesům. Procesy s nižší úrovní práv mají automaticky zablokován přístup k některým systémovým prostředkům, jako je zapisování a čtení z pevných disků. Místo toho se proces musí dotázat jádra operačního systému, zda mu přístup povolí. Tento způsob umožňuje operačnímu systému ověřit identitu procesu a případně přístup zakázat. [7]Vnější bezpečnost naproti tomu slouží ke kontrole vzdáleného přístupu k systémovým prostředkům pomocí služeb, které systém nabízí. [7]

3.2 Ochrana dat

V každém osobním počítači jsou uložena data, nejčastěji obsažená v souborech na pevném disku. Určitá data jsou také přenášena při síťové komunikaci, kterou operační systém realizuje. Některá z těchto dat mohou být citlivá. Existují tři základní důvody ochrany. Data mohou být vyzrazena a zneužita, změněna, nebo rovnou zničena. Kterákoliv z těchto možností by mohla vést ke značným finančním ztrátám, zejména v případě firemních dat. Proto je třeba tato data určitým způsobem chránit.

3.2.1 Základní typy dat

Data v systému je možné rozdělit na 4 základní skupiny. Jsou to [2]:

- Data uživatelů

Do této skupiny patří data, která uživatelé vytvářejí při své práci, například dokumenty. Jejich ochrana je důležitá, jejich ztráta však neohrozí činnost systému.

- Auditní záznamy

Do auditního záznamu jsou zaznamenány všechny události, které se v systému odehrály. Kdyby byl auditní záznam zničen, nebylo by možné dohledat původce narušení systému.

- Spustitelný kód

Jsou to veškeré programy v systému. Vhodnou změnou programu by útočník mohl docílit nestabilní chování systému, případně by program mohl dovést do stavu, kdy by sám o sobě páchal škodu.

- Autentizační informace

Autentizační informace jsou data obsahující informace o uživatelích systému, jejich přístupových právech a o způsobu jejich autentizace při přístupu. Kompromitací těchto dat by útočník získal možnost přístupu do systému pod identitou kteréhokoliv uživatele, nebo by jejich zničením mohl zabránit všem uživatelům v přístupu. Tato data jsou nejcitlivější a platí pro ně nejvyšší stupeň zabezpečení.

3.2.2 Druhy ochrany dat

Ochranu dat je možné rozdělit do několika kategorií podle toho, jaké zabezpečení je v konkrétním případě potřebné. Základními kategoriemi jsou :

3.2.2.1 Ochrana fyzického přístupu k datům

Nejdůležitějším prvkem ochrany každého osobního počítače je fyzické zabezpečení přístupu k němu. Obecně platí, že i velmi dobře zabezpečený operační systém může být snadným cílem útoku, pokud není dobře vyřešena fyzická ochrana počítače. Nejsnadnějším terčem útoků fyzického typu jsou bezesporu počítače přenosné (u stolních počítačů je toto riziko podstatně nižší), je proto vhodné je odpovídajícím způsobem chránit. Základní ochranou je mít počítač stále u sebe a na očích, což může být však v řadě případů obtížné. Výrobci, kteří se na ochranu přenosných počítačů zaměřují, proto nabízejí stále kvalitnější prvky ochrany, které je vhodné k přenosnému počítači pořídit. Za zmínku zde stojí alarm, který nabízí např. firma TrackIT. Sestává ze dvou částí, z nichž jedna bývá vložena do brašny s počítačem, druhou pak nosí uživatel u sebe. V případě, že se obě části od sebe vzdálí bez předchozí deaktivace, která se provádí klíčem, začne přístroj vydávat velmi hlasitý zvuk podobný alarmu používanému v automobilech.

Obrázek č. 2: Alarm TrackIT [23]

Ochrana stolních počítačů bývá vyřešena jednoduchým připevněním skříně ke konstrukci stolu, na kterém je uložen, a uzamčením skříně, aby nemohlo dojít k odcizení pevného disku.

3.2.2.2 Ochrana logického přístupu k datům

Pokud by došlo k prolomení ochrany fyzického přístupu k datům (například z důvodu odcizení přenosného počítače), je třeba eliminovat nebo alespoň minimalizovat možnosti jejich zneužití. První formou ochrany operačního systému je ochrana před neoprávněným přístupem k němu.

Téměř každý operační systém řídí přístup pomocí uživatelských účtů. Při pokusu o přístup musí uživatel systému zadat, kým je, tedy se identifikovat. To je nejčastěji realizováno zadáním uživatelského jména. Ve druhém kroku autentizace musí uživatel prokázat, že je skutečně tím, za koho se vydává. Existují tři základní možnosti autentizace [2]:

- Prvním způsobem je zadání uživatelského hesla či čísla PIN. Tento způsob se nazývá *důkaz znalostí*, protože uživatel prokazuje sou identitu tím, že zná své tajné heslo. Tento způsob je v dnešní době nejrozšířenější, není však příliš spolehlivý, protože prolomení hesla je vždy možné, nezávisle na jeho kvalitě.
- Druhou možností autentizace je tzv. *důkaz vlastnictvím*, což spočívá v poskytnutí nějakého předmětu (např. přenosný disk s USB rozhraním), na kterém může být tajný klíč, kterým systém uživatele jednoznačně identifikuje. Tento způsob je možné obejít odcizením identifikačního předmětu.
- Třetí možností spočívá v poskytnutí nějaké biologické informace, kterou operační systém sám změří, tato metoda bývá proto označována jako *důkaz vlastností*. Příkladem může být v dnešní době již poměrně rozšířená autentizace pomocí přečtení otisku prstu, některé systémy již umí využívat i obraz oční sítnice. Tato metoda je obecně nejspolehlivější, napodobit biologické údaje jiného jedince je prakticky nemožné. Její nevýhodou je ovšem finanční nákladnost, čtečky otisků prstů či obrazu oční sítnice jsou v dnešní době velmi drahé.

3.2.2.3 Ochrana uložených dat a dat přenášených počítačovou sítí

Data uložená na pevných discích počítače, případně na síťových discích je třeba zabezpečit nejen fyzicky a logicky, ale je vhodné je zabezpečit i další cestou, která zamezí přístupu k nim i jiným způsobem než přes osobní počítač, ke kterému disk patří. Pevný disk je totiž velmi snadno odcizitelný i v případě uzamčené skříně. Jeho velikost pak umožňuje odnést ho například v kapse. Data na pevných discích bývají proto šifrována. Šifrování jako takové je velmi komplikovaná a široká oblast, proto je popsána v samostatné kapitole.

3.2.2.4 Ochrana dat před zničením

V důsledku nevhodného jednání (úmyslného i neúmyslného) či vlivem přírodní katastrofy může dojít k fyzickému zničení dat. Proto je vhodné veškerá důležitá data pravidelně zálohovat. Toto je možné realizovat pomocí ukládání na přenosná média CD, DVD či nejnovější běžně dostupné disky Blu-ray, případně na externí pevný či flash disk. U pevných disků či flash pamětí však hrozí riziko "dosloužení". Z nefunkčního pevného disku je sice možné v některých případech data za pomoci specializované firmy později obnovit, je to však značně finančně nákladné. Proto je vhodné používat spíše jednorázová média, data zálohovat na několika odděleně uložených kopiích (tím zabráníme riziku zničení z hlediska přírodních vlivů). Po čase pak zálohovaná média kopírovat na nová, všechna média totiž s postupem času stárnou a po několika letech mohou být zcela nečitelná. Disky se zálohovanými daty je poté vhodné uložit na bezpečné místo, odděleně od samotných počítačů, aby nedošlo i ke zničení záložních kopií, např. při požáru.

Neméně důležité je zabránit ztrátě dat z důvodu výpadku napájení během práce s nimi. Jediná možnost ochrany je v tomto případě zálohované napájení.

Existují dva hlavní druhy záložních napájení. Jsou to [2]:

- **Přídavné akumulátory** – zařízení zapojené mezi počítačem a napájením, které se průběžně dle potřeby dobíjí a v případě výpadku běžného napájení dokáže krátkodobě (řádově několik desítek minut) počítač zásobovat energií. Během této doby má uživatel dostatek času všechna data uložit a ukončit práci.
- **Generátory** – většinou se používají v institucích, kde je běh počítačů nezbytný, například v nemocnicích. Generátor elektrickou energii sám vyrábí, proto je doba jeho provozu omezena pouze přísunem paliva.

V praxi se obvykle používá kombinace obou druhů, přičemž nejdříve přicházejí na řadu přídavné akumulátory a pokud není běžné napájení obnoveno do vyčerpání jejich kapacity, jsou aktivovány generátory.

3.3 Kryptologie

Kryptologie je matematický vědní obor, který se zabývá šifrovacími a kódovacími algoritmy. Dělí se na dvě velké skupiny – kryptografii, která se zabývá návrhem šifrovacích algoritmů, a kryptoanalýzu, která se naopak snaží šifrovací metody prolomit. [2] Slovo kryptografie pochází z řečtiny – kryptós je skrytý a gráphein znamená psát.

V současné době je šifrování nezbytnou součástí běžného života, obzvláště pak v oblasti komunikace. Firmy si potřebují vyměňovat důležité informace, je třeba archivovat citlivé údaje o zaměstnancích apod. I většina soukromých osob má potřebu některé ze svých osobních souborů šifrovat. Důležité je to zvláště v případě moderních metod, které dnes Internet a jiné technologie umožňují. Bylo by jistě zbytečné mít ke svému bankovnímu či jinému účtu heslo, kdyby bylo zasíláno v nezabezpečené podobě, a bylo by tedy kýmkoliv odposlechnutelné.

Kryptografické metody obecně využívají tzv. "klíč", pomocí kterého tajná data zašifrují a posléze opět rozšifrují. Současně některé metody umožňují nebo i vynucují použití více klíčů různých pro zakódování a rozkódování.

Utajení dokumentu se skládá z dvou částí: utajení šifrovací metody a utajení klíče. Zásadní je zejména utajení klíče, jelikož metod není takové množství, aby nemohlo dojít k jejímu odhalení. Často se tedy ani k utajení vlastní metody nepřistupuje a utajení zajišťuje jen klíč.

Většina moderních algoritmů je založena na matematické teorii čísel. Tzv. kryptografická transformace T je libovolné prosté zobrazení množiny celých čísel na odlišnou množinu celých čísel. [5]

3.3.1 Symetrická a asymetrická kryptografie

V počátcích šifrování bylo využíváno symetrických alogoritmů, což znamená, že text je jak zašifrován, tak rozšifrován oběma komunikujícími stranami pomocí stejného klíče (tajného, aby nemohlo dojít k rozšifrování nepovolanou osobou). Tato metoda je spolehlivá, je však vhodná pouze ke komunikaci dvou, případně několika málo stran. Pokud komunikují 4 strany a chtějí mít zajištěnou možnost nerušené komunikace každý s každým zvlášť, je již zapotřebí šesti klíčů, přičemž počet klíčů s počtem stran roste podle vzorce n*(n-1)/2, kde n je počet komunikujících stran. Časová náročnost i náročnost na správu klíčů je u symetrické kryptografie velmi vysoká. Hodí se tedy k šifrování dat uložených na discích, nikoli pro šifrování přenášených dat. [2, 5]

Symetrická kryptografie je založena na dvou základních principech. Prvním z nich je substituce, tedy nahrazení jednotlivých znaků jinými. Nejjednodušší ze všech substitučních šifer je tzv. monoalfabetická šifra, jejíž princip spočívá v posunutí jednotlivých znaků abecedy o několik dále (u tzv. Césarovy šifry o tři, u šifry ROT3 o 13 znaků), případně v přeházení jednotlivých znaků. Monoalfabetická šifra je velmi snadno rozluštitelná, v případě posunutí abecedy není třeba ani využití počítače k rozšifrování textu. Mírně složitější je tzv. homofonní šifra, která šifruje každé písmeno abecedy vždy na jedno z několika možných jiných písmen, je však stále poměrně jednoduše rozluštitelná. Polygramová šifra pracuje na stejném principu jako monoalfabetická s tím rozdílem, že zaměňuje celé skupiny znaků za jiné skupiny o stejné délce. Polyalfabetická šifra je nejsložitější ze skupiny substitučních šifer, její princip spočívá v kombinaci několika monoalfabetických šifer, jichž může být libovolný počet (n). První znak je šifrován první šifrou,druhý druhou až do n-tého znaku, který je šifrován n-tou šifrou. Znak číslo n+1 je pak šifrován opět šifrou první.[2]

Transpozice je druhý způsob symetrického šifrování založený na principu změny pořadí znaků ve zprávě. Princip této šifry spočívá v jednoduchém rozepsání textu do více řádků o stejné délce a poté v jeho opětovném složení, ovšem po sloupcích. To vede k až překvapivě dobrému zašifrování textu, zvláště tehdy, pokud je text takto přeuspořádán několikrát.

Z důvodu velkého počtu klíčů při šifrování přenášených dat symetrickými algoritmy byly vyvinuty tzv. asymetrické šifrovací algoritmy, které pracují na principu párových klíčů. Každá z komunikujících stran vlastní dva klíče – veřejný a privátní. Soukromý klíč uchovává v tajnosti a veřejný klíč předá všem, se kterými chce komunikovat. Text zašifrovaný soukromým klíčem je možno rozšifrovat pouze klíčem privátním a naopak. Výhoda této metody spočívá v nenáročnosti na správu klíčů a v možnosti zaslat text komukoliv, případně ho přijmout od kohokoliv, kdo má přístup ke klíči veřejnému. Nevýhodou je vyšší časová náročnost při šifrování větších objemů dat, asymetrická kryptografie potřebuje podstatně delší klíče než symetrická. [2]

V poslední době se rozšířilo využívání další možnosti – hybridních algoritmů. Jejich princip spočívá v zašifrování textu jednorázovým jednoduchým symetrickým klíčem, který je pak zašifrován asymetrickým klíčem. Příjemce musí nejprve rozšifrovat jednorázový klíč párovým asymetrickým klíčem, samotnou zprávu pak klíčem jednorázovým. Tento způsob eliminuje nevýhody jak symetrické (velký počet klíčů), tak asymetrické (délka klíčů a časová náročnost) kryptografie.

Pro maximální bezpečnost dané šifry musí šifrovaný text splňovat jednu podmínku. Musí být maximálně nerozeznatelný od náhodného šumu, ať je příslušný otevřený text jakýkoliv. V praxi to znamená, že při šifrování miliónu stejných znaků otevřeného textu musí být v šifrovaném textu rovnoměrně zastoupeny všechny možné znaky. [2] Důvodem je snaha zajistit, aby bylo nemožné odhadnout, z jakého jazyka původní text pochází.

3.3.2 Kryptoanalýza

Kryptoanalýza je jedna z oblastí kryptologie, která se zabývá luštěním šifrovaných textů. V současné době, kdy jsou téměř všechny šifrovací algoritmy odtajněny, aby mohly být testovány veřejností, je cílem kryptoanalýzy nejen získat šifrovaný text a klíč, jímž byl zašifrován, ale současně vyvinout i algoritmus opačný, tedy takový, který šifrovaný text převede zpět na čitelný.

Existuje několik možností útoků na šifrovaný text. Ne vždy je možno provést všechny tyto útoky, kryptoanalytik musí dobře zvážit své možnosti a také odhadnout, který přístup je pro konkrétní příklad nejvhodnější. [2]

Prvním a také nejzákladnějším způsobem je tzv. útok hrubou silou. Principem je snaha rozšifrovat text pomocí výpočetního systému postupným zkoušením všech možných klíčů. Nevýhodou je nejen velká časová náročnost (u dlouhých klíčů je často nemožné tuto metodu využít), ale i to, jak zajistit,aby systém poznal, že našel správný klíč. Řešením je většinou slovník, který luštící systém obsahuje a u každého klíče porovná slova s rozluštěným textem. Pokud text obsahuje některé slovo ze slovníku, je vysoká pravděpodobnost, že klíč je správný.

Luštění se znalostí šifrovaného textu spočívá v porovnávání několika textů zašifrovaných stejným algoritmem a stejným klíčem.[2, 11]

Luštění se znalostí otevřeného textu je obdobné jako v předchozím případě s tím rozdílem, že máme zároveň některé texty v původní podobě, nevíme ovšem, které texty přísluší k jednotlivým zašifrovaným textům. Tento způsob je výrazně jednodušší než v případě absence otevřených textů.[2, 11]

Luštění se znalostí vybraných otevřených textů je metoda využívaná v případě, že máme k dispozici šifrovací zařízení, můžeme tedy zašifrovat libovolný text. To nám umožní velmi efektivně určit, jakým algoritmem byl text zašifrován.[2]

Luštění se znalostí vybraných šifrovaných textů je způsob opačný než předchozí. Můžeme dešifrovat libovolný text, nemůžeme ho ovšem zašifrovat.[2, 11]

Poslední a často nejúčinnější způsob je tzv. **korupční metoda**, při které od osoby, které je klíč či algoritmus znám, přesvědčováním či naopak výhružkami algoritmus získáme. [2]

3.4 Síťová bezpečnost

Každému počítači, zvláště pak připojenému do sítě Internet, hrozí celá řada nebezpečí, ať už jde o odposlechnutí či dokonce modifikaci dat, nebo o možnost vniknutí nechtěného softwaru, který může napáchat v nezabezpečeném operačním systému řadu škod. V této kapitole proto bude popsána základní problematika škodlivého softwaru a síťových připojení.

3.4.1 Škodlivý software

Jako škodlivý software bývá obecně označován jakýkoliv software, který má (ať už jakýmkoliv způsobem) za úkol uživateli škodit. Bývá také často označován jako tzv. **malware** (malicious software). Existuje několik základních typů škodlivého softwaru

. Prvním a nejznámějším typem škodlivého softwaru je **virus**. Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele.[3] Název byl odvozen od skutečného biologického viru, protože stejně jako on je škodlivý, snaží se šířit a stejně tak potřebuje k životu hostitele. Tím je v případě počítačového viru nejčastěji soubor, případně některá část pevného disku. Viry můžeme rozdělit podle dvou základních hledisek, a to **podle hostitele** či **podle způsobu činnosti**. [2]

Dělení virů podle hostitele vypadá takto :

- **Viry šířící se pomocí boot sektoru** jsou viry, které infikují tzv. boot sektor na pevném disku. V boot sektoru je na nezavirovaném pevném disku uložen zavaděč operačního systému, který má za úkol na operační systém odkázat po zapnutí počítače. Virus tento sektor přemístí a na jeho místo se uloží sám. Po zapnutí počítače se tedy nejprve spustí virus, který až potom odkáže na operační systém. Výhodou tohoto typu viru je tedy to, že je spuštěn dříve než operační systém a tedy i dříve, než antivirová ochrana.

- **Viry šířící se pomocí spustitelných souborů** jsou viry uložené v některém souboru, u kterého je vysoká pravděpodobnost, že je uživatel sám spustí, případně ještě rozšíří do jiných počítačů.
- **Viry šířící se pomocí nespustitelných souborů** byly velmi dlouho málo využívané a prakticky neškodné, protože škodlivá činnost v souboru je velmi obtížná, nespustitelné soubory se navíc nešíří tolik jako spustitelné. Revolucí pro tyto viry byla implementace programovacího jazyka do kancelářského balíku Microsoft Office, tzv. maker (odtud tzv. makroviry). Makra umožňují vytvořit jednoduchá pravidla či spustit určitou činnost v daném dokumentu. Vzhledem k tomu, že makra se ukládají v tzv. šablonách, které jsou samy o sobě prakticky spustitelnými soubory, je jasné, jak tyto viry pracují. Uloží se do šablony (nejlépe globální, sloužící pro všechny dokumenty) a čekají na spuštění. Makra mohou být spuštěna nechtěně pomocí přiřazené klávesové zkratky či položkou v nabídce, bývají proto často aktivována bez vědomí uživatele. Zároveň málokterý uživatel tuší, že by se v dokumentu mohl skrývat virus, otevře tedy dokument bez obav. [2]

Podle způsobu činnosti jsou pak viry děleny takto [4]:

- **Rezidentní –** takto bývá označován virus, který se se spuštěním hostitele (a tedy i viru samotného) rozšíří do různých souborů na pevném disku.
- Jako **nerezidentní** jsou označovány viry, které se uloží po spuštění do operační paměti a infikují pouze ty soubory, se kterými uživatel pracuje. [22]

Dalším typem škodlivého softwaru je tzv. **červ** (worm). Základní rozdíl mezi červem a virem je ve většině případů ten, že červ nepotřebuje ke svému šíření hostitelský soubor, šíří se sám o sobě pomocí počítačové sítě. Červ navíc na rozdíl od viru zůstává v převážné většině stejný, neumí napadat jiné soubory. To však nemusí platit vždy, nejnovější červi dokáží mutovat a infikovat soubory stejně jako viry. Červ bývá většinou uložen v souboru, který imituje nějaký nespustitelný soubor, ale ve skutečnosti je souborem spustitelným. Například průzkumník Microsoft Windows v základním nastavení nezobrazuje přípony souborů, tedy soubor tvářící se jako obrázek

může být ve skutečnosti červ ve spustitelné podobě. Uživatel pak s klidným srdcem "obrázek" otevře, čímž spustí tělo červa a ten začne páchat škodu. [2]

Trojský kůň je program, který pracuje bez vědomí či dovolení oběti. Ačkoliv nemusí způsobovat žádnou škodu, většina trojských koní vykonává činnosti, které narušují zabezpečení počítače, například zneužíváním práv uživatelů. Trojský kůň je ve většině případů maskován v podobě nějakého programu, který je pro uživatele žádoucí (hra, spořič obrazovky, aktualizace operačního systému apod.). Ve skutečnosti ale po nainstalování získává různá data, např. hesla, nebo vykonává nechtěné změny v souborech, může dokonce odstranit soubory nezbytné pro běh systému. [3]

V poslední době se často objevují nové druhy nebezpečného softwaru, a to takové, které kombinují vlastnosti všech předchozích kategorií. Jejich výhodou (nebo naopak nevýhodou, a to pro uživatele) je schopnost rychleji se šířit, využívají totiž ke svému šíření přímo serverů, na rozdíl od běžných virů, které využívají poštovní schránky uživatelů. [3]

3.4.2 Obrana proti škodlivému softwaru

Nejjednodušším a zároveň nejspolehlivějším způsobem ochrany proti škodlivému softwaru je používání antiviru s pravidelně aktualizovanou databází. Prvními předchůdci antiviru byly programy, které se snažily chránit počítač před tehdejšími, velmi jednoduchými viry. V době takřka nulových znalostí fungování virů bylo ovšem velmi obtížné počítač chránit, proto se každý program zabýval pouze jedním či několika málo typy viru. Postupem času se jednotlivé programy rozšiřovaly, až vznikl první víceúčelový antivirus. Dnes existuje na trhu mnoho antivirů s komplexní ochranou operačního systému. Velká většina z nich pracuje na pricipu kombinace dvou základních metod vyhledávání škodlivého softwaru – vyhledávání na základě signatur a heuristické analýze. [2]

Vyhledávání na základě signatur vychází z předpokladu, že virus obsahuje jistý unikátní řetězec – signaturu, který ho dokáže jednoznačně identifikovat.[2] Pokud některý soubor obsahuje signaturu obsaženou v databázi, je infikován virem. Dřívější antiviry nedokázaly odhalit viry mutující, tedy měnící své tělo, dnešní antiviry si však bez problémů poradí i s těmi nejsložitějšími viry. Moderní antiviry navíc dokážou napadený soubor často opravit vyříznutím viru či nahrazením neškodnou částí.

Heuristická analýza funguje na zcela odlišném principu. Vyhledává totiž i viry, jejichž signatura dosud není obsažena v databázi. Vyhledávání v tomto případě provádí pomocí kontroly podezřelé činnosti. Pokud některý program provádí činnost, která není příliš běžná, ověří si, zda k tomu má skutečně oprávnění a důvod. Pokud nikoli, označí ho za virus. Tento způsob však snižuje rychlost počítače, u starších pak velmi výrazně, je totiž třeba kontrolovat každý běžící proces. [2]

Nejmodernější antiviry kromě kombinace těchto dvou metod dokáží i zaslat podezřelé soubory firmě, kterou jsou vyvíjeny, k analýze,aby mohly být následně případně zahrnuty do databáze signatur.

3.4.3 Síťová komunikace

V současné době, kdy je k síti Internet připojen již téměř každý počítač, je riziko napadení systému výrazně vyšší než v dobách, kdy jediná možnost napadení spočívala v prolomení fyzického přístupu k počítači, případně v přenesení škodlivého softwaru na disketě. Důvodem síťových útoků, ať už v jakékoliv podobě, je nejčastěji získání určitých citlivých informací či soukromých dat.

Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. [17]
V současné době je nejčastěji využívána architektura TCP/IP, která je členěna do čtyř vrstev [17]:

- **Vrstva síťového rozhraní** - Nejnižší vrstva, umožňuje přístup k fyzickému přenosovému médiu.
- **Síťová vrstva** - Vrstva zajišťuje síťovou adresaci, směrování a předávání datagramů.
- **Transportní vrstva** - Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace.
- **Aplikační vrstva** - Vrstva aplikací, což jsou programy (procesy), které využívají přenosu dat po síti ke konkrétním službám pro uživatele.

V síťové vrstvě je používán jeden základní protokol, a to protokol IP (Internet Protocol). Provádí vysílání datagramů na základě síťových IP adres obsažených v jejich záhlaví. Každý datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesilateli a pořadovém čísle datagramu ve zprávě. Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy.

V aplikační a v transportní vrstvě jsou používány dva protokoly: TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). Protokol TCP vytváří mezi počítači jakési dlouhodobé spojení, které zaručuje spolehlivé doručení všech dat, jež jsou mezi počítači zasílána. Pokud dojde na cestě mezi oběma počítači ke ztrátě určitých dat, je zajištěno jejich opětovné zaslání.[3] Druhý protokol, UDP, umožňuje sice menší velikost posílaných dat, zato však má pro svůj provoz menší nároky, dá se proto implementovat jednodušším softwarem. Na druhou stranu neumožňuje kontrolu a opětovné zaslání dat. Je proto využíván například pro přenos multimediálních souborů, u kterých je ztráta malé části dat těžko postřehnutelná, prodlevy při opětovném přenosu by však byly značné. [3]

Dalším důležitým pojmem v oblasti síťové komunikace jsou tzv. porty. Ty jsou pomyslnými čísly (od 1 do 65535), kterými počítače označují společný komunikační kanál na síti. Existují určité konvence, které přiřazují konkrétním službám jednotlivé porty pro komunikaci. Není však nutné využívat právě tyto porty, každý port může být využit k libovolnému účelu.[3] Komunikace v praxi vypadá tak, že pokud jeden počítač posílá jinému počítači po síti určitá data, musí definovat jeho adresu, jakým protokolem přenáší a také port, na kterém komunikuje. V případě protokolu TCP je otevřeno spojení a výchozí počítač čeká na potvrzení o doručení zprávy, případně pošle znovu nedoručená data. V případě protokolu UDP jsou data pouze odeslána, zda také dorazí, už není jisté. Pokud na správném portu na cílovém počítači naslouchá (přijímá data) určitá aplikace, jsou data přijata. [3]

Aby nemohlo dojít k narušení přístupu (zasláním nesprávných, nebezpečných dat), je vhodné využívat tzv. Firewall. Nastavením firewallu a jeho funkcí v systému Windows se bude zabývat kapitola *Správa zabezpečení systému Microsoft Windows XP*.

4 Správa zabezpečení systému Microsoft Windows XP

Operační systém Windows XP obsahuje celou řadu nástrojů pro správu zabezpečení. Tato kapitola se bude snažit co nejlépe charakterizovat ty nejdůležitější a popsat jejich funkce, dále pak doporučit nastavení pro dosažení maximální úrovně zabezpečení.

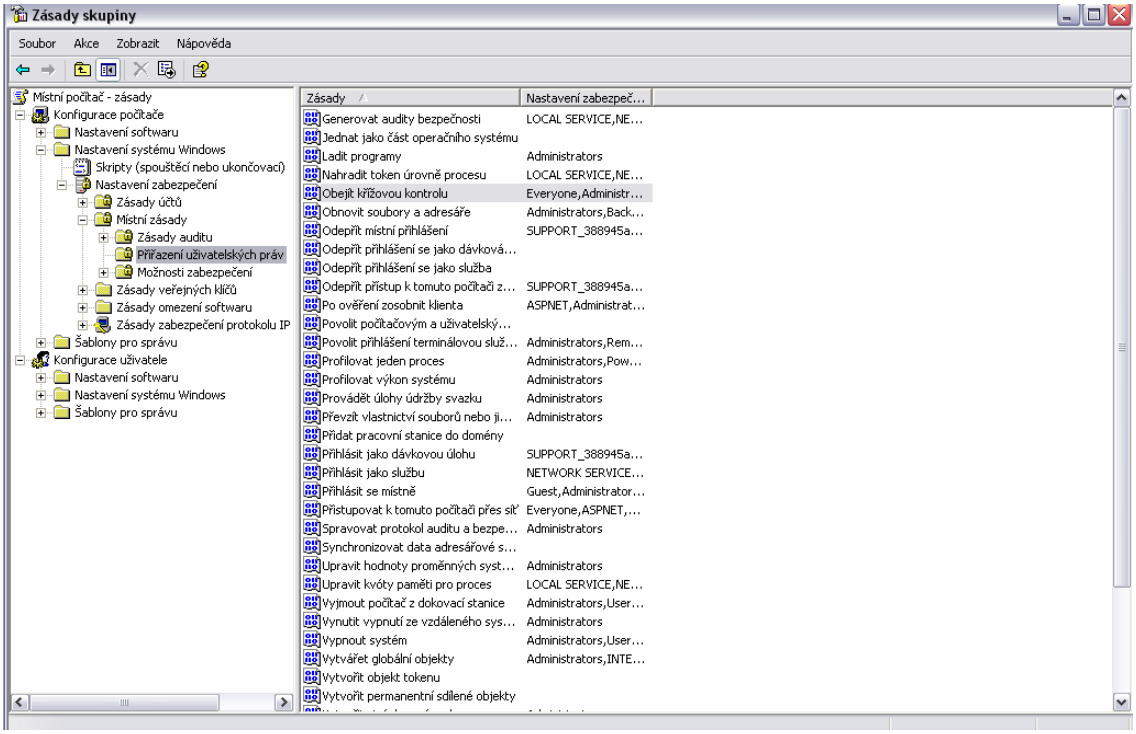
Hlavní funkcí systému Windows XP verze Professional, která umožňuje správci počítače konfigurovat systém a případně zabránit uživatelům, aby tuto konfiguraci mohli změnit, je funkce Zásady skupiny.[3] Správce počítače může pomocí konzole Zásady skupiny konfigurovat standardní nastavení pracovního rozhraní, přidělovat uživatelům detailní práva, stejně jako konfigurovat nastavení celého počítače. Primární funkcí této konzole je ovšem správa zabezpečení systému, proto je možné ji označit za hlavní nástroj správy zabezpečení Windows XP. Konzole Zásady skupiny obsahuje dvě hlavní části – *Konfigurace počítače* a *Konfigurace uživatele*.

Konfigurace počítače slouží k nastavení zásad, které jsou v daném počítači uplatňovány vždy, bez ohledu na to, který uživatel se k němu přihlásí [1]. Obsahuje tři základní položky.

- Nastavení softwaru
- Nastavení systému Windows
- Šablony pro správu

Z hlediska zabezpečení je významná především položka *Nastavení systému Windows*, neboť obsahuje podpoložky *Zásady účtů* (viz kapitola *Uživatelská hesla*), *Přiřazení uživatelských práv* (viz kapitola *Zabezpečení jednotlivých účtů a skupin*) a *Možnosti zabezpečení* (obsahuje např. nastavení zásad souvisejících s přihlašováním pomocí sítě a jejím zabezpečením či interaktivním přihlašováním).

Konfigurace uživatele slouží k upřesnění nastavení uživatelských účtů bez ohledu na to, ke kterému počítači je uživatel právě přihlášen (týká se pouze uživatelských účtů, které se přihlašují k doméně) [1]. Položky v této části konzole jsou analogické k položkám v části *Konfigurace počítače,* aplikují se však pro uživatele.



*Obrázek č. 3: Konzole **Zásady skupiny**, sloužící mimo jiné ke správě zabezpečení Windows XP*

Položka *šablony pro správu* slouží v obou částech konzole k nastavení hodnot registru pro jednotlivé zásady, což je nejnižší možná úroveň, tedy nejbližší samotnému jádru operačního systému. Jednotlivé šablony jsou textové soubory s příponou .inf, z nichž každá je přednastavena ke konkrétnímu účelu. Šablony je vhodné využít především při nastavování více počítačů stejným způsobem, kdy je možné použít některou z přednastavených šablon, případně určitou šablonu upravit a přenést na ostatní počítače.

4.1 Uživatelské účty a hesla

Uživatelské účty jsou základním kamenem téměř každého operačního systému, nejinak je tomu i u Windows XP. Díky uživatelským účtům a vhodně zvoleným heslům je možné úroveň zabezpečení operačního systému výrazně zvýšit, protože je možné takto konkrétním uživatelům, případně skupinám uživatelů ukládat různá omezení nebo jim naopak přidělovat různá privilegia. [3]

Tato kapitola se bude kromě uživatelských účtů zabývat heslům k nim, protože vhodně zvolené heslo je hůře prolomitelné a tím se riziko neoprávněného přístupu do systému minimalizuje. S uživatelskými účty a hesly úzce souvisí proces přihlašování, proto se jím tato kapitola bude také zabývat.

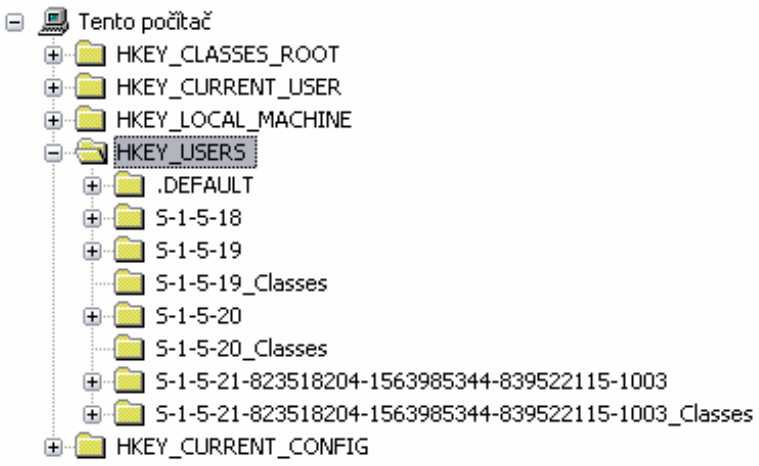
Uživatelské čty je možné rozdělit na dvě základní kategorie. *Místní účty* a *Doménové účty*. *Místní účty* jsou uloženy na daném počítači a přihlášení je tedy možné na něm. *Doménové účty* jsou využívány k vzdálenému přihlašování.

4.1.1 Výchozí uživatelské účty

Údaje o všech uživatelských účtech jsou ve Windows XP ukládány do chráněné databáze zvané Security Accounts Manager (SAM, správce bezpečnosti účtů). [3] Běžný uživatel se k uživatelským účtům odkazuje pomocí uživatelských jmen, systém však k jednoznačné identifikaci potřebuje bezpečnostní identifikátor SID, který je pro každý účet jedinečný, žádným dvěma uživatelským účtům tedy nemůže být za žádných okolností na stejné instalaci Windows přiřazen shodný identifikátor. I v případě, že by byl vymazán existující účet a poté vytvořen účet nový, se shodným jménem, systém by mu přiřadil nové SID. Toto vylučuje možnost, že by útočník obnovil některý účet pro získání vyšších práv, než jaká mu přísluší.

Každá instalace Windows XP obsahuje minimálně dva výchozí uživatelské účty. Prvním je účet Administrator, kterému přísluší veškerá práva nad celým počítačem a zobrazuje se tehdy, když nejsou vytvořeny žádné jiné účty. Tento účet je využíván k

vytváření nových uživatelských účtů bezprostředně po instalaci, případně slouží jako stálý účet správce. Druhým základním účtem je účet Guest (host), který slouží pro přístup osobám, které svůj vlastní účet nemají. Tento účet má velmi omezená práva a je možné ho deaktivovat. Windows XP má zpravidla vytvořeny ještě další dva skryté účty, a to účet HelpAssistant, sloužící pro vzdálený přístup asistenční služby firmy Microsoft, a účet Support, jehož plný název doplňuje číslo výrobce, ten pak slouží pro přístup servisních techniků při opravě počítače. [3]



Obrázek č. 4: Klíče registru značící hodnoty SID jednotlivých uživatelských účtů, kromě tří výchozích účtů označených hodnotami S-1-5-18 až 20 je na této instalaci pouze jeden uživatelský účet.

4.1.2 Bezpečnostní skupiny

Bezpečnostní skupiny, ve Windows XP nazývané *Typ účtu*, slouží k přiřazení určitých práv více než jednomu účtu. Představují výrazné ulehčení práce správce počítače, pokud na jednom počítači pracuje velké množství uživatelů. Nejen jednodušší, ale i bezpečnější, než přiřazovat každému uživateli jednotlivá práva, je vytvoření několika bezpečnostních skupin a následné přiřazování jednotlivých účtů skupinám. Touto cestou se sníží riziko případné chyby, protože počet operací je výrazně nižší než při přidělování práv jednotlivým uživatelům. [3]

Výchozí instalace Windows XP Professional obsahuje devět základních uživatelských skupin, přičemž je možné vytvořit libovolné množství dalších, pro zjednodušení se však zařazuje do jedné ze čtyř následujících skupin [3]:

- **Administrators** – skupina správců počítače s neomezenými právy
- **Users** – skupina uživatelů s omezeným přístupem
- **Guest** – účet typu host
- **Unknown** – nestandardní účet, vzniká při přenosu uživatelských účtů z předchozí verze Windows na verzi XP

4.1.3 Zabezpečení jednotlivých účtů a skupin

Systém Windows XP umožňuje detailní přidělování práv jednotlivým uživatelům a uživatelským skupinám. K tomuto přidělování slouží konzole pro správu *Zásady skupiny,* respektive její podpoložka *Přiřazení uživatelských práv.* V ní se nacházejí jednotlivé zásady, značící privilegia pro práci v systému a jeho správu. U každé zásady je možné nastavit, pro kterého uživatele či uživatelskou skupinu je platná.

Aby bylo omezení přístupu a práce pomocí uživatelských účtů a skupin efektivní, je vhodné dodržovat některá pravidla. Nejdůležitějším pravidlem je přiřazení patřičných práv jednotlivým účtům, respektive skupinám, do kterých účty patří.

Uživatelé typu **administrator**, tedy správci, mají neomezenou kontrolu nad systémem, náleží jim tedy všechna následující práva [3]:

- Vytvářet, měnit, odstraňovat uživatelské účty a skupiny a přiřazovat jim práva.
- Instalovat programy
- Sdílet složky
- Nastavovat oprávnění
- Přistupovat k veškerým souborům a přebírat jejich vlastnictví
- Instalovat nebo odstraňovat hardwarová zařízení
- Přihlašovat se v nouzovém režimu

Uživatelé patřící do skupiny **Users** by neměli mít následující práva [3]:

- Modifikovat záznamy registru, které se týkají celého počítače
- Modifikovat soubory operačního systému
- Modifikovat soubory programů, které nainstaloval správce pro všechny uživatele
- Instalovat programy, které by mohli spouštět ostatní uživatelé, nebo spouštět programy, které nainstalovali jiní uživatelé na úrovni Users

Podle společnosti Microsoft by měl být účet typu Administrator využíván co nejméně, aby bylo minimalizováno riziko poškození konfigurace počítače. I správce by měl pro běžnou práci využívat účet s nižším oprávněním, pokud právě nepotřebuje vykonávat činnost, ke které je účet typu Administrator nutný. [3]

4.1.4 Omezení přístupu k datům pomocí uživatelských účtů a skupin

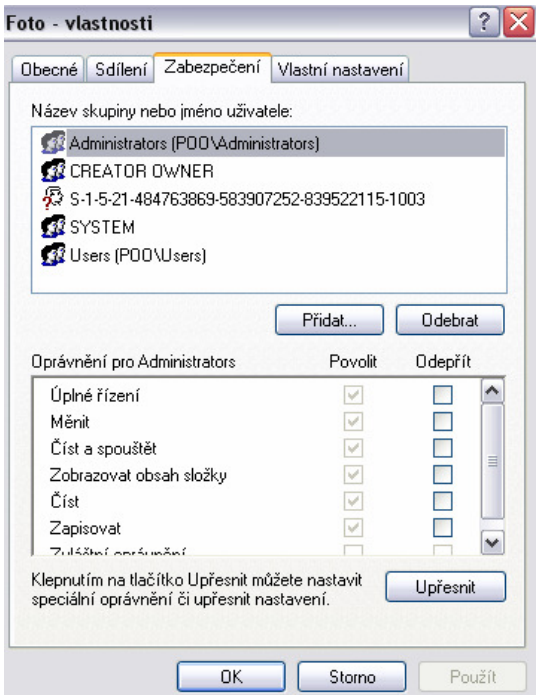
V systému Windows XP je používán systém souborů NTFS (New Technology File System [12]), který umožňuje rozšířené řízení přístupu ke každé jednotlivé složce a souboru (tento systém souborů nahradil dříve používaný systém souborů FAT, který rozšířené řízení přístupu neobsahoval). Na disku naformátovaném tímto systémem souborů tabulka souborů obsahuje pro každou složku a soubor seznam řízení souborů ACL (access control list), který jednoznačně určuje, kteří uživatelé (případně uživatelské skupiny) mohou k danému souboru přistupovat. Jednotlivé položky ACL se označují ACE (access control entry, neboli záznam o řízení přístupu) a skládají se z identifikátorů uživatelských účtů SID (pro jednoznačné rozpoznání účtů, systém Windows zobrazuje místo SID název účtu či skupiny) a z oprávnění, která jsou pro daný SID přidělena. Právo povolovat či omezovat přístup k souborům a složkám má jejich vlastník (nejčastěji ten, kdo je vytvořil) a členové skupiny Administrators, pokud jim přístup vlastník nezakáže. [3]

Přidělování práv pro jednotlivé složky se provádí pomocí Průzkumníku Windows.[1] Uživatel klikne pravým tlačítkem na soubor či složku, kterou chce šifrovat, vybere volbu *Vlastnosti* a následně kartu *Zabezpečení.* V této kartě lze poté jednoduše přidělovat šest základních typů oprávnění jednotlivým uživatelům či skupinám.
Jednotlivá oprávnění jsou:

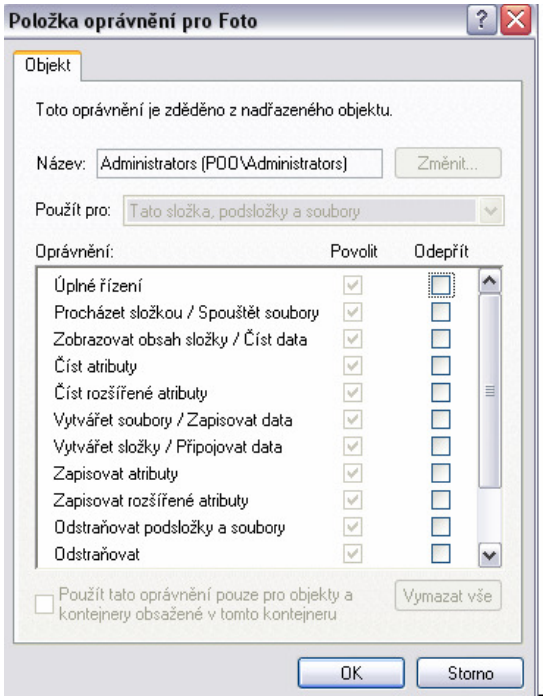
- **Úplné řízení** – Dává příslušnému uživateli veškerá práva k práci se složkou či souborem. Uživatel může nejen soubory číst a měnit,ale i přidělovat oprávnění k nim jiným uživatelům (pokud je oprávění přiděleno, jsou automaticky přidělena i veškerá oprávnění, která leží na kartě pod ním).

[1] V systému MS Windows XP je standardně nastaveno zjednodušené sdílení souborů. Pro přidělování práv jednotlivým uživatelům je tuto volbu nutno vypnout, což lze jednoduše provést ve verzi Professional, ve verzi Home pouze v nouzovém režimu. V obou případech toto může učinit pouze správce systému. Návod, jak toto provést lze nalézt na internetových stránkách podpory firmy Microsoft [10].

- **Měnit** – Dává uživateli oprávnění soubory číst, modifikovat a mazat, nedává mu však možnost přidělovat oprávnění jiným uživatelům (pokud je oprávění přiděleno, jsou automaticky přidělena i veškerá oprávnění, která leží na kartě pod ním).
- **Číst a spouštět** – Dává uživateli oprávnění otevírat soubory, případně je spouštět, jde-li o spustitelný program.
- **Zobrazovat obsah složek** – Tato položka je k dispozici pouze u složek. Její princip je stejný jako u položky *Číst a spouštět*, rozdíl je však v tom, že uživatel může zobrazovat a otvírat pouze složky této složce podřízené, nikoliv soubory, které obsahuje.
- **Číst** – Umožňuje uživateli prohlížet soubory, složky a jejich vlastnosti, nemůže je však modifikovat.
- **Zapisovat** – Umožňuje vytvářet soubory v příslušné složce a číst jejich vlastnosti.



*Obrázek č. 5: Karta **Zabezpečení**, sloužící k přidělování práv pro přístup k souborům a složkám jednotlivým uživatelům a uživatelským skupinám.*

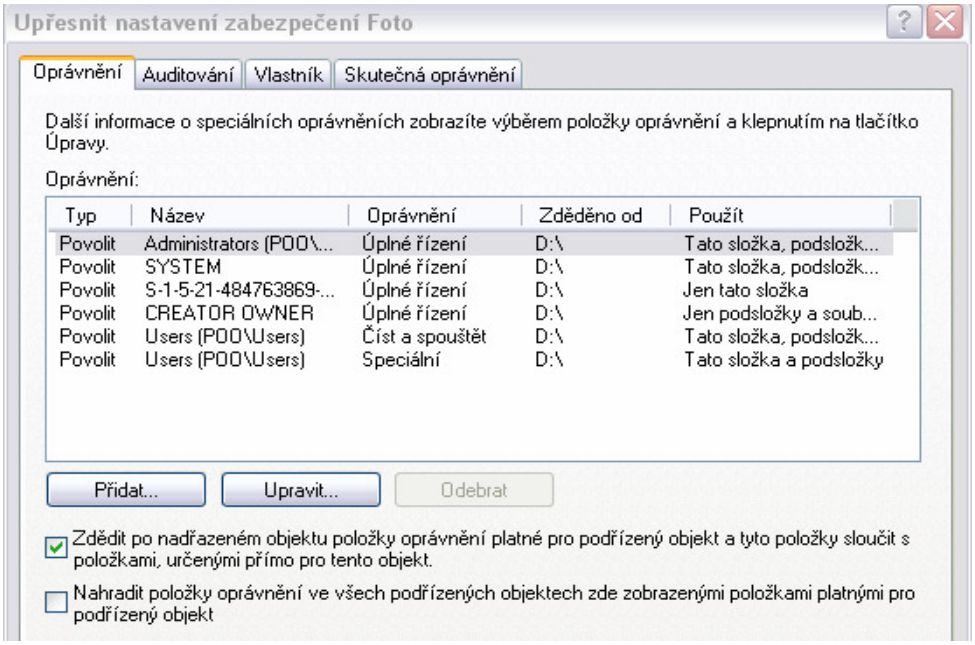


Obrázek č. 6: Dialogové okno Položka oprávnění, sloužící k detailnímu nastavení přístupových práv.

Kromě těchto šesti základních oprávnění je v nabídce ještě jedna volba, a to *Zvláštní oprávnění*, kterou však nelze vybrat. Využívá se tehdy, pokud základní možnosti neodpovídají požadavkům uživatele. V tomto případě tato položka umožňuje nastavit podrobnější oprávnění s rozšířenými možnostmi.

Důležitou vlastností přidělování oprávnění ke složkám je tzv. *dědění*. Pokud uživatel nastaví určitá oprávnění uživatelům či skupinám ke své složce, přechází tato práva na všechny podsložky a soubory v podsložkách obsažené. Je však možné nastavit, aby podsložky oprávnění nedědily, případně práva k nim odebrat. K nastavení dědění oprávnění, případně jejich odebrání, slouží dialogové okno *Upřesnit nastavení zabezpečení*, k němuž se uživatel dostane kliknutím na tlačítko *Upřesnit* v kartě *Zabezpečení*. Zrušením zaškrtnutí políčka *Zdědit po nadřazeném objektu položky oprávnění platné pro podřízený objekt* uživatel vyvolá dialogové okno, ve kterém má možnost výběru ze dvou možností (kromě možnosti *storno*, která pouze zruší předchozí krok):

- **Kopírovat** – Tato možnost zkopíruje oprávnění z nadřazené složky a následně odstraní dědičnou vazbu na ní. Po výběru této možnosti je možné oprávnění nadále upravovat.
- **Odstranit** – Odstraní veškerá oprávnění pro příslušnou složku či soubor zděděná, je tedy následně nutné složce oprávnění přidělit znovu, protože by nemusela mít přidělena žádná oprávnění.

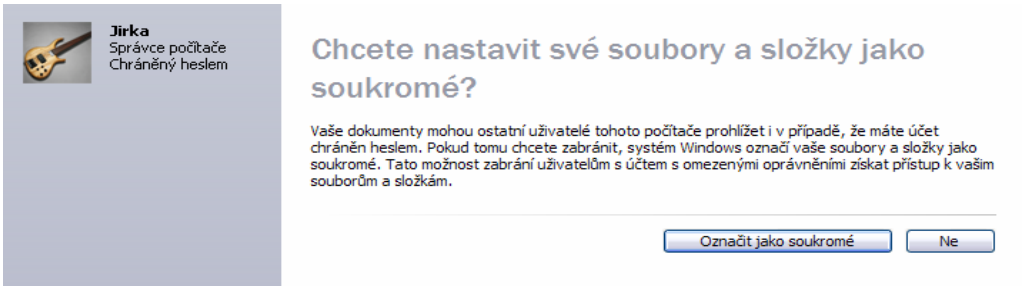


*Obrázek č. 7: Karta **Oprávnění**, sloužící k nastavení dědění práv pro přístup z nadřazených složek*

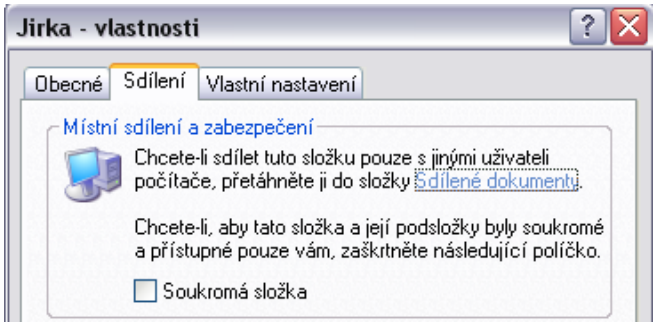
Windows XP obsahuje ještě jednu možnost omezení přístupu k určitým dokumentům, a to šifrování složky Dokumenty jednotlivých uživatelů. Každý uživatel má pro své účely přiřazenou tuto složku, která je standardně přístupná všem uživatelům ze skupiny Administrators a jemu samotnému. Existuje však možnost zamezit v přístupu k této složce všem uživatelům, včetně skupiny Administrators. Pro umožnění šifrování složky Dokumenty však musí být splněno několik podmínek. Kromě naformátování pevného disku systémem souborů NTFS, což se u Windows XP považuje za samozřejmost, nesmí být vypnuta volba Zjednodušené sdílení souborů a účet by měl by měl být chráněn heslem (šifrovat složky uživatelského účtu, ke kterému se může přihlásit každý, je sice možné, ale neefektivní).[3] Nastavit šifrování soukromé složky je uživateli umožněno po nastavení hesla k účtu, kdy se zobrazí dialogové okno, které mu šifrování soukromé složky nabídne. Pokud si uživatel nejprve vybere složku nešifrovat a později své rozhodnutí změní, může postupovat dvěma způsoby.[3] Prvním je odebrání hesla ke svému účtu a jeho opětovné přiřazení, což nabídku k šifrování vyvolá znovu. Druhou možností je přechod do složky Documents and settings na

systémovém disku, kliknutí pravým tlačítkem myši na složku s názvem příslušného účtu, u které se v nabídce Vlastnosti a dále pak v záložce Sdílení nachází položka Soukromá složka, která způsobí již zmíněné zašifrování složky.

Technicky pak zašifrování složky dokumenty vypadá následovně. Ve výchozím stavu jsou ke každé uživatelské složce přiřazena maximální přístupová práva nejen jejímu vlastníkovi, ale i systémovému účtu System a skupině Administrators. Zašifrováním soukromé složky systém Windows XP odebere práva k této složce skupině Administrators, složka tedy zůstane přístupná pouze jejímu vlastníkovi.



Obrázek č. 8: Nabídka umožňující uživateli chránit svoji soukromou složku proti přístupu ostatních uživatelů.



Obrázek č. 9: Karta Sdílení umožňující uživateli chránit svoji soukromou složku proti neoprávněnému přístupu.

4.1.5 Uživatelská hesla

Vhodně zvolené heslo ke každému uživatelskému účtu je základem jeho bezpečnosti. V případě, že se v počítači nenacházejí žádná důvěrná data, není připojen na síť a nehrozí riziko jeho odcizení či narušení fyzického přístupu k němu, není nutné heslo využívat. Všechna tato kritéria jsou ovšem splněna jen u zlomku počítačů, proto se tato kapitola bude zabývat zásadami vytváření uživatelských hesel.

Každé kvalitní uživatelské heslo musí splňovat několik základních podmínek, jak uvádí mnoho autorů odborné literatury. Nejčastějšími chybami při vytváření a používání hesel jsou [3, 8]:

- Používání hesel složených ze slov, které obsahují slovníky (programy na luštění hesel obsahují často databázi několika tisíc slov, která se nejprve snaží využít).
- Používání pojmů, které jsou dotyčným osobám blízké (jméno rodinného příslušníka, oblíbeného sportovního klubu, ale i datum narození ap.) To by mohlo být problematické, pokud by se snažil heslo prolomit někdo, kdo danou osobu zná.
- Používání hesla shodného nebo velmi podobného uživatelskému jménu
- Ukládání hesel na místa blízko k počítači (nejhorší variantou je nalepení papírku s heslem přímo na monitor)

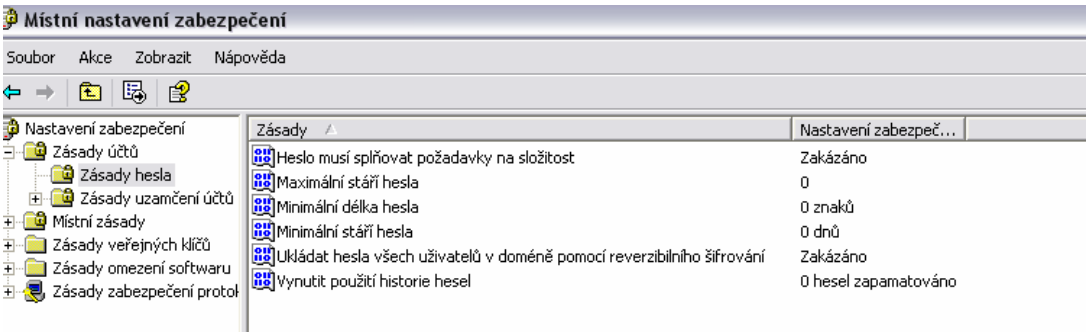
V poslední době se často objevuje pojem tzv. silného hesla. Silné heslo splňuje několik podmínek. Je tvořeno alespoň osmi (některé prameny uvádí šest či sedm) znaky (někteří odborníci doporučují alespoň 15 znaků, systém Windows XP však umožňuje heslo dlouhé až 127 znaků), obsahuje alespoň jedno malé a jedno velké písmeno, jednu číslici a jeden nestandardní symbol (tečky, čárky, mezery apod.).[3][8] Některé internetové aplikace, zejména účty internetového bankovnictví, ale také např. e-mailové schránky používání silného hesla přímo vyžadují. Silné heslo je možné automaticky vygenerovat na mnoha internetových serverech (např. http://www.randpass.com) , případně pomocí programů, které jsou volně ke stažení.

Důležitým faktorem je i pravidelná změna hesla (alespoň jednou za 90 dní [3]), neboť může být odpozorováno nepovolanou osobou při zadávání, případně časem rozluštěno. Heslo by rovněž nemělo být nikde zapsáno.

Kromě toho, že by heslem měl být zabezpečen každý uživatelský účet, je možné zvýšit bezpečnost i dalšími cestami. Windows XP umožňuje správci přinutit uživatele, aby dodržoval zásady bezpečnosti hesel. K tomu slouží konzole místních nastavení zabezpečení, konkrétně její část *Zásady hesla.* Ta obsahuje tyto položky [1, 3, 6]:

- **Heslo musí splňovat požadavky na složitost** – pokud je tato položka povolena, nebude systémem přijato heslo, které je kratší než 6 znaků, neobsahuje kombinaci alespoň jednoho velkého a jednoho malého písmena, jedné číslice a jednoho symbolu a které obsahuje uživatelské jméno nebo část jména osoby. Toto se ovšem nevztahuje na již použitá hesla, proto se tato položka nejčastěji využívá v kombinaci s položkou *maximální stáří hesla*
- **Maximální stáří hesla –** zadáním čísla od 0 do 999 nastaví správce maximální dobu ve dnech, po kterou je heslo platné, poté musí být změněno. Zadání 0 značí neomezenou platnost
- **Minimální stáří hesla** – analogické k předchozí položce, ovšem naopak značí, jak dlouho musí uživatel heslo používat, než jej může změnit. Zadání 0 značí, že uživatel může heslo měnit libovolně
- **Minimální délka hesla** – zadáním čísla 0 až 14 správce povoluje hesla pouze s vyšším počtem znaků, než je zadáno. 0 značí možnost mít účet bez hesla. Opět se nevztahuje na již použitá hesla.
- **Ukládat hesla všech uživatelů v doméně pomocí reverzibilního šifrování –** tato položka při aktivaci zaručí, že hesla nebudou šifrována. V praxi se nepoužívá, slouží pouze pro umožnění spolupráce se staršími aplikacemi.
- **Vynutit použití historie hesel –** 0 značí, že uživatel může měnit heslo na takové, které již někdy použil, naopak číslo od 1 do 24 zadává, kolik předchozích hesel si systém pamatuje a žádné ze zapamatovaných hesel nepřijme.

Uvedené metody jsou vzájemně silně provázány, vždy je tedy vhodné jejich použití kombinovat.



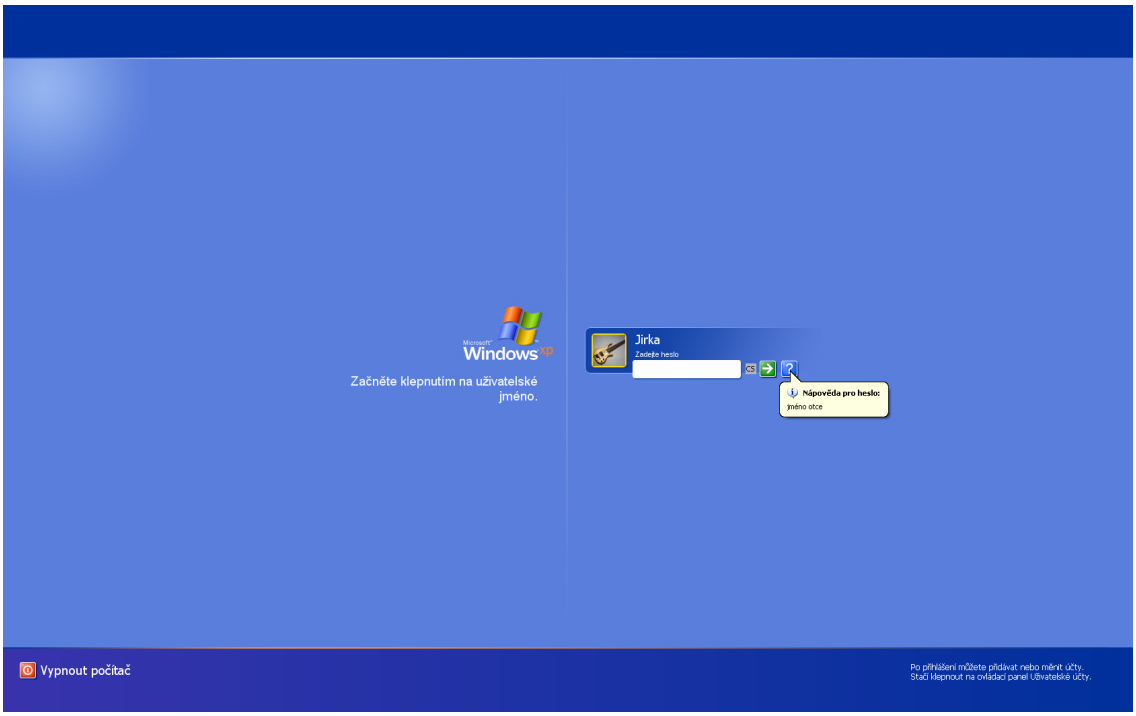
*Obrázek č. 10: Konzole **Místní nastavení zabezpečení**, sloužící kromě jiného pro stanovení zásad pro uživatelská hesla.*

Další možnosti pro ochranu uživatelských účtů a přístupu k nim nabízí skupina nastavení *Zásady uzamčení účtů*. Tyto zásady určují, za jakých podmínek bude zablokován k příslušný uživatelský účet. Je na výběr z těchto položek [1, 3]:

- **Prahová hodnota pro uzamknutí účtu** - určuje počet neúspěšných pokusů pro zadání hesla, který způsobí, že účet uživatele bude uzamčen. Uzamčený účet nelze použít, dokud není odblokován správcem nebo dokud nevyprší doba trvání uzamčení účtu. Počet neúspěšných pokusů je možno nastavit v rozmezí od 1 do 999. Pokud je nastavena hodnota 0, účet nebude uzamčen.
- **Doba uzamčení účtu** - určuje počet minut, po který uzamčený účet zůstane uzamčený, než se znovu automaticky odemkne. Přípustné hodnoty jsou v rozmezí od 1 do 99,999. Je možné také určit, aby byl účet uzamčen do té doby, dokud ho správce sám neodemkne nastavením hodnoty na 0.
- **Vynulovat čítač pro zamknutí účtů po** - určuje počet minut, které musí uběhnout po neúspěšném zadání hesla předtím, než je čítač počtu neúspěšných pokusů nastaven na 0. Přípustné rozmezí je od 1 do 99999.

4.1.6 Proces přihlašování

Proces přihlašování pod systémem Windows probíhá pomocí protokolu Kerberos. Z hlediska uživatele Systém Windows XP nabízí dvě hlavní možnosti přihlašování: interaktivní a klasické. Interaktivní přihlašování zobrazí po startu systému obrazovku se jmény všech uživatelských účtů, pokud nejsou skryty. Pro přihlášení stačí kliknout na příslušný účet a proběhne přihlášení, případně je uživatel vyzván k zadání hesla. Tento způsob přihlašování rovněž umožňuje nastavit k heslu nápovědu, která se zobrazí po kliknutí na příslušnou ikonu. Výhodou tohoto způsobu je možnost přihlášení více uživatelů najednou a přepnutí mezi nimi, uživatel se tedy k přihlášení na jiný účet nemusí odhlašovat. Nevýhodou je naopak zobrazení jmen účtů – případný útočník by nemusel znát uživatelské jméno a přesto by se mohl přihlásit, a to v případě, že by heslo nebylo nastaveno, nebo by se mu heslo podařilo prolomit.



Obrázek č. 11: Obrazovka interaktivního přihlašování se zobrazenou nápovědou k heslu

Druhou možností je klasické přihlašování. V tomto případě se zobrazí dialogové okno se dvěma textovými poli, jedním pro uživatelské jméno a jedním pro heslo. Uživatel v tomto případě musí znát i jméno, což zvyšuje kvalitu zabezpečení, protože je prakticky nemožné uhodnout kombinaci jména a hesla. Naopak při tomto způsobu neexistuje možnost přepínání uživatelských účtů a tedy přihlášení více uživatelů najednou.

Obrázek č. 12: Dialogové okno klasického přihlášení

Pro dosažení maximální úrovně zabezpečení při přihlašování je možné vynutit před zobrazením dialogového pro přihlášení ještě jedno dialogové okno, které vyžádá od uživatele stisknutí kombinace kláves Ctrl, Alt a Delete. Tento způsob zajistí, že bude zobrazeno skutečně dialogové okno Windows a nikoli okno škodlivého programu, který by se mohl pokusit okno napodobit, zmást uživatele a odposlechnout uživatelské jméno a heslo. [3]

Obrázek č. 13: Dialogové okno vyžadující stisknutí kláves Ctrl+Alt+Delete [25]

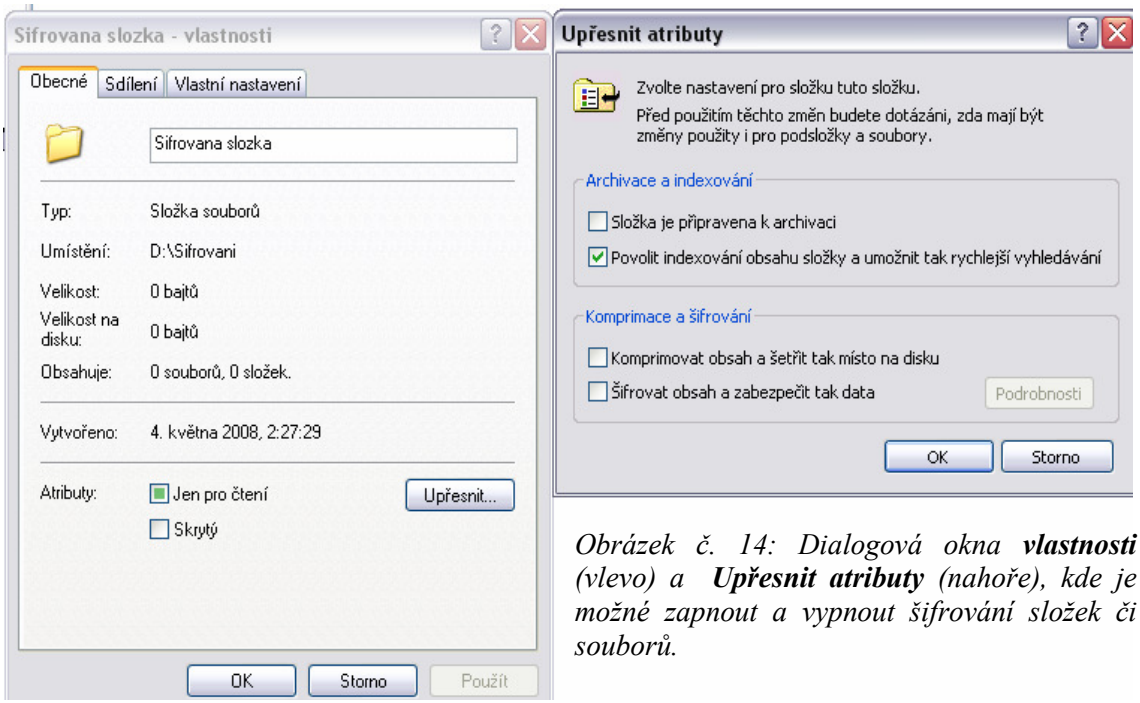
4.2 Šifrování dat pod Windows XP

Každý osobní počítač obsahuje citlivá data, jejichž vyzrazení či odcizení by mohlo vést k určitým ztrátám. Toto platí především pro přenosné počítače ve firmách, ty jsou totiž nejnáchylnější k odcizení. Je proto vhodné data v nich uložená chránit nejen uživatelskými účty operačního systému, každý počítač je možné spustit i bez přihlášení do samotného operačního systému (spouštěcí disketou či instalací odlišného operačního systému). Ani systém souborů NTFS a přístupová práva ke složkám a souborům by nebyla dostatečným nástrojem pro ochranu dat, pokud by byl počítač odcizen, v dnešní době je možné přístupová práva obejít pomocí nástroje NTFSDOS [3].

Operační systém MS Windows XP nabízí velmi spolehlivou ochranu dat v podobě šifrování dat systémem EFS (Encrypting File System). Šifrování pomocí systému EFS vypadá následovně. Při prvním šifrování Windows vytvoří uživateli soukromý certifikát se dvěma asymetrickými párovými šifrovacími klíčí, soukromým a veřejným. Soukromý šifrovací klíč je bezpečně uložen a přístup k němu je možný výlučně při přihlášení na uživatelský účet, na kterém byl vytvořen. Dále systém vytvoří zcela náhodný symetrický šifrovací klíč FEK (File Encryption Key), kterým zašifruje uživatelem zvolená data. Klíč FEK je pak zašifrován veřejným šifrovacím klíčem, rozšifrovat jej (a tedy i zašifrovaná data) je možné pouze privátním asymetrickým klíčem uživatele. Tento způsob tedy kombinuje symetrický a asymetrický způsob šifrování (viz. kapitola 3.3.2). [3, 13]

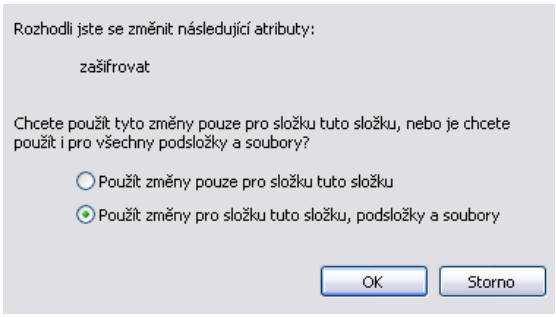
Certifikát s oběma párovými klíči je uživatelskému účtu přiřazen na základě identifikátoru SID. Pokud by byl tedy uživatelský účet odstraněn, nebude data již nikdy možné rozšifrovat.[13] Existuje však možnost, jak zabránit ztrátě dat pro případ, že by příslušný uživatelský účet byl neočekávaně a nenávratně ztracen. Touto možností je zálohování certifikátu ještě před jeho použitím (návod pro zálohování certifikátů je možné nalézt na internetových stránkách podpory firmy Microsoft) . Jak již bylo řečeno, certifikát je vytvořen při prvním použití šifrování pomocí EFS, je tedy vhodné šifrování nejprve použít na zkušební soubor, a to dříve, než je použit v praxi.[3]

Pro případ ztráty soukromého klíče (nejčastěji z důvodu již zmíněného odstranění uživatelského účtu) je možné také určit tzv. *Agenta obnovení*, což znamená poskytnout určenému uživateli (nejčastěji správci počítače) soukromý klíč. Šifrovat systémem EFS je možné jakoukoliv složku či soubor na svazku naformátovaném systémem NTFS (kromě souborů systémových a souborů a složek obsažených v hlavní složce systému Windows), není však možné data zároveň šifrovat a komprimovat (systém Windows XP nabízí komprimaci dat za účelem šetření prostoru na pevném disku, při zašifrování dat je komprimování příslušných souborů či složek automaticky zrušeno) [3]. Samotné šifrování jednotlivých dat se provádí v dialogovém okně *Upřesnit atributy*, které je možné vyvolat kliknutím na tlačítko *Upřesnit* v kartě *Vlastnosti* příslušného souboru či složky. Druhou možností je použití příkazu *cipher* s příslušnými parametry v příkazovém řádku.

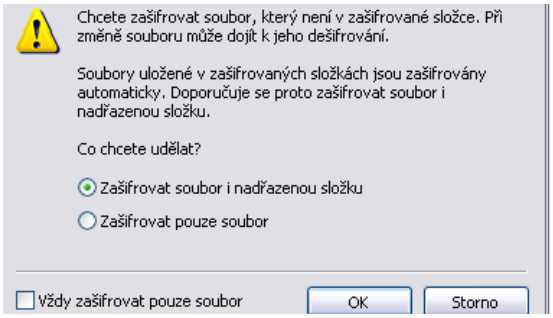


Obrázek č. 14: Dialogová okna ***vlastnosti*** *(vlevo) a* ***Upřesnit atributy*** *(nahoře), kde je možné zapnout a vypnout šifrování složek či souborů.*

V případě šifrování složek systém Windows automaticky nabízí dvě možnosti: zašifrovat pouze samotnou složku a soubory v ní, nebo zašifrovat i podsložky a soubory v nich obsažené Naopak při šifrování jednotlivých souborů systém nabídne zašifrování složky, ve které je soubor obsažen, nebo pouze souboru samotného.[3]



Obrázek č. 15: Dialogové okno dotazující se uživatele, zda zašifrovat pouze složku



Obrázek č. 16: Dialogové okno dotazující se uživatele, zda zašifrovat pouze soubor

Šifrované a nešifrované složky a soubory lze v systému Windows XP jednoznačně odlišit, ve výchozím nastavení se totiž text zašifrovaných složek a souborů zobrazuje v Průzkumníku Windows zeleně, na rozdíl od nešifrovaných černých. Toto rozlišení lze potlačit vypnutím nastavení *Zobrazovat komprimované a šifrované soubory a složky NTFS jinou barvou* v okně *Možnosti složky.*

Obrázek č. 17: Odlišné barevné zobrazení šifrované a nešifrované složky

Šifrování systémem EFS je tzv. transparentní, práce se šifrovanými soubory a složkami je tedy stejná jako s nešifrovanými [1, 3]. To ovšem platí jen tehdy, je-li uživatel přihlášen na účtu, který k nim má povolen přístup (takový účet, na kterém byly zašifrovány, případně takový, kterému vlastník předal svůj soukromý šifrovací klíč). Pokud by byl učiněn pokus o přístup k šifrovaným souborům z jiného účtu, zobrazí se zpráva o odepření přístupu. Uživatel, který má k dané složce či souboru práva systému NTFS nazvaná Měnit nebo Úplné řízení, může ovšem dané soubory či složky odstranit či přejmenovat.

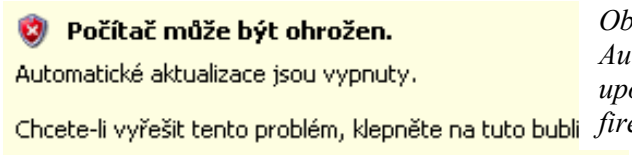
Při zkopírování souboru na jednotku naformátovanou systémem souborů FAT je kopie souboru rozšifrována [3]. Pro maximální ochranu dat je proto vhodné všechny svazky naformátovat systémem souborů NTFS.

4.3 Centrum zabezpečení Windows XP

Centrum zabezpečení je nástroj pro zjednodušení správy ochrany operačního systému Windows XP, který byl implementován v opravném balíčku Service Pack 2.

Obrázek č. 18 : Centrum zabezpečení Windows XP

Pomocí centra zabezpečení je umožněna jednoduchá správa tří základních funkcí pro ochranu operačního systému. Jsou to: Brána firewall, Automatické aktualizace a Ochrana proti virům. Centrum zabezpečení u každé z těchto položek zobrazuje, zda jsou zapnuty či vypnuty, případně zda jsou jejich databáze aktuální (což se týká především Brány firewall a Antivirové ochrany). Pokud se uživatel rozhodne mít některou z těchto položek neaktivní, systém Windows ho bude upozorňovat na nedostatečnou ochranu v oznamovací oblasti v pravém dolním rohu obrazovky.



Obrázek č. 19: Upozornění na absenci Automatických aktualizací (analogické upozornění se zobrazuje při absenci brány firewall či antivirové ochrany).

4.3.1 Automatické aktualizace

Každý operační systém obsahuje při uvedení na veřejnost určité chyby. Různá rizika se dále objevují postupem času, někteří lidé se totiž snaží nalézt mezery v ochraně počítačů a tyto mezery zneužít. Firma Microsoft proto systém Windows XP stále zdokonaluje, opravuje a tyto opravy a zdokonalení šíří mezi uživatele. K šíření těchto oprav (aktualizací) slouží právě nástroj Automatické aktualizace. Základním předpokladem k instalaci automatických aktualizací je připojení do sítě Internet, což je dnes však prakticky samozřejmostí. Nejvíce rizik, kvůli kterým jsou aktualizace vůbec vznikají, jsou navíc s používáním internetového připojení spojeny. Existuje několik možností, jak operační systém udržovat v aktualizovaném stavu, ze kterých má uživatel na výběr:

- **Automaticky (doporučeno firmou Microsoft)** – Aktualizace jsou automaticky staženy a v uživatelem zvolenou dobu vždy automaticky nainstalovány
- **Stahovat aktualizace, ale umožnit volbu doby jejich instalace**[2] – Systém Windows ověřuje, zda je k dispozici nová aktualizace a pokud ano, sám ji stáhne. Na stažení aktualizace upozorní uživatele ikonou v oznamovací oblasti a uživatel se sám rozhodne, kdy aktualizaci nainstaluje.
- **Oznamovat, ale aktualizace automaticky nestahovat ani neinstalovat**[2] – Systém Windows stejně jako u předchozí možnosti upozorňuje, že jsou k dispozici nové aktualizace, opět ikonou v oznamovací oblasti. Pokud se uživatel rozhodne aktualizaci nainstalovat, dá systému pokyn klepnutím na ikonu a systém stáhne aktualizaci na pozadí. Po dokončení stahování systém uživatele upozorní, že aktualizace byla stažena a uživatel může dát systému pokyn k instalaci.
- **Vypnout aktualizace** – Systém Windows nebude na nové aktualizace upozorňovat. Pokud se uživatel rozhodne vyhledat nové aktualizace, může tak učinit na internetových stránkách podpory firmy Microsoft. Tuto možnost nelze doporučit.

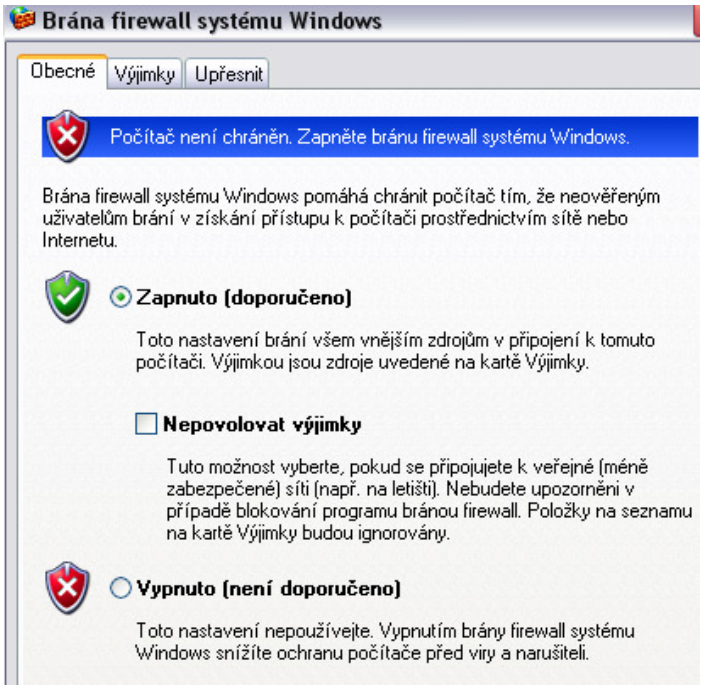
[2] Přijímat oznámení o dostupnosti nových aktualizací nebo aktualizace ručně stahovat a instalovat mohou pouze členové skupiny Administrators [4].

4.3.2 Brána firewall

Brána firewall je nástrojem pro filtrování přístupu do systému pomocí síťového rozhraní. Dá se říci, že podle určitých kritérií rozlišuje data vyžádaná a nevyžádaná a na základě tohoto rozlišení některá propouští a jiná blokuje. Poskytuje ochranu proti uživatelům, kteří by se mohli pokusit o přístup k počítači z prostoru vně systému Windows bez povolení uživatele [15].

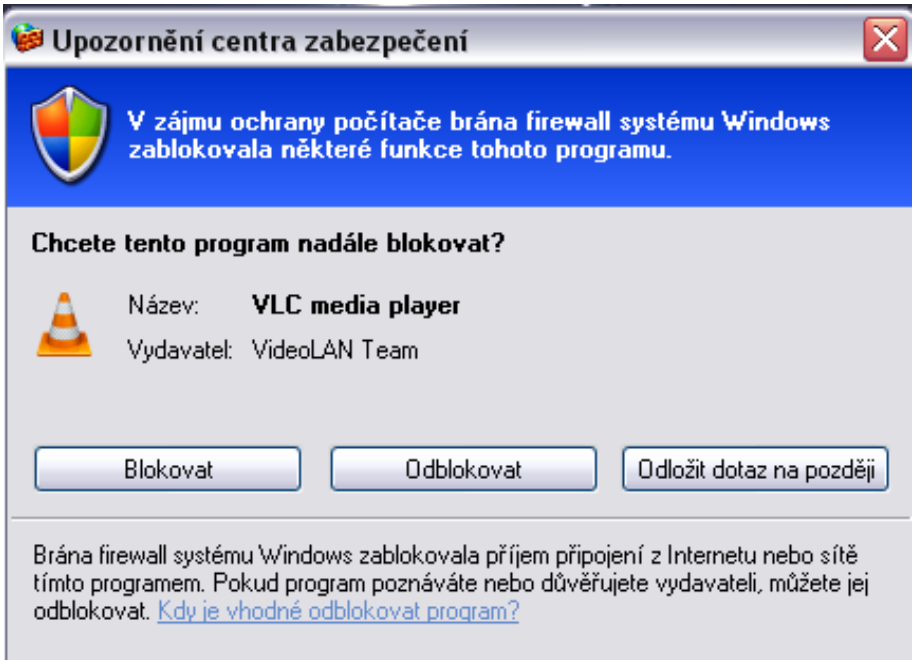
Společně s Centrem zabezpečení obsahuje balíček Service Pack 2 i Bránu firewall systému Windows (dříve nazývanou Brána firewall pro připojení k Internetu [15]). Na tomto místě se práce pokusí vysvětlit základní princip fungování Brány firewall systému Windows. Dle společnosti Microsoft poskytuje Brána firewall tyto funkce [15]:

- Blokování přijetí počítačových virů a červů do počítače.
- Vyžádání povolení blokovat nebo zrušit blokování určitých požadavků na připojení.
- Vytvoření volitelného záznamu (protokolu zabezpečení), do kterého jsou zaznamenávány úspěšné a neúspěšné pokusy o připojení k počítači.



Obrázek č. 20: Uživatelské rozhraní Brány firewall systému Windows

Brána firewall pracuje na následujícím principu. V případě zaznamenání pokusu o komunikaci pomocí síťového rozhraní (ať už mezí místními servery či do sítě Internet) ji automaticky zablokuje a dotáže se uživatele pomocí dialogového okna, zda má komunikaci povolit či nadále blokovat. Dialogové okno s dotazem je vidět na následujícím obrázku.



Obrázek č. 21 : Dialogové okno Brány firewall systému Windows dotazující se uživatele, zda blokovat či povolit síťovou komunikaci pro danou aplikaci.

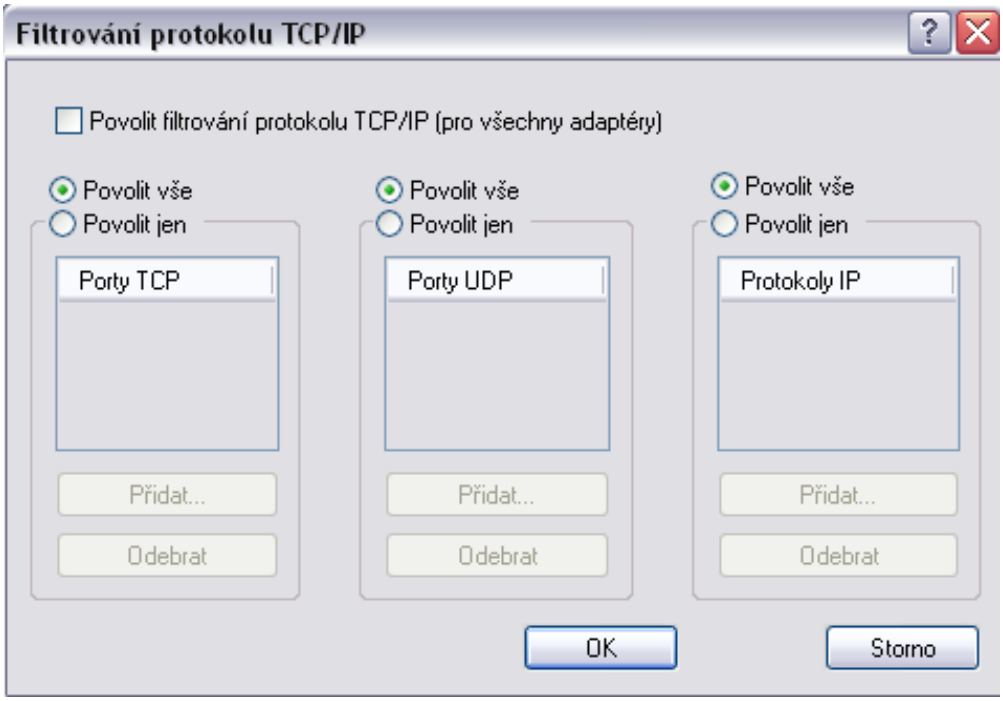
Pokud se uživatel rozhodne komunikaci pro danou aplikaci povolit, je komunikace této aplikace na portu, který byl použit, automaticky zařazena do seznamu tzv. výjimek. Tento seznam slouží k určení aplikací, pro které bude komunikace vždy povolena. Seznam výjimek tedy obsahuje možnost nastavit pro jakou aplikaci bude komunikace automaticky povolena, jakým protokolem a na jakém portu může komunikace probíhat.

Brána firewall umí pracovat i s více síťovými připojeními najednou. U každého je možné nastavit, jaké služby či protokoly mohou uživatelé libovolně využívat, případně s jakými počítači v síti může daná služba či protokol komunikovat.

Další možností, kterou Brána firewall systému Windows nabízí, je protokolování záznamů. To je možné nastavit v kartě *Upřesnit*. Je možné zvolit do jakého souboru

bude protokol ukládat, zda budou protokolována zablokovaná či povolená připojení a maximální velikost souboru s protokolem. Pokud by velikost protokolu měla překročit zadanou velikost, starší záznamy budou automaticky smazány.

Jak již bylo zmíněno, Brána firewall systému Windows XP umožňuje povolit síťovou komunikaci jednotlivým aplikacím a přiřadit jim port nebo rozsah portů, na kterých je síťová komunikace daným protokolem umožněna. Brána firewall však nemusí zachytit všechny pokusy o útok přes síťové rozhraní, je proto vhodné ponechat otevřené pouze ty porty, které jsou pro vyžádanou komunikaci nezbytně potřebné a zbývající porty pro daný protokol uzavřít. Uzavření portů je možné provést v nastavení protokolu TCP/IP daného síťového připojení. Zde je na výběr ze dvou možností: *povolit vše*, což povolí komunikaci na všech portech pro daný protokol a *povolit jen*, což zablokuje všechny porty kromě zadaných.



Obrázek č. 22: Nastavení filtrování na základě čísel portů pro jednotlivé protokoly

Uživatel nemusí používat pro ochranu komunikace pouze Bránu firewall systému Windows. V kombinací s ní může využívat i brány firewall jiných výrobců, případně Bránu firewall systému Windows zcela nahradit jinou bránou. I v případě využívání jiné

brány Centrum zabezpečení stále dokáže monitorovat, zda je brána firewall aktivní. Na trhu je v současné době celá řada firewallů různých výrobců. Jedním z možných firewallů jiných výrobců je Sunbelt Personal Firewall (dříve Kerio Personal Firewall) vyvíjený firmou Sunbelt, (poslední verze 4.5.916 z května roku 2007 [9]), jehož zjednodušená verze je k dispozici zdarma. Tento firewall oproti standardnímu firewallu systému Windows nabízí řadu rozšířených možností, například blokování jednotlivých portů nezávisle na aplikaci, která je využívá.

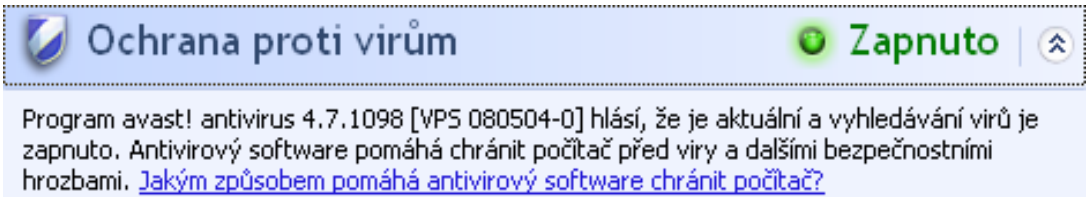
Obrázek č. 23: Grafické rozhraní brány Kerio Personal Firewall verze 4

4.3.3 Ochrana proti virům

Antivirový software slouží k obraně počítače před škodlivým softwarem, který se do počítače dostává převážně pomocí síťového rozhraní. Přestože brána firewall blokuje nevyžádanou komunikaci, viry a jiný škodlivý software dokáží bránu často obejít, případně se mohou do systému dostat současně s vyžádanými daty.

Centrum zabezpečení dokáže monitorovat chod a aktualizace antivirových programů, systém Windows XP však sám o sobě žádný antivirový software nenabízí. Je proto nutné využívat antivirovou ochranu jiného výrobce.

V současné době je na síti Internet volně ke stažení mnoho antivirových programů zdarma, případně je některé placené antivirové programy možné využívat k nekomerčním účelům bez placení za licenci. Seznam některých antivirů, které je možné využívat zdarma, je možné nalézt zde [16].



Obrázek č. 24: Centrum zabezpečení monitoruje chod a aktualizaci antivirového softwaru

4.4 Další funkce zabezpečení Windows XP

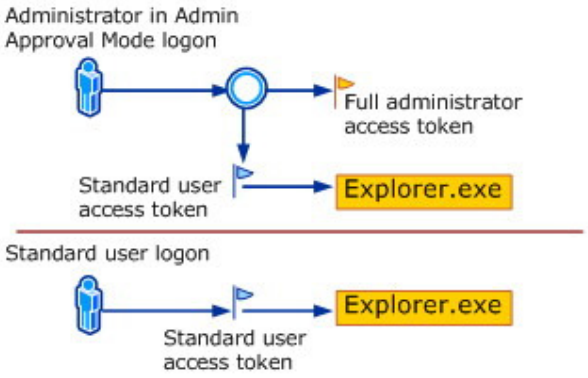
Systém Windows XP nabízí kromě výše uvedených možností zabezpečení mnoho dalších. Běžní uživatelé systému Windows nejčastěji využijí ochranu soukromí a blokování závadného obsahu internetových stránek, ochranu elektronické pošty, ochranu sdíleného připojení do sítě Internet nebo nástroj pro automatické zálohování dat. Především pro správce systému je naopak určena možnost auditování událostí v systému či rozšířené zabezpečení síťových připojení realizovaných pomocí jiných protokolů, než je nejpoužívanější protokol TCP/IP.

5 Změny zabezpečení v systému Windows Vista

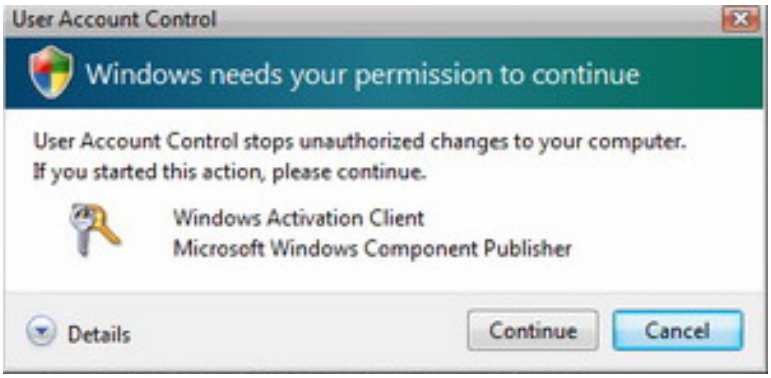
Operační systém Windows Vista se vyznačuje mnohem robustnějším zabezpečením, než předchozí operační systémy Windows. Některé funkce jsou nové, zatímco jiné rozšiřují ochrany, které již byly k dispozici v předchozích verzích systému Windows. [18]

Novinkami v zabezpečení jsou mimo jiné:

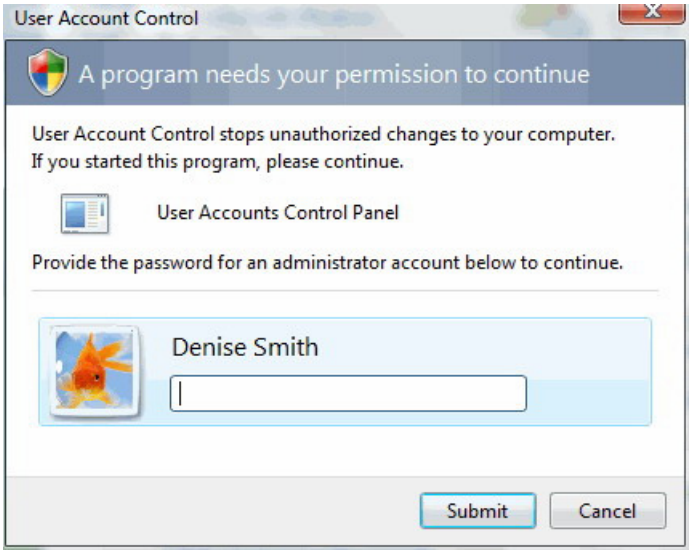
- **Restriktivní instalace -** V předchozích verzích operačního systému Windows mohly nebezpečné programy provádět stahování a instalace bez vědomí uživatele. Při každém pokusu o instalaci softwaru v operačním systému Vista je uživatel vyzván, aby instalaci potvrdil. [18]
- **Kontrola uživatelského účtu** - Funkce, která způsobuje, že každý uživatel - bez ohledu na jeho administrátorská práva - automaticky pracuje v modu běžného uživatele. V případě administrátorských akcí systém vyžaduje potvrzení. Princip této funkce je následující. V okamžiku, kdy se uživatel ze skupiny Administrators přihlásí k systému, rozdělí Windows jeho oprávnění na dvě části („tokeny“). Ty obsahují informace o členství účtu ve skupině, jeho autorizaci a o řízení povolení přístupu. Systém podle nich určuje, ke kterým zdrojům a úlohám přístup uživateli povolí. Uživatel standardně pracuje pouze s částí práv „standardního uživatele“, zatímco administrátorská část oprávnění je deaktivována.Standardní uživatelská práva Windows použijí ke spuštění Plochy a Průzkumníka. Protože všechny aplikace dědí přístupová práva od Plochy, budou rovněž spouštěny pouze s uživatelskými oprávněními. Administrátorská práva se pro uživatele aktivují až ve chvíli, kdy k tomu dá souhlas. Pokud však je k systému přihlášen uživatel bez administrátorských oprávnění, systém bude požadovat potvrzení jeho prověření, tedy zadání hesla k některému účtu skupiny Administrators. V *Editoru systémových politik* je možné nastavit, aby systém vyžadoval zadání hesla i po správcích. Microsoft nechal plně na správcích systému, zda budou *kontrolu uživatelských účtů* používat. Vypnutí je možné, je k němu však potřeba editovat nastavení systémových politik. [19]



Obrázek č. 25: Přihlášení administrátora a uživatele: práva Administrátora se rozdělí na administrátorskou a uživatelskou část [19]



Obrázek č. 26 : Dialogové okno vyžadující od správce potvrzení pro další krok [19]



Obrázek č. 27: Dialogové okno vyžadující od uživatelepřístupové heslo k účtu správce [19]

- **Vylepšená brána firewall** — Brány firewall předchozích verzí systémů Windows kontrolovaly pouze příchozí provoz. V operačním systému Vista je možné nakonfigurovat bránu firewall tak, aby řídila také odchozí provoz. [18]
- **Vylepšené šifrování souborů** – Umožňuje snadno chránit data na přenosných paměťových médiích či přenosných počítačích. [20]
- **Rodičovská kontrola** – má několik součástí - **Webový filtr**, sloužící k omezení přístupu na určité webové stránky, **Časové limity**, sloužící k omezení času přihlášení uživatele, **Hry**, sloužící k zablokování spuštění některých her podle hodnocení nebo podle názvu, a **Blokování programů.** Všechny tyto možnosti je možné protokolovat. [21]
- **Windows Defender** – Nástroj umožňující automatické stahování aktualizací a skenování na pozadí. Dokáže detekovat a odstranit nebezpečné programy a upozornit, pokud se některý pokusí vytvářet změny v chráněných oblastech systému. Dále umožňuje naplánovat automatické skenování systému na určitý čas. Stále však nenahrazuje antivirus. [21]

6 Závěr

Na počátku devadesátých let minulého století, kdy se počítače začaly rozšiřovat i do domácností, existovalo velmi malé množství rizik narušení bezpečnosti operačních systémů. Tehdejší operační systémy nepřinášely téměř žádnou nebo velmi nízkou úroveň zabezpečení, která však byla postačující. Vždy se však najdou lidé, kteří se snaží nalézt způsob, jak bezpečnost systému narušit a toto zneužití využít ve svůj prospěch. S rostoucím počtem rizik bylo nutné postupně zvyšovat i úroveň zabezpečení až do té míry, jaké dosahuje v současné době.

Operační systém Windows XP ve verzi Professional přináší velmi komplexní systém zabezpečení. Jednotlivé aspekty jeho zabezpečení jsou velmi kvalitní při zachování jednoduchosti a využitelnosti i pro méně zkušené uživatele. Pro zajištění bezpečnosti je však třeba dodržet celkovou ochranu počítače ve všech úrovních.

Pokud se počítače, a tedy i operační systémy, budou nadále rozšiřovat do všech oborů lidské činnosti, což je vysoce pravděpodobné, bude stoupat i počet rizik a možností narušení jejich bezpečnosti. Poroste tedy i úroveň zabezpečení, nejdůležitější součásti této bezpečnosti však je a nadále bude informovanost uživatelů, jejich svědomitost, opatrnost a ochota učit se.

7 Seznam literatury

1. EISENKOLB, Kerstin - GÖKHAN, Mehmet - WEICKARDT, Helge. *Bezpečnost Windows 2000/XP*., 1. vyd., Praha: Computer Press, 2003. 516 stran, ISBN: 80-7226-789-2
2. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Praha: Computer Press, 2004, 200 stran. ISBN: 80-2510-106-1.
3. BOTT, Edd - SIECHERT, Carl. *Mistrovství v zabezpečení Microsoft Windows 2000 a XP*. Praha: Computer Press, 2004. 696 stran. ISBN: 80-7226-878-3.
4. SZOR, Peter. *Počítačové viry - analýza útoku a obrana*. Zoner Press, 2006. 608 stran. ISBN: 80-8681-504-8.
5. *Stručný úvod do kryptografie*-[online], [cit. 2008-03-25], URL:<http://krypto.krokonet.com/>
6. *Tipy a triky ve Windows XP* – [online], poslední úpravy 28. 4. 2007 URL: <http://www.pc-help.cz/viewtopic.php?t=6752>
7. *Wikipedia.org – Operating system - security* – [online], poslední úpravy 5. 5. 2008 URL: <http://en.wikipedia.org/wiki/Operating_system#Security>
8. *Vytvoření silných hesel* – [online], [cit. 2008-03-22] URL:<http://www.microsoft.com/cze/mojefirma/themes/techwise/effectivepassword.mspx>
9. *Sunbelt-software* – [online], [cit. 2008-04-01] URL: <http://www.sunbelt.cz/>
10. *Jak zakázat zjednodušené sdílení a nastavit oprávnění u sdílené složky v systému Windows XP* – [online] poslední úpravy 01.12.2007, revize 3.2, URL: <http://support.microsoft.com/kb/307874/cs>
11. PŘIBYL, J. - *1. Přednáška – Informační bezpečnost a přehled kryptologie* – [online], [cit. 2008-04-11], URL: <www.comtel.cz/files/download.php?id=3195>
12. *NTFS – Wikipedie, otevřená encyklopedie* – [online], poslední úpravy 2.4.2008 URL: <http://cs.wikipedia.org/wiki/NTFS>
13. *AdminXP.cz: Encrypting File System (EFS)* – [online], [cit. 2008-03-29] URL: <http://www.adminxp.cz/windowsxp/index.php?aid=114>
14. *Doporučené postupy šifrování systému souborů* – [online], Poslední úpravy 26. října 2007, Revize 12.2, URL: <http://support.microsoft.com/kb/223316/cs>
15. *Principy Brány firewall systému Windows v systému Windows XP s aktualizací Service Pack 2* – [online], Publikováno 1. září 2004, [cit. 2008-04-18] URL:<http://www.microsoft.com/cze/windows/xp/using/security/internet/sp2_wfintro.mspx>
16. *Antiviry, antivirové programy – Zdarma.org* – [online] URL: <http://www.zdarma.org/?s=antiviry-antivirove-programy>
17. *Sada protokolů Internetu - Wikipedie, otevřená encyklopedie* – [online], poslední úpravy 31. 3. 2008 URL:<http://cs.wikipedia.org/wiki/Sada_protokol%C5%AF_Internetu>
18. *Zabezpečení operačního systému Windows Vista* – [online], 01.03.2007, [cit. 2008-04-06], URL:<http://www.symantec.com/cs/cz/norton/library/article.jsp?aid=article1_03_07>
19. WAIC, Vlastimil - *Pohled do Windows Vista: Kontrola uživatelského účtu* – [online], poslední úpravy 21. 7. 2006, [cit. 2008-04-06] URL:<http://www.zive.cz/default.aspx?article=131315>
20. *Windows Vista - Wikipedie, otevřená encyklopedie* – [online], poslední úpravy 19.03.2008, URL:<http://cs.wikipedia.org/wiki/Windows_Vista#Dal.C5.A1.C3.AD_novinky>
21. BUDAI, David - *Bezpečnost Windows Vista v kostce I.* – [online], 25. 6. 2007, [cit. 2008-04-08], URL:<http://www.zive.cz/default.aspx?textart=1&article=136775>
22. *Cs.wikipedia.org – počítačový virus* – [online], poslední úpravy 07.04.2008, URL: < http://cs.wikipedia.org/wiki/Počítačový_virus>
23. *TrackIT Anti-Theft Alarm – Archived Article*, [cit. 2007-12-19], URL:<http://europeforvisitors.com/europe/articles/trackit_antitheft_alarm.htm>
24. *Přístup domácností a jednotlivců k vybraným informačním technologiím*, [cit. 2008-03-25] URL:< http://www.czso.cz/csu/2007edicniplan.nsf/t/70002633A9/$File/970107k1-CZ.pdf>
25. *CSUCI > Information Technology - How to Logon to the Computer Labs,* [cit. 2008-04-11], URL: <http://www.csuci.edu/it/computerlablogon.htm>

8 Seznam obrázků