GRADA

Bezpečnost malých počítačových sítí

(praktické rady a návody)

Jaroslav Horák

PODROBNÝ PRŮVODCE
ZAČÍNAJÍCÍHO UŽIVATELE

Ochrana dat před jinými osobami

Ohrožení dat v lokální síti a z internetu

Microsoft Baseline Security Analyzer

Encrypting File System

Upozornění pro čtenáře a uživatele této knihy

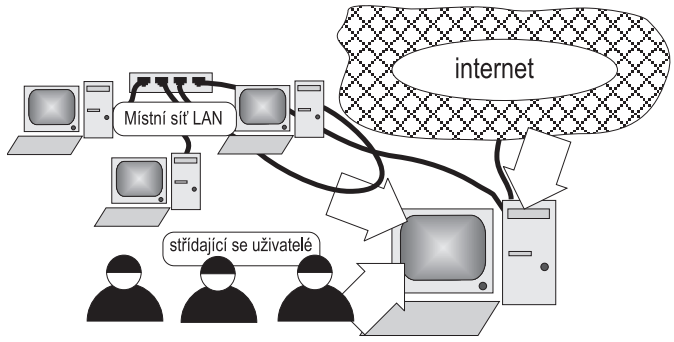
Obsah

Úvod

Úvod

Počítačovou síť dnes najdeme téměř v každé firmě, neobvyklá není ani v domácnostech. Hardwarové a softwarové konstrukci počítačových sítí jsem věnoval knihu *Malá počítačová síť doma a ve firmě*. Kniha, jejíž úvod právě čtete, představuje její volné pokračování. Je věnována ochraně dat v síti. (Bezpečnostní vlastnosti starších verzí *Windows* jsou chabé, navíc tyto operační systémy v současnosti dosluhují. Proto najdete v této knize popisy konfigurace *Windows XP* a *Windows 2000*.) Problematiku ochrany dat jsem rozdělil do čtyř hlavních oblastí, které se kryjí s možnými variantami průniku k našim datům. Nebezpečí hrozí od:

- jiného uživatele, který používá můj počítač,
- jiného uživatele, který přistupuje k mému počítači z lokální sítě,
- jiného uživatele, který přistupuje k mému počítači z vnější sítě (z internetu),
- programu, který se do mého počítače dostane z internetu (například bezpečnostní dírou) a může se v něm spustit.



Možnost průniku do PC

Jednotlivé kapitoly knihy však nelze číst odděleně, protože bezpečnostní rizika (a nastavení, která je snižují) jsou většinou obecná a platí pro několik variant možného průniku (ke sdílené složce se dostaneme stejným způsobem z lokální sítě, z internetu, pravidla pro práci s heslem jsou obecná atd.).

V první kapitole, nazvané *Ochrana dat před jiným uživatelem počítače*, jsou popsány základy víceuživatelského charakteru dnešních *Windows* – uživatelský profil a účet. Na toto téma navazuje popis zásad práce s účty a hesly (například objasníme pojem „silné heslo“). S tím úzce souvisí vysvětlení práce se skupinami uživatelů. Dále se budeme věnovat popisu potenciálně nebezpečných prvků *Windows*: Auto Logon a Guest. Jejich nastavení občas musíme provést v systémové registrační databázi, setkáme se tedy s programem *Regedit* a některými příkazy na příkazovém řádku. Obecné zásady pro práci s hesly a účty (konzola MMC Zásady skupiny) proto budou dalším tématem první kapitoly. Ve druhé části pak shrneme pravidla pro sdílení souborů mezi uživateli jednoho počítače.

První část knihy je velmi důležitá, protože popisuje základní bezpečnostní vlastnosti, s nimiž se budeme setkávat i v následujících kapitolách knihy.

Nosnou částí druhé kapitoly *Ochrana dat před přístupem z lokální sítě* je práce s oprávněními (jimiž se přístup ke složkám řídí). V této činnosti se jednotlivé verze *Windows* liší, proto je popis věnován jak *Windows XP Home*, tak *Windows XP Professional* a *2000*. Bezpečnost práce ovlivňují nejen oprávnění, následující část je proto věnována dalším potenciálním rizikům: anonymnímu přihlášení (Anonymous) a vzdálenému přístupu k *Windows XP*.

Třetí kapitola *Windows Update* vysvětluje obranu před nebezpečím, které hrozí našemu systému z internetu. Při práci s internetem probíhá uvnitř operačního systému mnoho akcí, vyvolaných internetovým serverem, který jsme navštívili. Ty mohou být zneužity (například počítačovými viry). Proto je nutné systém pravidelně kontrolovat a nově objevená nebezpečí eliminovat. K tomu je určen systém *Windows Update*. Dozvíme se, jak s *Windows Update* pracovat, jak nastavit automatické aktualizace, jak *Windows Update* použít v síti. Bodem, přes které může být operační systém zneužit, je *Internet Explorer*. Zásady, jak zvýšit odolnost Exploreru, najdete v další části teto kapitoly.

Čtvrtá kapitola *Microsoft Baseline Security Analyzer (MBSA)* je věnována programu *MBSA*, který kontroluje bezpečnostní konfiguraci operačního systému. Popis *MBSA* je fakticky shrnutím znalostí z předchozího výkladu. Bude popsána kontrola místního počítače i počítačů síťových. Součástí *MBSA* je program *MBSACLI*, který kontroluje instalaci opravných balíčků (instalovaných *Windows Update*). Popisu práce s *MBSACLI* je věnována druhá část čtvrté kapitoly.

Předposlední, pátá kapitola *Ochrana před průnikem z vnější sítě*, objasňuje práci s firewallem. K ochraně sítě před zneužitím z internetu je nezbytné pochopit základní principy práce protokolů *TCP/IP*, vědět, co jsou porty, porozumět funkci sdíleného připojení k internetu a principu práce služby NAT. To vše najdete v první části poslední kapitoly knihy. Dále budeme pokračovat popisem práce a nastavování jednoduchého firewallu, který najdeme ve *Windows XP*. Řekneme si něco o povolování služeb, omezování funkcí protokolu ICMP a filtrování paketů. Nakonec si předvedeme ještě dva programy, určené pro práci s firewallem. Jde o program *PortQuery*, který nás informuje o stavu portů *TCP/IP*, a řádkový příkaz *Netstat*. Ten je schopen vypsat seznam právě probíhajících spojení mezi operačním systémem a vzdálenými počítači.

Poslední kapitola EFS (Encrypting File System) pojednává o šifrování dat systémem EFS. Tento systém je součástí operačního systému a zvyšuje stupeň ochrany dat. V kapitole bude vysvětlen princip kódování, praktická práce při šifrování a dešifrování dat. Základem EFS jsou digitální certifikáty, bez nichž celý systém EFS nefunguje. Proto je exportu a importu certifikátů věnována další část kapitoly. Na závěr je zařazen popis práce s agenty obnovení dat.

Na závěr knihy jsem ještě připojil stručný přehled činností, vysvětlovaných v jednotlivých kapitolách. Čtenář tedy má k dispozici pomůcku pro urychlení praktické práce.

Závěrem těchto úvodních poznámek bych rád upozornil na důležitý fakt, který je nutné vždy respektovat. Každé zvýšení bezpečnosti je založeno na restrikci – tedy na snížení funkčnosti systému. Proto je nutné po jakékoliv změně konfigurace otestovat funkčnost systému! (K čemu je nám platné, že se do složky nedostane nikdo nepovolaný, když se tam nedostane ani náš šéf, který zde ještě včera pracoval. Nikdo neocení ani to, že jsme zabezpečili přístup z internetu, když přestala fungovat pošta, atd.)

Použité konvence

V knize jsou pro usnadnění orientace v textu použity následující typografické prvky:

- **Tučným písmem** jsou vysázeny názvy nabídek, příkazů a ovládacích prvků dialogových oken. Uvidíte-li tedy zápis „zadejte příkaz **Soubor → Otevřít**“, znamená to, že musíte klepnout v nabídce **Soubor** na položku **Otevřít**.
- *Kurzivou* jsou zvýrazněny názvy softwaru.
- KAPITÁLKY slouží k popisu kláves a klávesových zkratek, jako například CTRL+ALT+DEL.

V textu se také setkáte s odstavci, označenými ikonou, která bude charakterizovat druh informace, obsažené v daném odstavci.

Tato ikona označuje poznámku, která není nezbytná k pochopení dané problematiky, ale týká se tématu a prozrazuje další souvislosti.

Pokud uvidíte takovéto vítězné gesto, můžete si být jisti, že je nablízku nějaký tip nebo trik, pomocí něhož si můžete usnadnit práci, případně snadno dosáhnout efektivně svého cíle.

Varovně vztyčený prst označuje text, který vás upozorňuje na něco, na co byste si měli dát pozor, co vás může nepříjemně překvapit nebo co by vám mohlo způsobit problémy.

Ochrana dat před jiným uživatelem

1. Ochrana dat před jiným uživatelem

V první kapitole se zamyslíme nad možnostmi, jak chránit svoje data před uživateli, střídajícími se s námi u počítače. Většina zde uvedených skutečností platí obecně a budeme se s nimi setkávat i v dalších částech knihy. Nebudu se zabývat podrobným popisem konfigurace *Windows*, ten najdete například v knize *Malá počítačová síť doma a ve firmě*.

1.1 Víceuživatelská práce ve Windows

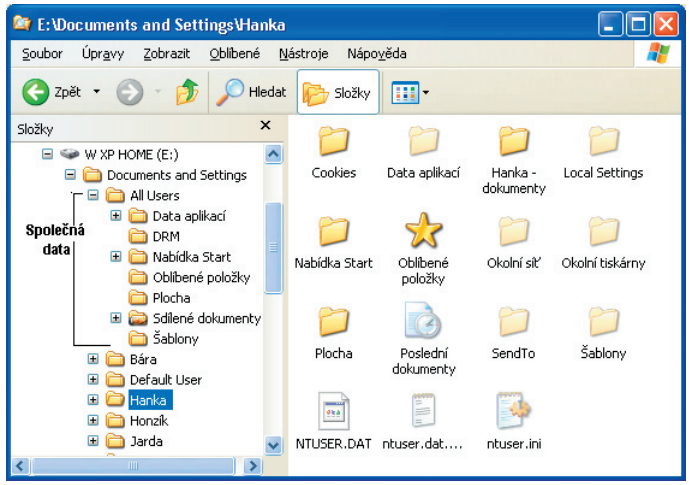
U jednoho počítače se může střídat více uživatelů, ale možnost utajení dat jednotlivých uživatelů závisí na vlastnostech operačního systému:

- *Windows 95*, *98* a *Millennium* nejsou víceuživatelskými systémy, data uložená jedním uživatelem jsou přístupná všem. Víceuživatelská ochrana dat zde možná není (a dále proto nemá v této knize o těchto operačních systémech smysl hovořit).
- *Windows 2000* a *XP* umožňují skrýt data jednoho uživatele před druhým, právě jim se tedy budeme věnovat.

1.2 Uživatelský profil a účet

Uživatelský profil

Základem práce více uživatelů v těchto operačních systémech je *uživatelský profil* a s ním související *uživatelské účty*. Každý, kdo bude v systému pracovat, má k dispozici vlastní soustavu složek – uživatelský profil. Jednotlivé uživatelské profily jsou uloženy ve složce **Documents and Settings**. Najdeme zde data, typická pro každého uživatele. Důležité je, že složky profilu nejsou přístupné ostatním uživatelům počítače (s výjimkou uživatele s oprávněním správce počítače, ale i před ním je možné složky ochránit).



1.1 Uživatelský profil uživatele Hanka

Všimněme si následujících složek:

- **Uživatel – Dokumenty** je určitě nejpoužívanější složkou, určenou pro data uživatele. Ukládání na toto místo mají přednastaveno všechny programy.
- Nabídka **Start** je určena pro programy, zobrazované v nabídce **Start** konkrétního uživatele. Nabídka **Start** má dvě části: osobní a společnou. (Konfiguraci společné nabídky **Start** najdeme ve společném profilu – **Documents and Settings\All Users\Nabídka Start**).
- Do složky **Oblíbené položky** se zapisuje nastavení oblíbených položek uživatele (například z *Internet Exploreru*).
- Ve složce **Plocha** jsou zaznamenány všechny objekty, zobrazované na ploše uživatele (každý má tedy svoji plochu).
- Ve složce **Cookies** jsou uloženy soubory cookie (je o nich řeč ve třetí kapitole, kde jim je věnována zvláštní podkapitola).
- Ve složce **Data aplikací** najdeme datové soubory aplikací (například adresář a soubory *Outlook Expressu*, nastavení programů *Office* atd.)

Windows automaticky vytvářejí společný profil (přístupný všem uživatelům), nazvaný **All Users**. Jeho struktura je stejná jako u jiných profilů, ale složka určená pro data se jmenuje **Sdílené dokumenty**. Je přístupná všem a je vhodné ji používat k výměně dat (týká se i uživatelů, kteří používají počítač ze sítě).

Složky profilu založí operační systém automaticky, a to při prvním přihlášení uživatele k systému.

Uživatelský účet

Víceuživatelské *Windows* si vedou databázi uživatelů. V jedné položce databáze – v *uživatelském účtu* – jsou zapsány základní údaje o každém uživateli (jeho přihlašovací jméno a heslo, oprávnění pro práci se složkami a tiskárnami, práva ke správě dalších účtů atd.). Účet je základním bezpečnostním prvkem operačního systému, proto je jeho konfiguraci nutné věnovat náležitou pozornost.

S uživatelskými účty úzce souvisí *skupiny.* Do skupin je možné sdružovat *uživatelské účty*. Účty ve skupině pak mají stejná práva. Ve *Windows* jsou některé skupiny (s předem definovanými právy) již vytvořeny, což nám správu účtů usnadňuje – přiřazením účtu ke skupině jsou účtu přiděleny vlastnosti skupiny (a my je již nemusíme definovat).

Práce s účty a skupinami ve Windows 2000

Během instalace *Windows 2000* se vytvoří dva účty:

- **Administrator** je účtem určeným pro správu počítače, přidělování oprávnění a podobně. S jeho pomocí budeme postupně vytvářet další účty.
- **Guest** je účtem pro příležitostné uživatele systému. Ve výchozím stavu je tento účet sice zřízen, ale zároveň zakázán. Je na administrátorovi, zda jej umožní používat a co uživatelům tohoto účtu povolí. Z hlediska bezpečnosti je tento účet velmi nevhodný, proto mu je věnována zvláštní podkapitola (jmenuje se *Zesílení ochrany uživatelských účtů*).

Také jsou vytvořeny následující předdefinované skupiny:

- Skupina administrátorů, **Administrators**: vlastníci účtů zařazených do této skupiny mají maximální práva ke správě *Windows*.
- Skupina **Backup Operators** sdružuje majitele účtů, kteří mohou zálohovat a obnovovat soubory prostřednictvím programu *Microsoft Backup*.
- Skupina uživatelů se standardním oprávněním, **Power Users**, může provádět všechny běžné činnosti: instalovat a spouštět programy, měnit nastavení počítače, nemůže však pracovat s daty ostatních uživatelů. Může ovšem také vytvářet nové účty.
- Skupina uživatelů s omezeným oprávněním, **Users**, může spouštět programy a pracovat s vlastními daty.
- Do skupiny **Everyone** patří všichni uživatelé, momentálně přihlášení k počítači. Je skupinou systémovou, účty do ní nepřidává administrátor, ale operační systém *Windows*. Z hlediska bezpečnosti představuje skupinu velmi problémovou. Musíme na ni myslet především při definici sdílení složek a při práci s účtem **Anonymous**.

Z dalšího textu postupně vyplyne, že pro běžnou práci je vhodné používat účet ze skupiny **Power Users** nebo **Users**. Administrátorský účet by neměl být obecně známý a při práci s ním je vhodné dodržovat určitá pravidla:

- Účtů ze skupiny **Administrator** by mělo být co nejméně.
- Měly by však existovat minimálně dva: kdyby jeden havaroval, bude k dispozici záložní účet.
- V dalším textu budu popisovat práci s účty a skupinami. Tu můžeme provádět pouze tehdy, pokud jsme přihlášeni pod administrátorským účtem. Pro běžnou práci však tento účet nepoužívejte!

Vytvoření účtu pomocí ovládacího panelu Uživatelé a hesla

Pro práci s účty je určen ovládací panel **Uživatelé a hesla** (**Start → Nastavení → Ovládací panely → Uživatelé a hesla**). Zde máme k dispozici tři tlačítka, můžeme tedy **Přidat** nebo **Odebrat** účet, případně změnit jeho **Vlastnosti**. Stiskem tlačítka **Přidat** zahájíme tvorbu nového účtu (skládá se z vyplnění údajů ve třech oknech průvodce). Do prvního okna napíšeme základní údaje o uživateli účtu:

- **Uživatelská jméno**, pod nímž se bude do systému *Windows 2000 Professional* hlásit.
- **Jméno a příjmení** vlastníka účtu.
- **Popis** obsahuje nepovinné doplňující údaje o účtu.

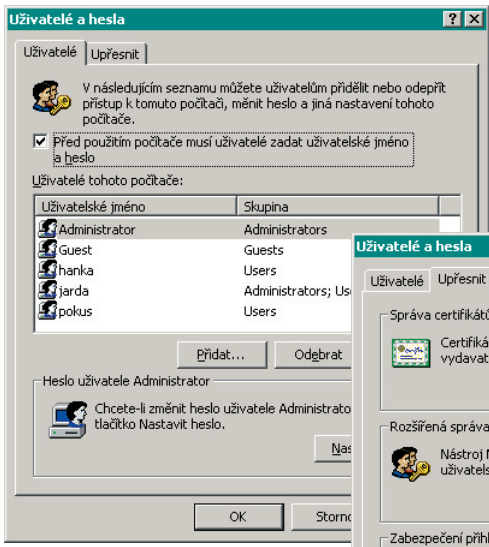
Pak přejdeme do druhého okna, v němž specifikujeme heslo (zadáváme jej do obou řádků). Ve třetím okně přiřadíme účet do některé ze skupin. Pokud chceme vytvořit další administrátorský účet, použijeme třetí řádek **jiná**.

Poklepáním na účet (nebo stiskem tlačítka **Vlastnosti**) máme k dispozici první a třetí okno průvodce – můžeme upravit identifikační údaje či zařazení do skupiny. Heslo změníme tlačítkem **Nastavit heslo** v pravém spodním rohu panelu **Uživatelé a hesla**.

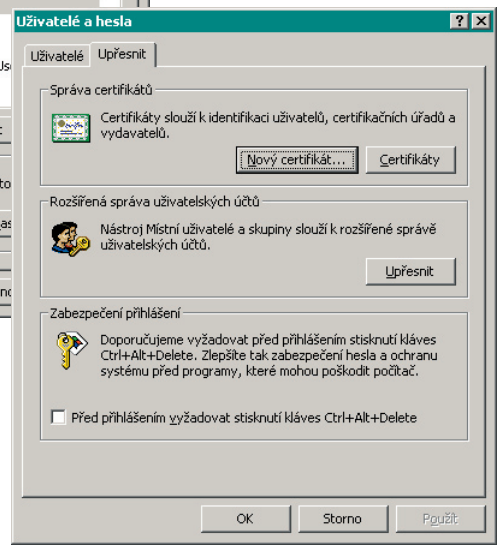
V ovládacím panelu najdeme některá nastavení, týkající se bezpečnosti během přihlašování k *Windows*:

- V horní části okna **Uživatelé a hesla** si všimněte zaškrtávacího políčka **Před použitím počítače musí uživatel zadat...** Pokud není vyplněno, bude přihlašování do *Windows* automatické, bez nutnosti zadávání jména a hesla (což porušuje základní bezpečnostní princip). Změnou hodnoty v políčku měníme hodnotu klíče **AutoAdminLogon**, což je popsáno na jiném místě v kapitole *Automatické přihlášení (Auto Logon)*.

- Přejdeme-li na kartu **Upřesnit**, uvidíme v její spodní části políčko **Před přihlašováním vyžadovat stisknutí kláves Ctrl+Alt+Del**. Přihlašovací obrazovka *Windows* se objeví až po stisku uvedené klávesové zkratky. Protože současný stisk těchto tří kláves se používá pro restart počítače, budou tímto způsobem oklamány některé virové programy.



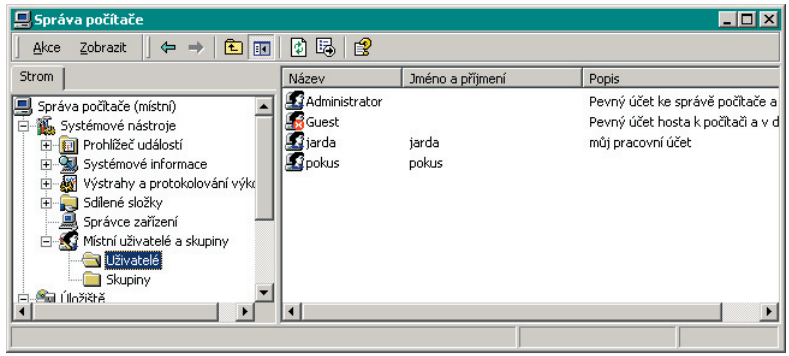
1.2 Ovlivnění automatického přihlášení



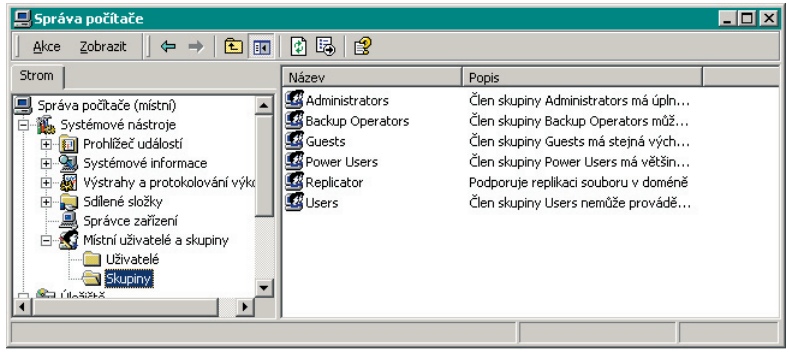
1.3 Ovlivnění stisku Ctrl+Alt+Del při přihlášení k Windows

Práce s účty prostřednictvím konzoly Správa počítače

Klepneme-li pravým tlačítkem myši na ikoně **Tento počítač** a z místní nabídky zadáme příkaz **Spravovat**, zobrazíme konzolu **Správa počítače**. Jedná se o konzolu MMC, jejímž prostřednictvím je možné ovládat *Windows 2000* a *XP*. Každá tato konzola má v levé části **strom konzoly**, v němž se nacházejí jednotlivé kategorie. Nás zajímají **Místní uživatelé a skupiny**. Klepnutím na znaménko + kategorii otevřeme a můžeme si prohlédnout její složky: **Uživatelé**



1.4 Uživatelské účty v konzole Správa počítače



1.5 Skupiny v konzole Správa počítače

a **Skupiny**. Dalším klepnutím přímo na složku zobrazíme v pravé části konzoly její obsah. Na rozdíl od práce s ovládacím panelem uvidíme v pravém okně všechny uživatele a skupiny.

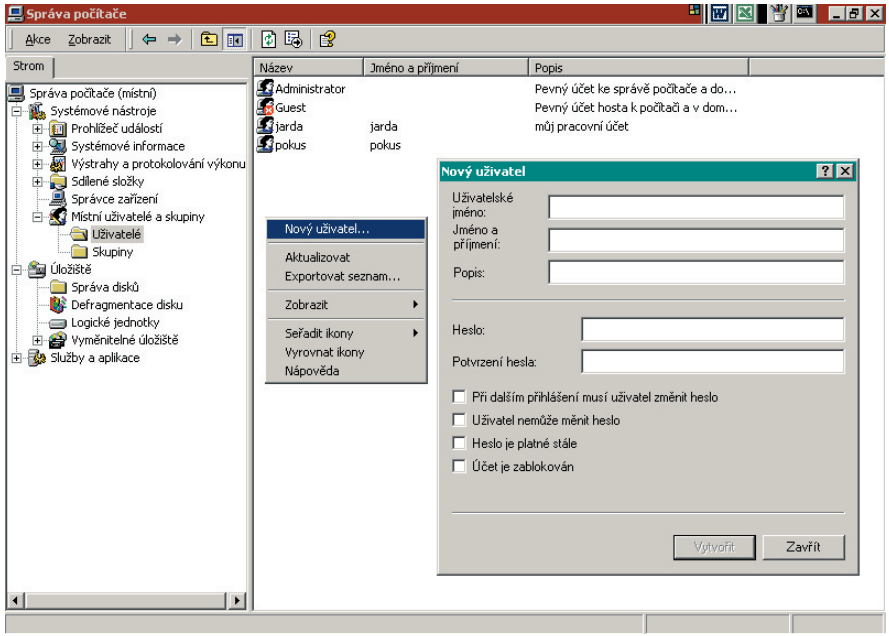
Uživatele i skupiny můžeme spravovat velmi jednoduše.

Založení uživatele

Klepněte pravým tlačítkem myši ve volném prostoru pravého okna konzoly a v zobrazené nabídce vyberte příkaz **Nový uživatel**. Význam příkazů v okně **Nový uživatel** je zřejmý (shoduje se s popisem v odstavci *Vytvoření účtu pomocí ovládacího panelu Uživatelé a hesla*).

V konzole **Správa počítače** však máme k dispozici další, rozšířené možnosti pro správu hesla:

- **Při dalším přihlášení musí uživatel změnit heslo**: zaškrtnutím přinutíme uživatele nastavit při dalším přihlášení k *Windows* nové heslo.
- **Uživatel nemůže měnit heslo**: uživatel nebude moci své heslo měnit.
- **Heslo je stále platné**: heslo může mít trvalou platnost, jinak je uživatel bude muset po určité době měnit.
- **Účet je zablokován**: pokud uživatel nebude s účtem delší dobu pracovat, je možné jej zablokovat. (Zablokovaný učet **Guest** vidíte na obrázku 1.4).



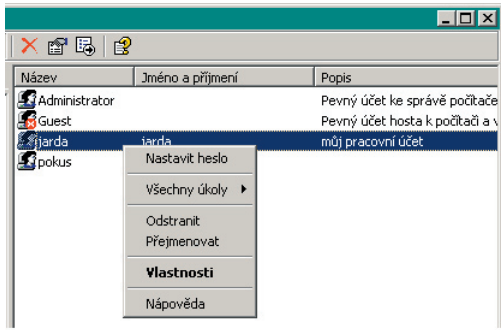
1.6 Tvorba účtu

Změna vlastností uživatele

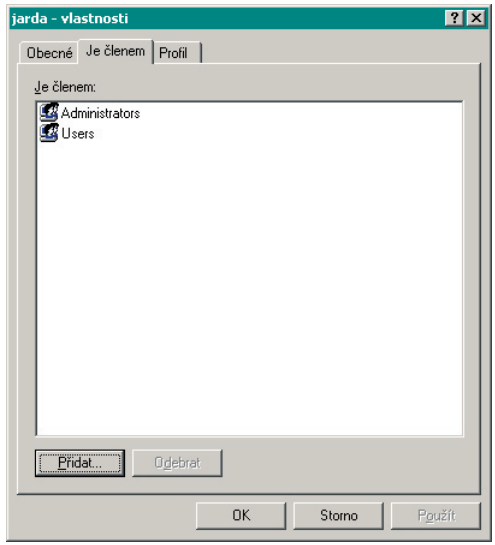
Vlastnosti existujícího účtu můžeme snadno měnit. Klepneme pravým tlačítkem myši na příslušném účtu a v nabídce uvidíme jednotlivé možnosti. Varianty **Nastavit heslo**, **Odstranit** a **Přejmenovat** nepotřebují další vysvětlení.

U položky **Vlastnosti** se ovšem ještě chvíli zdržíme. Zobrazí se okno, která má tři karty:

- Karta **Obecné** je podobná oknu **Založení uživatele**, můžeme zde měnit především možnosti hesla.
- Na kartě **Je členem** vidíme skupiny, do nichž je uživatel zařazen. Stiskem tlačítka **Přidat** zobrazíme existující skupiny, poklepáním na skupině pak uživatele do skupiny přiřadíme.



1.7 Nabídka pro práci s účtem



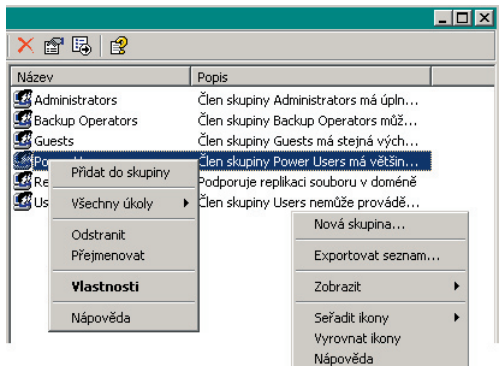
1.8 Karta Je členem

O bezpečnostních pravidlech a konfiguraci všeobecných zásad pro práci se jmény a hesly pojednává kapitola Zesílení ochrany uživatelských účtů.

Práce se skupinami prostřednictvím konzoly Správa počítače

V konzole **Správa počítače** (spustíme klepnutím pravým tlačítkem myši na ikoně **Tento počítač** a příkazem **Spravovat** z místní nabídky) otevřeme kategorii **Místní uživatelé a skupiny**. Přejdeme do složky **Skupiny**. V pravé části obrazovky vidíme všechny existující skupiny. Práce se skupinami je velmi podobná práci s účty:

- Klepnutí pravým tlačítkem myši v prázdné části okna otevře nabídku, v níž je nejdůležitější první řádek – **Nová skupina**. Pomocí tohoto řádku vytvoříme skupinu.
- Klepneme-li pravým tlačítkem myši na konkrétní skupině, spatříme téměř stejnou nabídku jako u účtu. Jediným rozdílem je první příkaz místní nabídky, **Přidat do skupiny**. Jeho



1.9 Nabídka pro práci se skupinami