Tajné triky

PRO WINDOWS XP

Seznamte se se zásadami zabezpečení ve Windows XP a ochraňte svoje data před všetečnými pohledy! (CD)

DAVID ČEPIČKA, HERMANN APFELBÖCK A CHRISTIAN LÖBERING

Každý má ve svém počítači data, u nichž by určitě nechtěl, aby je viděl kdokoli nepovolaný. Ať se jedná o údaje o našich příjmech či výdajích, všemožné literární pokusy či obrázky různého charakteru. Jak ale tyto soubory ochránit před ostatními uživateli našeho počítače a jak zabránit tomu, aby se k nim pomocí počítačové sítě nedostal někdo nepovolaný?

Windows 2000 a XP patří mezi systémy, které může používat více uživatelů. Slouží k tomu transparentní způsob přihlašování, jasné oddělení dat jednotlivých uživatelů a možnost zabezpečení sdílených prostředků. Ideální nastavení zabezpečení počítače (totiž takové, aby každý uživatel směl pouze tam, kam mu správce počítače dovolí) však není vůbec snadné. Pokusili jsme se pro vás rozmotat klubko všech možných přihlašovacích procedur, zásad skupin, přidělování práv, konfigurací uživatelů či počítačů nebo nejrůznějších možností pro sdílení prostředků. Relativně snadno přístupná jsou pravidla pro přihlašování uživatelů. O něco složitější je situace při nastavování autorizace oprávněných uživatelů či uživatelských skupin, konfigurace zásad skupiny nebo přímé přidělování přístupových práv jednotlivým souborům a složkám. Prostřednictvím našich tipů a triků ale bude vše jasné i méně zkušeným uživatelům, případně těm, kdo přecházejí na Windows XP z verzí Windows 9x/ME. Samozřejmě, že se každá Windows (a zvláště Windows XP Home) chovají trochu jinak. Po přečtení článku však bude záležet pouze na vašem rozhodnutí, do jaké míry chcete svůj počítač zabezpečit.

Přihlašování a Zásady skupiny

Windows 2000, XP Professional i Windows XP Home (i když v tomto případě se značnými omezeními) jsou z hlediska zabezpečení na daleko vyšší úrovni než Windows 98/ME. Rozhodujícím činitelem je zde systém souborů NTFS (viz odstavec Přístupová práva na diskovém oddílu NTFS). I když Windows 2000/XP instalujeme na systém souborů FAT32, stejně nabízejí mnohem lepší zabezpečení před neoprávněným přístupem při přihlašování, během provozu i při použití konzoly pro zotavení než Windows 9x/ME. A právě obecné systémové politiky jsou tématem první části.

1) Zabezpečení při přihlašování do systému

Přihlašovací dialogové okno při lokálním přihlašování neúprosně vyžaduje zadání v systému existujícího uživatelského jména a k němu příslušného hesla. To se může zdát jako dostatečné zabezpečení a také tomu tak teoreticky je. Prakticky je však celý systém zabezpečený až tehdy, pokud budete respektovat několik užitečných zásad.

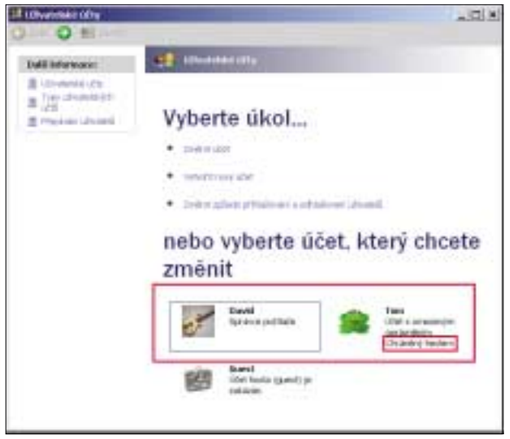
Uvítací obrazovka Windows XP ukazuje všechny na počítači existující účty (představované uživatelským jménem); operační systém je tak otevřenější než při použití klasického přihlašovacího dialogového okna, v němž musí uživatel zadat i příslušné uživatelské jméno. Upřednostňovaný způsob přihlašování do systému můžete nastavit pomocí Ovládacích panelů, poklepete-li na ikonu *Uživatelské účty* a následně stisknete odkaz *Změnit způsob přihlašování a odhlašování uživatelů*.

Zabezpečení systému při přihlašování je samozřejmě pryč, pokud se v něm vyskytují uživatelská jména, která nevyžadují zadání hesla. Zní to sice triviálně, ale o to je to důležitější, jelikož některé v systému přednastavené uživatelské účty zadání hesla vůbec nevyžadují. Situace je o to horší, že většina uživatelů o existenci takových účtů vůbec neví. Například ve Windows XP Home je účet *Administrator* standardně nastaven tak, aby při přihlašování nepotřeboval zadání hesla. Důsledkem je, že prakticky každý uživatel může nad takovým počítačem získat neomezenou kontrolu, pokud počítač spustí v nouzovém režimu a při přihlašování vybere účet *Administrator*, případně pokud spustí počítač a přihlásí se po spuštění *Konzoly pro zotavení* jako administrátor.

Tuto kritickou chybu odstraníte tím, že na příkazovém řádku zadáte příkaz:

net user administrator <heslo>

Pokud je povolen standardní účet *Guest*, pak se do systému rovněž může dostat kdekdo i bez zadání hesla. Neexistuje žádný závažný důvod, proč by měl být přístup přes účet *Guest* (pro přihlášení na lokálním počítači) povolen. Dokonce i když budete sdílet některé prostředky tohoto počítače (viz odstavec **Windows v síti**) pro všechny uživatele v síti, nepotřebujete účet *Guest* povolovat. Pokud se chce nějaký uživatel anonymně přihlašovat do sítě přes účet *Guest*, je třeba v počítači provést několik nastavení pravidel právě pro tento účet. Lokální přihlášení přes účet *Guest* na počítač však není ani v tomto případě nutné.



▶ **Prázdná hesla: přihlašování bez hesla byste rozhodně měli vyloučit. Týká se to zejména lokálně povoleného účtu *Guest* a standardně existujícího účtu *Administrator* v systému Windows XP Home.**

2) Zabezpečení při zadávání hesla

Na rozdíl od přihlašovacích jmen, která lze zadat libovolně – velkými písmeny, malými písmeny či oběma druhy – vyžadují Windows při psaní hesla přesné zadání velkých nebo malých písmen (heslo je tzv. *case-sensitive*). Další požadavky na jeho podobu můžete nastavit v *Nastavení zabezpečení* (vyvoláte je stiskem tlačítka *Start/Spustit*, do políčka *Otevřít*: napíšete příkaz SECPOL.MSC). Zde poklepejte na položku *Zásady účtů* a dále klepněte na položku *Zásady hesla* (není k dispozici ve Windows XP Home). Ze zde dostupných voleb můžeme doporučit například požadavek na minimální délku hesla nebo povolení zásady *Heslo musí splňovat požadavky na složitost*. Znamená to, že každé heslo, které má tomuto požadavku vyhovovat, musí splňovat tři ze čtyř kritérií, tj. musí obsahovat velká písmena, malá písmena, číslice a znaky. Změna nastavení této zásady nemá vliv na již existující hesla, platí pouze pro nově zadaná hesla či při změnách již existujícího hesla.

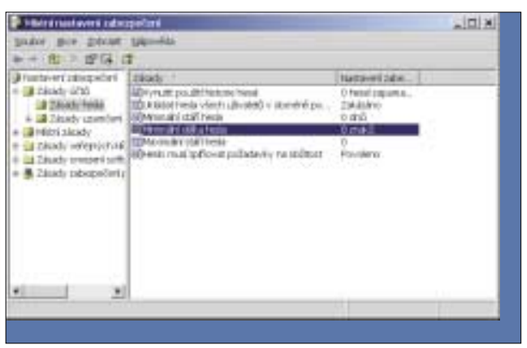
Přesvědčte se, že se z každého účtu ze skupiny administrátorů dají změnit všechna hesla a nastavit všechny politiky pro zabezpečení systému. Na druhou stranu čím méně administrátorských účtů v systému existuje, tím lepší je zabezpečení při přihlašování do systému.

3) Administrátoři a uživatelé s omezenými přístupovými právy

Pro zjednodušení přidělování přístupových práv rozlišují Windows mezi nadřazenými uživatelskými skupinami a ostatními. Každý uživatelský účet v počítači patří minimálně do jedné skupiny. Dialogové okno *Uživatelské účty* ve Windows XP dokonce zná standardně pouze dvě skupiny: správce počítače a účty s omezeným oprávněním. Toto rozdělení je však velmi zjednodušené, jelikož se účty s omezeným oprávněním dělí na další podskupiny. Každý správce počítače by měl minimálně vědět, že sem patří podskupiny uživatelů se standardním oprávněním, omezeným oprávněním a *Guests*.

TIP: Prostřednictvím nikde nedokumentovaného příkazu **control userpasswords2** se můžete i ve Windows XP dostat k dialogovému oknu pro uživatelské účty, kde je možné nastavit podrobnější nastavení omezení jednotlivých uživatelů. Nezapomeňte ale, že ve verzi Windows XP Home mezi uživatelem se standardním a omezeným oprávněním žádný rozdíl neexistuje.

Pokud nejsou pro jednotlivé uživatelské účty nastavena žádná další omezení, kupříkladu pomocí konzoly *Gpedit* nebo stanovením přístupo-



▶ **Vynucené zadávání bezpečných hesel v Místním nastavení zabezpečení: zadáním minimální délky hesla a povolením zásady Heslo musí splňovat požadavky na složitost zakážete použití prázdných nebo příliš jednoduchých hesel.**

Centrála zabezpečení systému Windows

Způsob přihlašování do systému, bezpečnostní politiky a přidělování přístupových práv pro složky a soubory na diskovém oddílu NTFS – to jsou nejúčinnější prostředky, které Windows používají pro ochranu dat před neoprávněným přístupem nebo pro bezpečné předávání těchto dat dále. Windows však rovněž nabízejí několik utilit, jimiž můžete tato nastavení zabezpečení ladit.

CACLS.EXE: K přidělování přístupových práv pro soubory a složky na diskových oddílech NTFS můžete kromě grafických prostředků Windows použít i utilitu CACLS.EXE. Chcete-li například uživateli Anna přidělit úplný přístup ke složce **C:\Program Files**, použijte následující příkaz:

cacls C:\Program Files /g Anna:F

Informace o nejrůznějších dalších přepínačích získáte po zadání příkazu **cacls /?**.

FSMGMT.MSC: *Průvodce pro sdílené složky* pomůže udržet přehled o všech sdílených síťových prostředcích. Pokud na sdílenou složku klepnete pravým tlačítkem myši a z kontextového menu zvolíte příkaz *Vlastnosti*, pak si můžete ve Windows 2000 a XP Professional prohlédnout a upravit přístupová práva k této složce (viz také příkaz **net share**).

GPEDIT.MSC (2000, XP Professional): Editor pro zásady skupin je centrálou pro celou řadu nastavení zabezpečení, zapisovaných do registru. Pokud chcete nastavení nějaké zásady změnit nebo nějakou povolit, poklepejte na ni a přiřaďte jí požadovanou hodnotu.

LUSRMGR.MSC: Tento správce místních uživatelů a skupin zobrazí všechny v systému existující uživatele a jejich účty, skupiny a členství v nich. Zde je rovněž můžete upravovat, mazat libovolné účty nebo vytvářet uživatelské účty nové (viz také příkaz **net user**).

Net localgroup: Tento příkaz dovoluje dokonce i ve Windows XP Home vytvoření a odstranění uživatelských skupin (***net localgroup /add <jméno skupiny>***).

Net share: Tento příkaz zobrazí všechny sdílené prostředky, vytvoří nová sdílení (příkazem **net share <jméno sdíleného prostředku> <cesta>)** nebo odstraní již existující prostředek.

Upozornění: Při sdílení pomocí příkazu **net share** mají všichni v systému autorizovaní uživatelé a uživatel *Guest* práva ke čtení a k zápisu, samozřejmě pokud to dovoluje nastavení přístupových práv na diskovém oddílu NTFS.

Net user: Příkaz **net user** se svými přepínači (viz příkaz **net user /?**) je jednou z nejvýkonnějších alternativ ke konzole LUSRMGR.MSC. Běží na příkazovém řádku. Zobrazí uživatelské účty, vytvoří nové (*/add*) nebo smaže existující (*/delete*), aktivuje a deaktivuje účty (*/active:yes* a */active:no*). S jeho pomocí se rovněž dají nastavovat přístupová hesla (příkaz **net user <jméno účtu> <heslo>**). Nikde není dokumentována možnost omezit přihlašování uživatelů na určité rozpětí hodin, například pomocí příkazu **net user <uživatelský účet> /times:Po-Pá,14-18.** Příkaz **net user <uživatelský účet > /times:all** zase výše nastavené časově omezené přihlašování zruší.

XCACLS.EXE: Tuto utilitu naleznete v *Resource Kitu* Windows 2000, popřípadě NA NAŠEM CD. Funguje také ve Windows XP a nabízí – podle standardní utility CACLS.EXE – podrobnější přidělování přístupových práv a především možnost převzetí vlastnictví souborových objektů.

vých práv na diskovém oddílu NTFS, pak o tom, co může uživatel přihlášený pod určitým uživatelským účtem na počítači provádět, rozhoduje pouze příslušnost k té či oné skupině uživatelů. Například uživatel *Tom* nesmí provádět to, co uživatel *Administrator*, pokud ovšem nepatří do stejné skupiny uživatelů.

Uživatelské účty ve skupině *Administrators* a ve skupině účtů s omezením mají v každém případě globálně přidělena rozdílná práva, a to i tehdy, pokud systém nemá žádný diskový oddíl typu NTFS a tedy není možné jednotlivým souborům a složkám přidělovat přístupová práva. Uživatelské účty ze skupiny *Administrators* smějí v počítači provádět v podstatě vše, a proto mohou například nastavit omezení i pro ostatní účty ve skupině *Administrators*. Uživatelé s omezeným oprávněním samozřejmě nemohou vytvářet nové účty a měnit nastavení účtů (a rovněž nemají přístup k utilitám *Gpedit*, *Secpol* a *Lusrmgr*). Všechny zásahy s globálním účinkem na systém jsou rovněž zakázány – týká se to například instalace ovladačů, písem či instalace programů do složky *Program Files*. Dále je zakázáno provádět jakékoliv změny v registru, v systémových službách, typech souborů, nelze měnit čas nebo nastavení sdílení síťových prostředků. To samé platí i pro přístup do *Správce disků*, defragmentaci nebo i pro možnost nastavení systémových proměnných či nastavení Koše.

Členové skupiny *Users* však mohou upravovat svůj vlastní profil. Účtům ze skupiny *Power User* (uživatel se standardním oprávněním) – nejsou k dispozici ve Windows XP Home – je povoleno ještě o něco více, například instalovat aplikace do libovolné složky, měnit nastavení systémového času, tiskáren či napájení. Pro všechny běžné a nejen ryze administrátorské činnosti postačí pracovat pod účtem ze skupiny *Power User*, často je dostatečný i účet ze skupiny *Users*.

Kromě apletu *Uživatelské účty* existuje v Ovládacích panelech ve Windows 2000 a XP Professional *Správce místních uživatelů a skupin*. Spustíte jej příkazem LUSRMGR.MSC. Tato utilita je prakticky nepostradatelná v případě, kdy chcete vytvořit svoje vlastní uživatelské skupiny.

TIP: V systému Windows XP Home modul LUSRMGR.MSC chybí. Pro vytvoření nové uživatelské skupiny proto použijte následující variantu příkazu **net**:

net localgroup /add <jméno skupiny>

Pro odstranění skupiny nahraďte parametr */add* parametrem */delete*.

Pokud u nějakého účtu zrušíte jeho členství ve všech skupinách, ať již prostřednictvím příkazu **net** nebo LUSRMGR.MSC, přesunou jej Windows automaticky do skupiny uživatelů s omezeným oprávněním (*Users*).

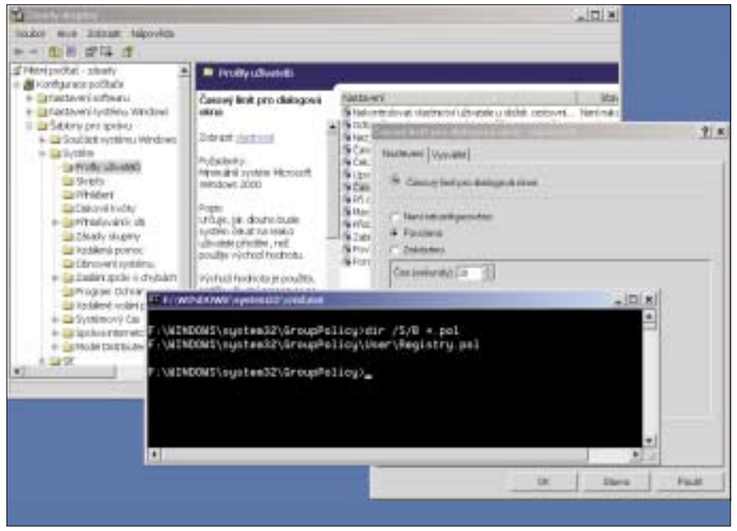
Kromě doposud jmenovaných standardních uživatelských skupin ještě existuje skupina *Everyone*. Nemyslí se tím v pravém slova smyslu každý uživatel, jak by se mohlo podle překladu do češtiny zdát, nýbrž je to skupina pro všechny v systému autorizované uživatele včetně uživatelů *Guest* – toto byste měli mít na paměti, pokud chcete obsah svého počítače zpřístupnit opravdu každému.

Klasický správce uživatelských účtů z Windows 2000: pomocí nedokumentovaného příkazu jej použijete i ve Windows XP.

4) Ochrana souborů při bootování přes externí média

Po spuštění počítače může uživatel spustit *Konzolu pro zotavení*. I tato velmi jednoduchá utilita ovládaná z příkazového řádku žádá pro zpřístupnění všech dat heslo administrátora. Toto je standardní nastavení, které lze změnit pomocí *Zásad skupin*, konkrétně pomocí utility GPEDIT.MSC. Jedná se o zásadu *Konzola pro zotavení: Umožnit automatické přihlášení správce*.

Ochrana vůči neoprávněnému přístupu k datům je však prakticky bezcenná, pokud se počítač spustí prostřednictvím externího média. Pro přístup k datům na diskovém oddílu FAT32 stačí spouštěcí disketa systému MS-DOS, pro diskový oddíl NTFS pak CD s libovolnou distribucí Linuxu, popřípadě Windows PE (získáte je instalací **PE Builderu** ve verzi **3.1.3** – jedná se o freeware, který naleznete NA NAŠEM CD, popřípadě na internetové adrese **www.nu2.nu/pebuilder**). Dokonce i konzola pro zotavení z Windows 2000 přihlásí uživatele do systému Windows XP, aniž by vyžadovala zadání hesla. Pokud se tedy na vašem počítači nacházejí nějaká důvěrná data, jež by se mohla hodit i někomu jinému, pak byste měli určitě v BIOSu zakázat možnost bootování z CD a z diskety a přístup do BIOSu chránit heslem. Ještě lepším řešením je použití šifrování dat na diskovém oddílu NTFS.



Pozor při používání konzoly GPEDIT.MSC: utilita zapisuje všechna omezení, včetně těch, která se týkají jednotlivých uživatelů, do POL souborů a zde uvedené informace následně používá při přihlašování uživatele do systému. Proto byste měli soubory patřičně přejmenovat.

5) Zásady skupiny v GPEDIT.MSC

Modul snap-in s názvem GPEDIT.MSC, který patří do **Microsoft Management Console** (MMC.EXE), obsahuje několik set možností globálního nastavení zabezpečení systému. Právě z něj vychází konzola SECPOL.MSC, jež nabízí pouze část velmi rozsáhlé konzoly GPEDIT.MSC. Zásady skupiny definované v modulu GPEDIT.MSC ve skupině *Šablony pro správu* závisí na obsahu ADM souborů, které se nacházejí ve složce **%windir%\system32\GroupPolicy\Adm**. Ve Windows XP Home moduly GPEDIT a SECPOL chybí a nelze je doinstalovat.

Jak již bylo zmíněno, po otevření souboru GPEDIT.MSC získáte přístup k velkému množství globálních (*Konfigurace počítače*) a uživatelských (*Konfigurace uživatele*) nastavení. Jedná se vesměs o údaje z registru, které je možné prostřednictvím tohoto modulu pohodlně zpřístupnit a dosáhnout požadované konfigurace počínaje pracovní plochou, přes nabídku *Start* a zásady účtu až k zákazu spouštění libovolných programů. Na tomto místě vás musíme varovat před příliš velkým experimentováním. Několik ukvapených klepnutí myší v GPEDITU může způsobit zablokování systému na těch nejnevhodnějších místech, můžete dokonce zrušit přístup ke svému účtu či naopak dosáhnout značného oslabení zabezpečení systému.

Při používání GPEDITU proto musíte postupovat nejen obzvlášť pečlivě, nýbrž je nutno zachovávat následující pravidla, která jsou spíše technického rázu:

1. GPEDIT lze spustit, jak je zřejmé, pouze z účtu, který patří do skupiny *Administrators*.
2. Změna nastavení v GPEDITU vede ke vzniku souboru s příponou POL. Naleznete jej ve složce **%windir%\system32\GroupPolicy** nebo ve složce **\Machine** nebo **\User** nebo v obou, podle toho, zda byla změněna konfigurace počítače nebo uživatele.
3. Cesta **%windir%\system32\GroupPolicy** je na diskovém oddílu NTFS přístupná pouze pro členy skupiny *Administrators*.
4. Windows výše zmiňovaný POL soubor ve složce **\Machine** či **\User** načítají po přihlášení uživatele do systému, a to pro každý účet zvlášť.

Neřešte dílčí problémy, zajistěte bezpečnost KOMPLEXNĚ!
TrustPort® Phoenix Rebel
The Ultimate Security Solution
ANTIVIROVÝ PROGRAM
PERSONÁLNÍ FIREWALL
ON-LINE ŠIFROVÁNÍ
BEZPEČNÁ SKARTACE
ELEKTRONICKÝ PODPIS
TrustPort® Phoenix Rebel Workstation je kompletní řešení pro antivirovou ochranu a zabezpečení dat na pracovních stanicích a noteboocích. V jednom funkčním celku spojuje zcela nový antivirový program TrustPort® Antivirus pocházející z dílny společnosti AEC, personální firewall, program pro spolehlivé skartování elektronických dat, aplikaci pro použití elektronického podpisu a nástroj pro online šifrování na virtuálním disku.
KOMPLEXNÍ ZABEZPEČENÍ IT OD JEDINÉHO DODAVATELE !
AEC
DATA SECURITY COMPANY
AEC, spol. s r. o.
Bystrc 738/30, 602 00 Brno
tel.: +420 541 235 465?
e-mail: info@aec.cz
www.aec.cz
Registrujte se na http://registrace.aec.cz a získejte roční zkušební verzi ZDARMA!
www.phoenixrebel.cz

Z výše uvedeného plynou pro nás jako administrátory dvě upozornění. Za prvé: omezení stanovovaná přes modul GPEDIT, ačkoliv jsou většinou určena pro účty s omezeným oprávněním, smíme definovat pouze my jako správci počítače. Za druhé platí, že musíme dávat velmi dobrý pozor, abychom omezení definovaná v POL souboru omylem neaplikovali na špatné uživatelské účty. Nejjednodušeji se oběma výše zmíněným problémům vyhnete takto:

1. Přihlaste se do systému Windows 2000 a tam zobrazte dialogové okno *Uživatelské účty*. Ve Windows XP vynuťte podobné dialogové okno pomocí již zmíněného příkazu **control userpasswords2**.

2. Přemístěte uživatelský účet, který budete chtít konfigurovat, dočasně do skupiny *Administrators*.

3. Nyní se přihlaste do systému pod přihlašovacím jménem toho účtu, který budete upravovat, a spusťte *Gpedit*. Zde nastavte pro tento účet všechna omezení, jež vyžadujete.

4. Přejmenujte soubor REGISTRY.POL na <uživatelské jméno>.POL – tato operace je nutná, protože tím se vyhnete tomu, aby se provedená nastavení projevila i v jiných účtech.

5. Nakonec se přihlašte do systému jako administrátor a upravovaný účet přesuňte zase zpět ze skupiny *Administrators* do skupiny, kam původně patřil.

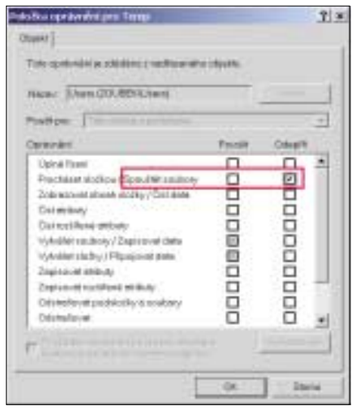
Pokud pomocí *Gpeditu* vytvořené POL soubory nesmažete, ale přidělíte jim nějaké výstižné názvy, pak můžete později již existující politiky uživatelských účtů pomocí několika málo kroků dále upravovat a nemusíte začínat úplně znovu.

Pokud se divíte, že se Microsoft touto problematikou zabýval tak intenzivně a zašel až do takových podrobností, vysvětlení je vcelku prosté. Popisované *Zásady skupiny* jsou určené zejména pro domény, které se zřizují na síťových serverech. Se zde popisovaným způsobem nasazení pro případ operačního systému s několika uživateli na jednom počítači Microsoft určitě nepočítal.

Přístupová práva na diskovém oddílu NTFS

Pokud instalujete Windows 2000 nebo XP, pak byste měli i v případě, kdy pro to neexistují žádné pádné důvody, tento systém instalovat vždy na diskový oddíl typu NTFS. Ale i když instalujete operační systém na diskový oddíl typu FAT, vždy jej můžete konvertovat na NTFS pomocí programu CONVERT.EXE. Na diskovém oddílu NTFS máte jako administrátor daleko pestřejší možnosti, jak pro ostatní uživatele vašeho počítače nastavit přístupová práva ke složkám a souborům. Všechna práva k souborům a složkám včetně jejich šifrování jsou totiž vázána výlučně na tento systém souborů.

6) Přidělování lokálních přístupových práv na diskovém oddílu NTFS



▲ **Zákaz spouštění: v takové složce, kde je zakázáno spouštění souborů, nemá ani malware žádnou šanci.**

Lokální přístupová práva k jednotlivým souborům nebo složkám můžete přiřazovat jak jednotlivým uživatelům (uživatelským účtům), tak celým uživatelským skupinám. Existuje 14 oprávnění, která můžete povolit, nepovolit, odepřít nebo ne odepřít. Pokud je vybráno několik práv, pak se vždy prosadí to přísnější. Zmíněná diferenciace slouží k tomu, aby bylo možné definovat přístupová práva jinak pro člena skupiny a jinak pro celou skupinu.

Jako ukázkový příklad si představme následující situaci: mějme uživatelskou skupinu *Users*, které přidělíme u nějaké složky právo pro zápis, na druhé straně zase jednomu členu této skupiny toto právo odepřeme. Výsledkem je, že daný člen skupiny právo zápisu do složky nemá. Pokud budete chtít ve Windows XP Professional tato lokální práva přidělovat, musíte ze všeho nejdříve v Průzkumníku v menu *Nástroje/Možnosti složky* na kartě *Zobrazení* zrušit zatržítko u položky *Použít zjednodušené sdílení souborů*. Teprve potom se objeví po klepnutí pravým tlačítkem myši na soubor či složku a po zadání příkazu *Vlastnosti* záložka *Zabezpečení*. Ve Windows 2000 je zobrazení záložky *Zabezpečení* standardně nastaveno.

TIP: Ve Windows XP Home popisovaná záložka úplně chybí. V rámečku **Windows XP Home: Přidělování lokálních práv** vám prozradíme, jak ji do tohoto operačního systému zabudovat.

Každý uživatel, který smí nějakým způsobem k objektu přistupovat, je uveden v seznamu *Název skupiny nebo jméno uživatele*. Účty, jež v tomto seznamu nejsou uvedeny vůbec, a to ani jako případní členové některé z uživatelských skupin, nemají k tomuto objektu explicitně žádné právo přístupu. Pomocí tlačítek *Přidat* a *Odebrat* můžete k tomuto objektu přidávat nové nebo odebírat existující uživatele. Po stisku tlačítka *Přidat* Windows 2000 přímo zobrazí všechny uživatelské účty a uživatelské skupiny. Windows XP vyžadují další dvě klepnutí myší, nejprve na tlačítko *Upřesnit* a posléze na *Najít* .

Na záložce *Zabezpečení*, kterou, jak již bylo zmíněno, vyvoláme klepnutím pravého tlačítka myši na objekt (soubor, složku či jiný prostředek) a následným zadáním příkazu *Vlastnosti*, můžeme účtu (nebo skupině), která je uvedena v seznamu objektů nejvýše, ve spodní polovině okna s popiskem *Oprávnění pro ...* přiřazovat nebo odepírat například práva číst, zapisovat, měnit, spouštět nebo i úplné řízení. Stačí pouze vybrat daného uživatele nebo skupinu a umístit zatržítko do sloupečku *Povolit*, čímž přístup k objektu povolíte, nebo *Odepřít*, čímž přístup k objektu zakážete.

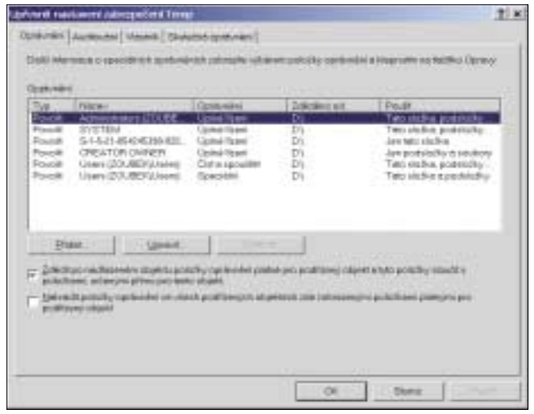
Pokud byste chtěli skupině *Users* povolit přístup pro čtení k nějaké složce, ale pouze pro jednoho z jejich členů, například Martinovi, toto právo odepřít, pak označte v horní polovině okna danou skupinu. Ve spodní polovině nastavte právo *Číst* na hodnotu *Povolit*, dále označte v horní polovině okna uživatele Martin a jemu nastavte právo *Číst* na hodnotu *Odepřít*. Pokud byste u uživatele Martina pouze zrušili zatržítko u práva *Číst* u hodnoty *Povolit*, uplatnilo by se právo ke čtení nastavené pro celou skupinu a uživateli Martinovi by právo *Číst* zůstalo přiděleno.

Prostřednictvím tlačítka *Upřesnit* na záložce *Zabezpečení* a po klepnutí na libovolný účet se vám zpřístupní 14 nejrůznějších druhů práv, přístupných na diskovém oddílu NTFS. Tyto položky dále upřesňují obecně nastavená práva v předchozím dialogovém okně. Tak můžete například zakázat spouštění souborů, i když jejich čtení povolíte. Navíc se v popisovaném dialogovém okně zpřístupní i možnosti pro nastavení dědičnosti práv na podsložky a soubory v této složce (viz tip č. 7).

7) Dědičnost a skutečná oprávnění

Dědičnost znamená, že práva nastavená pro jednu složku platí i pro její podřazené objekty (podsložky a soubory v ní). Dědičnost práv může být samozřejmě nastavena pouze u složek. Když klepnete na složku pravým tlačítkem myši a z kontextového menu vyberete příkaz *Vlastnosti*, máte na záložce *Zabezpečení* možnost nastavit přístupová práva. Když zde navíc stisknete tlačítko *Upřesnit*, objeví se dialogové okno pro rozšířené nastavení přístupových práv, kde můžete zadat, pro které objekty mají vámi nastavená práva platit. Standardně jsou zde uvedena práva pro vybranou složku, její podsložky a pro všechny soubory ve složce. Při poklepání na jednotlivé položky v poli *Oprávnění* můžete v dialogovém okně, které se objeví, v poli *Použít pro:* zvolit, kde chcete, aby přístupová práva platila – buď pouze ve vybrané složce, nebo i ve všech jejích podsložkách. Kromě toho můžete dědičnost práv omezit pouze na úroveň pod vybranou složkou. Ale pozor: za jistých okolností se tím mohou odstranit všechna existující oprávnění na nižších úrovních.

Obráceně můžete pro soubory či složky jejich zděděná práva upravovat. K tomu účelu v dialogovém okně *Upřesnit nastavení zabezpečení*, jež jsme popisovali v minulém odstavci, zrušte zatržítko u položky *Zdědit po nadřazeném objektu položky oprávnění platné pro podřízený objekt a tyto položky sloučit s položkami, určenými přímo pro tento objekt*.



◀ **Zděděná práva: nové složce jsou vždy nejprve přidělena stejná práva jako nadřazené složce. Tato práva však můžete podle své aktuální potřeby sami upravit.**

Jaká skutečná oprávnění k nějakému objektu pro každého uživatele platí, je záležitost členství daného uživatele ve skupinách, dále dědičnosti a konečně individuálních práv uživatele, která mu jsou pro daný objekt přiřazena nebo odepřena. Není snadné to rychle zjistit, ale Windows XP je naštěstí dokáží určit, a to na záložce *Skutečná oprávnění*. Zde si můžete vybrat libovolného uživatele a zobrazit jeho skutečná přístupová práva. V operačním systému Windows 2000 však musíte sami zjistit, jaká práva skutečně vlastníte. Světlou výjimkou jsou účty administrátorů. I ty mohou být zdánlivě jinými administrátory nějakým způsobem omezeny, ale plný přístup k systému je možné velmi jednoduše vrátit zpět.

8) Účty administrátorů bez omezení přístupu

Pro žádný účet ze skupiny *Administrators* neexistují omezení přístupu. Je sice možné nějakému účtu ze skupiny *Administrators* odepřít přístup k libovolným souborům či složkám, v praxi to však nemá žádný smysl. Každý administrátor totiž může jednoduše převzít vlastnictví libovolného souboru či složky a přístupová práva si upravit podle svého.

Pokud chcete jako administrátor převzít vlastnictví složky, otevřete nejprve dialogové okno *Upřesnit nastavení zabezpečení* (postup byl zmíněn v předchozích tipech) a zde se přesuňte na záložku *Vlastník*. Tady vyberte konto administrátora a stiskněte tlačítko *Použít*. Úplný přístup ke složce získáte zase zpět, pokud dialogové okno se záložkou *Zabezpečení* nejprve zavřete, poté hned zase otevřete, do seznamu skupin či uživatelů přidáte svůj účet a přidělíte si právo *Úplného řízení*.

9) Zabezpečení dat pomocí šifrování na oddílech NTFS

Jak již bylo uvedeno v tipu č. 4, všechna pravidla pro přístup k souborům jsou k ničemu, pokud existuje možnost dostat se k datům oklikou přes spuštění jiného operačního systému. Ten, kdo chce zabezpečit svoje data i před tímto nebezpečím, by měl použít možnost šifrování souborů na diskovém oddílu NTFS. Tuto funkci nabízejí Windows 2000 a Windows XP Professional. Pro zašifrování souboru nebo složky na ně stačí klepnout pravým tlačítkem myši a z kontextového menu zvolit příkaz *Vlastnosti*. Na záložce *Obecné* je pak třeba stisknout tlačítko *Upřesnit*. Svá data ochráníte, pokud zde umístíte zatržítko před položku *Šifrovat obsah a zabezpečit tak data* a potvrdíte vše stiskem tlačítka *OK*.

TIP: Soubory a složky můžete šifrovat také prostřednictvím kontextového menu. Pro vytvoření potřebné položky kontextového menu si spusťte Editor registru a otevřete klíč **Hkey_Current_User\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced**. Zde vytvořte novou hodnotu typu DWORD s názvem **EncryptionContextMenu** a s údajem hodnoty **1** a restartujte počítač.

Po zašifrování můžete soubor či složku používat stejně jako předtím, ale žádný jiný uživatel, dokonce ani nikdo ze skupiny *Administrators*, nebude moci daný soubor číst nebo kopírovat na disk se souborovým systémem FAT32. Výjimkou je ve Windows 2000 *Administrator* (nikoliv skupina *Administrators*!). Zde je administrátor standardně nastaven skutečně jako všemocný uživatel, neboť může číst všechna šifrovaná data, a to jen díky tomu, že disponuje *klíčem pro obnovení dat*.

Pokud byste disk se šifrovanými soubory připojili do jiného počítače nebo pokud byste na něj znovu nainstalovali operační systém, ztratíte přístup ke všem šifrovaným složkám a souborům. Z tohoto důvodu byste si rozhodně měli vytvořit

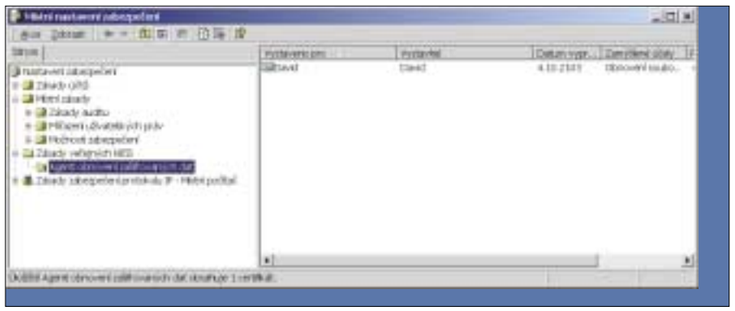
Windows XP Home: Přidělování lokálních práv

Když ve Windows XP Home klepnete pravým tlačítkem na složku či soubor a z kontextového menu zvolíte příkaz *Vlastnosti*, zjistíte, že záložka *Zabezpečení* chybí. Teprve až v nouzovém režimu objevíte, že i Windows XP Home dokáží přidělovat přístupová práva na diskovém oddílu NTFS. Dalším důkazem pak je samotná existence utility CACLS.EXE.

Samotný Microsoft poskytuje pohodlné řešení, jehož původ sahá daleko do doby před Windows XP. **Microsoft Security Manager** pro Windows NT4 Service Pack 4 je doplňkovým modulem pro **Microsoft Management Console** (MMC), která do systémů založených na NT technologii poskytovala podstatnou část zabezpečení. Pro Windows XP Home jsou činnosti, kvůli nimž byl **Microsoft Security Manager** vyvinut, v podstatě nezajímavé, ale o to zajímavější je nepřehlédnutelný vedlejší efekt. Utilita totiž dokáže v Průzkumníku ve Windows XP Home zobrazit chybějící záložku *Zabezpečení*.

Instalace je jednoduchá. **Microsoft Security Manager** naleznete NA NAŠEM CD jako samorozbalující archiv. Spusťte jej a jeho obsah se rozbalí do dočasné složky. Přesuňte se do ní a klepněte pravým tlačítkem na soubor SETUP.INF. Z kontextového menu pak vyberte příkaz *Nainstalovat*. Vzhledem k tomu, že se jedná o anglickou verzi utility, budete u české verze Windows XP Home varováni před kopírováním knihovny ESENT.DLL. Zde stiskněte tlačítko *Ne*, abyste si ponechali českou verzi této knihovny. Po skončení instalace restartujte počítač a nyní můžete přidělovat přístupová práva na diskových oddílech NTFS stejně jako ve Windows XP Professional.

zálohu svého soukromého klíče. Tu uděláte tak, že spustíte Internet Explorer a klepnete do menu *Nástroje/Možnosti Internetu*. Přesuňte se na záložku *Obsah* a stiskněte tlačítko *Certifikáty*. Nyní si označte svůj klíč. Poznáte jej tak, že jeho název vychází z vašeho přihlašovacího jména, je platný 100 let a v poli *Zamýšlené účely certifikátu* je uveden popis *Šifrování systému souborů*. V dalším kroku klepněte na tlačítko *Exportovat* a v průvodci vyberte položku *Ano, exportovat soukromý klíč*, zadejte heslo a soubor s klíčem uložte kupříkladu na disketu. Po instalaci nového systému importujte klíč tak, že na soubor poklepete a následně zadáte přístupové heslo.



▲ **Šifrování složek a souborů: administrátor systému ve Windows 2000 může zobrazit všechna zašifrovaná data, neboť klíč pro obnovu dat je standardně v jeho účtu k dispozici.**

Windows v síti

Právo přistupovat k nějaké složce sdílené na síti, se ve Windows 2000 a XP řídí stejnými pravidly jako kdyby se jednalo o přístup ke složce lokální. I zde existují uživatelé a uživatelské skupiny s možností individuálního přiřazení rozličných práv. Pouze Windows XP Home poněkud vybočují z řady. Považují totiž vlastně každého uživatele, který přistupuje do systému z jiného počítače v síti, za hosta (uživatele *Guest* – viz rámeček **„Guest“: Pohostinnost nezávislá na systému**).

10) Zabezpečené sdílení síťových prostředků

Místní oprávnění pro přístup k nějakému objektu se nastavují na záložce *Zabezpečení* (pro Windows XP), popřípadě na záložce *Nastavení zabezpečení* (Windows 2000). Klepneme-li na nějakou složku pravým tlačítkem myši, pak budeme mít v kontextovém menu k dispozici příkaz *Sdílení a zabezpečení*. Pokud jej vybereme, objeví se dialogové okno, v němž je k dispozici záložka *Sdílení*. Na tomto místě můžeme jako administrátoři systému přidělit složce jméno, pod kterým bude v síti sdílena, a prostřednictvím tlačítka *Oprávnění* můžeme složce přidělit přístupová práva pro všechny uživatelské účty nebo uživatelské skupiny, jež v počítači existují. Na rozdíl od Windows 9x/ME může tedy ke sdílenému prostředku ze sítě přistupovat pouze ten, kdo má na tomto počítači založen uživatelský účet. Ve Windows XP Professional musí být pro přidělování práv splněn předpoklad, že je zrušena volba zjednodušeného sdílení souborů, jak již bylo uvedeno v tipu č. 6.

Obecně platí, že všechny sdílené prostředky, k nimž mají mít přístup všichni uživatelé z libovolného místa, musí mít právo přístupu pro uživatele *Guest*. Windows XP Home, jak je uvedeno v rámečku **„Guest“: Pohostinnost nezávislá na systému**, znají v síti pouze přístup přes účet uživatele *Guest*. Pokud se přistupuje k síťovému prostředku přes něj, není třeba žádné heslo.

Průzkumník Windows označuje sdílenou složku ikonkou složky se symbolem ruky, daleko lepší přehled o všech sdílených složkách však poskytne speciální utilita FSMGMT.MSC. Zobrazí totiž všechny sdílené prostředky včetně kompletní cesty k nim, dále všechna oprávnění, jakož i všechny otevřené soubory. Navíc dokáže sdílení prostředku zrušit nebo vytvořit znovu.

Ve Windows XP Home je utilita FSMGMT.MSC omezena pouze na výpis sdílených prostředků. Tady musíte pro další operace buď použít Průzkumníka, nebo na příkazovém řádku příkaz **net share**. Tento příkaz vám kupř. ukáže, že složka **\Documents and Settings\All Users\Dokumenty** je pro všechny automaticky sdílena jako **SharedDocs**. Toto sdílení pak můžete zrušit příkazem **net share shareddocs /delete**.

TIP: Mějte neustále na paměti, že lokální přístupová práva ke složce či souboru vždy dominují nad právy k souboru či složce jako sdílenému síťovému prostředku. Pokud tedy například uživateli Martin přidělíte právo k nějaké složce, ale lokálně mu odepřete právo ke čtení, nebude moci tento uživatel složku sdílet. Každý přístup uživatele ze sítě tedy musí zdolat dvě překážky: první je právo uživatele na přístup ke složce jako ke sdílenému síťovému prostředku, tou druhou je vlastnictví lokálního oprávnění pro přístup k objektu.

11) Skrytí sdílených prostředků pomocí „$“

Pokud ve Windows 2000 nebo XP Professional otevřete konzolu *Sdílené složky*, představovanou souborem FSMGMT.MSC, objeví se standardně každý diskový oddíl jako sdílený pod názvem **<písmenko disku>$**. V tomto případě se jedná o sdílení pro účely administrace systému. Uži-

Sdílení ve Windows XP Home: Jen pro hosty

Na rozdíl od Windows XP Professional dokáží Windows XP Home sdílet složky na diskových oddílech NTFS výlučně prostřednictvím zjednodušeného sdílení souborů. Konkrétně to znamená, že složku umožníte sdílet buď všem uživatelům, nebo nikomu. Windows XP Home při přístupu ke složce ze sítě nerozlišují jednotlivé uživatele, nýbrž každý přístup definují jako kdyby přistupoval uživatel *Guest* (neboli *Host*). Z přístupových práv se rozlišuje pouze mezi právem ke čtení a právem k zápisu.

Takové zjednodušené sdílení se sice velmi jednoduše používá, má ale celou řadu závažných nedostatků: princip autorizace uživatelů pomocí uživatelských účtů je mimo hru a úroveň zabezpečení systému se náhle propadá na úroveň představovanou systémy Windows 9x, kde sdílení prostředků platilo také obecně, ale alespoň bylo možné přístup k nim zabezpečit heslem.

V této svízelné situaci však přece jen lze něco udělat. Jak již bylo zmíněno v rámečku s názvem **Windows XP Home: Přidělování lokálních práv**, je možné záložku *Zabezpečení* do systému instalovat, čímž můžete přístupová oprávnění k síťovým sdíleným prostředkům upravit tak, že kupříkladu uživateli *Guest* přiřadíte patřičná oprávnění pro čtení, zápis, změnu či možnost prohlížení obsahu složky.

Upozornění: Pokud účtu *Guest* úplně odepřete přístup k nějaké složce, nebude k ní moci přistupovat ze sítě žádný uživatel.

TIP: Známe ještě jeden nikde nedokumentovaný trik, jak omezit okruh uživatelů nějakého sdíleného prostředku. Spusťte příkazový řádek příkazem CMD.EXE a zadejte příkaz:

```
net user guest <heslo>
```

čímž účet *Guest* opatříte heslem – standardně je heslo prázdné. Potom všichni, kdo budou přistupovat ke sdílenému prostředku na počítači s Windows XP Home, budou muset zadat heslo. Tím dostanete nejmodernější operační systém z roku 2005 (rozuměj Windows XP) alespoň na úroveň Windows 95.

vatel s právy administrátora tak může přes síť z jiného počítače zapisovat a číst ze všech diskových oddílů. Znak **$** způsobuje, že tato sdílení se neobjeví, pokud poklepete na jiných počítačích na ikonku *Okolní počítače* nebo *Místa v síti*. Prostřednictvím příkazu **\\<jméno počítače>\C$** a s právy administrátora je však přístup k tomuto počítači možný. A pokud jste účet administrátora a všechny ostatní účty ve skupině *Administrators* vytvořili vy sami, nepředstavují tato sdílení žádné bezpečnostní riziko.

TIP: Pokud byste přesto výše zmiňovaná sdílení pro účely správy chtěli zrušit, spusťte Editor registru a otevřete klíč **Hkey_Local_Machine\System\CurrentControlSet\Services\LanManServer\Parameters** a vytvořte zde novou hodnotu typu DWORD s názvem **AutoShareWks** a jako údaj hodnoty napište číslo **0**. Po restartu počítače budou všechna administrativní sdílení pryč.

Upozornění: Stejným způsobem jako administrativní sdílení můžete nastavit i svoje sdílené prostředky. Pokud za jejich název zadáte jako poslední znak **$**, stanou se i tyto při poklepání na ikonu *Okolní počítače* nebo *Místa v síti* na jiných počítačích neviditelnými. Tento způsob skrytí sdílených prostředků je však účinný pouze v Průzkumníku Windows, proto raději všechna oprávnění nastavte tak, aby se k nim nemohl dostat nikdo nepovolaný. 5 0146/OK ❑

„Guest“: Pohostinnost nezávislá na systému

Při standardním nastavení není uživateli *Guest* vůbec povoleno se do systému lokálně přihlásit. Měnit toto nastavení by určitě nebylo vhodné, neboť účet *Guest* povoluje přihlášení do systému bez nutnosti zadání hesla. Pro přístup ke sdíleným prostředkům z prostředí sítě to však může být někdy užitečné, protože v opačném případě byste museli pro každého uživatele přistupujícího ze sítě definovat na počítači vlastní uživatelský účet.

Windows 2000: V tomto systému je účet *Guest* úplně deaktivován – jak lokálně, tak v síti. Pokud chcete zpřístupnit nějaký síťový prostředek všem uživatelům, spusťte LUSMGR.MSC, klepněte pravým tlačítkem na položku *Guest*, z kontextového menu vyberte příkaz *Vlastnosti* a zrušte zatržítko u položky *Účet je zablokován*.

Aby se do systému nemohl přes účet *Guest* nikdo lokálně přihlásit, spusťte SECPOL.MSC, zde vyberte postupně položky *Místní zásady/ /Přiřazení uživatelských práv* a ručně přidejte účet *Guest* do zásady *Odepřít místní přihlášení*. Pro přístup do počítače ze sítě pak ve stejném dialogovém okně odstraňte položku *Guest* ze zásady *Odepřít přístup k tomuto počítači ze sítě*.

Windows XP Home: V tomto operačním systému smějí všichni uživatelé přistupovat k tomuto počítači ze sítě, a to i přesto, že je účet *Guest* zdánlivě zakázán. Proto není třeba provádět pro zajištění přístupu ze sítě do tohoto počítače řádné další kroky.

Windows XP Professional: Přístup ke sdíleným prostředkům přes účet *Guest* zde zajistíte stejně jako u Windows 2000 – tedy přes zásadu *Odepřít přístup k tomuto počítači ze síti*. Dialogové okno *Místní uživatelé a skupiny* (LUSMGR.MSC) je v tomto případě poněkud zmatené. Podobně jako v systému Windows XP Home je i tady účet *Guest* standardně deaktivovaný. Toto nastavení se však vztahuje pouze a jedině na možnost lokálního přihlášení (v tomto případě se jedná spíše o možnost nepřihlášení se).

Nezapomeňte, že přístup ke sdíleným prostředkům prostřednictvím účtu *Guest* je možný jen v tom případě, kdy má uživatel *Guest* k danému prostředku minimálně lokální právo ke čtení.