kapitola

8

Konfigurace zabezpečení systému Windows

Obsah kapitoly:

Zabezpečení nepatří v rámci registru k zajímavým tématům a není ani příliš oblíbené. Jedná se však o jeden z nejdůležitějších prvků dnešních informačních technologií.

Zabezpečení má stovky aspektů, v této kapitole se ale zaměříme jen na jeden: registr. Můžete změnit seznam ACL (Access Control List) klíče. Klíče lze auditovat. Můžete také převzít vlastnictví klíčů. Žádnou z těchto možností však nemůžete využít u samostatných hodnot, jako tomu je u jednotlivých souborů. Zkušení uživatelé se o zabezpečení registru obvykle příliš nezajímají, IT profesionálové však často nemají jinou volbu.

Možnost upravovat seznamy ACL však neznamená, že byste tak měli činit. Změna zabezpečení registru není dobrý nápad, pokud k ní nemáte určitý důvod. V nejlepším případě provedete změnu, která není podstatná. V horším případě byste mohli způsobit chybné fungování systému Microsoft Windows XP nebo serveru Windows Server 2003. Proč tedy má zabezpečení registru své místo v této knize? Může dojít k situacím, kdy musí IT profesionálové změnit výchozí oprávnění registru pro zavedení softwaru. To se zcela liší od provádění úprav v zabezpečení registru jen ze zvědavosti. Uživatelé mohou mít například aplikaci, kterou lze spouštět pouze v případě, že se do operačního systému přihlásí jako členové skupiny Administrators. V podnikovém prostředí však určitě nechcete do této skupiny zařazovat všechny uživatele. Řešením je zavedení systému Windows s vlastními oprávněními, aby uživatelé mohli takové programy spouštět jako členové skupiny Power Users nebo Users. Protože je tento případ nejčastější, zaměřuje se na něj tato kapitola především.

Vlastní oprávnění můžete nasadit dvěma způsoby. Prvním z nich je ruční nastavení. Pro úplnost si ukážeme, jak změnit oprávnění klíče v editoru Registry Editor (`Regedit`). Poté vytvoříte šablonu zabezpečení s vlastními oprávněními registru a následně ji uplatníte pro požadovaný počítač. Nebudete však muset běhat od počítače k počítači a nasazovat šablonu; před zavedením zařadíte danou šablonu do obrazů disků. Druhou metodou je použití Group Policy. Vytvoříte objekt GPO (Group Policy Object) a potom do něj importujete šablonu zabezpečení pro vytvo-

ření zásady zabezpečení pro vaši síť. Systém Windows automaticky uplatní vlastní oprávnění z vaší šablony pro počítač a uživatele, jež jsou v oblasti působení objektu GPO. V této knize se příliš nehovoří o Group Policy, avšak poslední část v kapitole 7, „Zásady založené na registru“, uvádí mnoho dobrých a navíc bezplatných zdrojů informací k tomuto tématu.

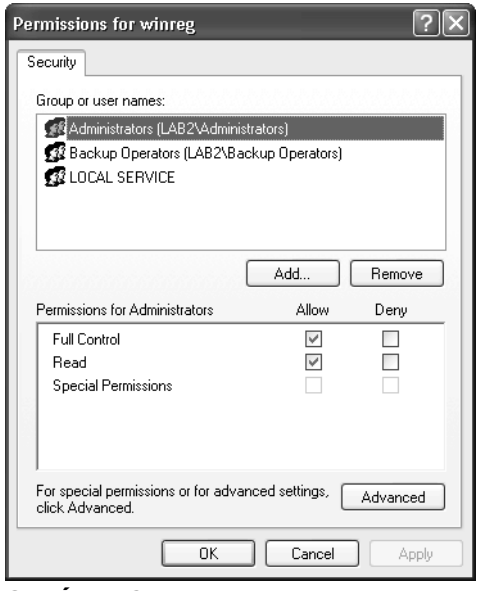
Windows XP Service Pack 2 (SP2) a Windows Server 2003 Service Pack 1 (SP1) nabízí velký počet nových funkcí zabezpečení. Například Windows Security Center pomáhá uživatelům s konfigurací zabezpečení na maximální úroveň ochrany. Windows Firewall brání nežádoucímu přístupu k počítačům, což umožňuje bezpečnější procházení sítí Internet a otevírání příloh elektronických zpráv. V této kapitole nebudeme tyto funkce probírat podrobně; místo toho si vysvětlíme, jak používat registr k jejich úpravám. Více informací o funkcích zabezpečení v opravném balíčku Windows XP SP2 získáte na internetové adrese `http://www.microsoft.com/windowsxp/sp2/default.mspx`. Další informace o funkcích zabezpečení v opravném balíčku Windows Server 2003 SP1 naleznete na internetové adrese `http://www.microsoft.com/technet/prodtechnol/windowsserver2003/servicepack/default.mspx`.

8.1 Nastavení oprávnění pro klíče

Zabezpečení registru se podobá zabezpečení systému souborů. Rozdíl je pouze v tom, že můžete nastavit pouze oprávnění pro klíče, ne pro hodnoty. Dialogová okna vypadají podobně, stejně jako oprávnění atd. Neznáte-li základní principy zabezpečení, věnujte nejdříve chvíli jejich přehledu v Help and Support Center. Základní principy v této kapitole nenaleznete, předpokládáme, že jste IT profesionálové a základy zabezpečení jsou vám tedy známé.

Pokud máte úplnou kontrolu nad klíčem registru nebo jej přímo vlastníte, můžete upravovat oprávnění pro uživatele a skupiny v seznamu ACL klíče:

1. V editoru `Regedit` klepněte na klíč se seznamem ACL, který chcete upravit.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění) (viz obrázek 8.1).
3. V seznamu Group Or User Names (Jméno skupiny nebo uživatele) klepněte na uživatele nebo skupinu, u kterých chcete upravit oprávnění, a poté označte zaškrtávací políčko ve sloupci Allow (Povolit) nebo Deny (Odepřít), čímž povolíte nebo zakážete tato oprávnění:
   - **Full Control (Úplné řízení).** Přidělí uživateli nebo skupině oprávnění pro otevření, úpravu a převzetí vlastnictví klíče. Toto oprávnění v podstatě dává úplnou kontrolu nad klíčem.
   - **Read (Číst).** Přidělí uživateli nebo skupině oprávnění pro čtení obsahu klíče, není však možné ukládat provedené změny. Toto oprávnění umožňuje *pouze čtení*.
   - **Special Permissions (Zvláštní oprávnění).** Přidělí uživateli nebo skupině speciální kombinaci oprávnění. Pro přidělení speciálních oprávnění klepněte na tlačítko Advanced (Upřesnit). O nastavení tohoto oprávnění se více dozvíte v části „Přiřazení speciálních oprávnění“ dále v této kapitole.



OBRÁZEK 8.1: Toto dialogové okno se téměř shoduje s dialogovým oknem pro zabezpečení systému souborů.

Zaškrtávací políčka v oblasti Permissions For (Oprávnění pro) *Název* někdy nejsou aktivní. Nemůžete je změnit. Důvodem je to, že klíč zdědí dané oprávnění z nadřazeného klíče. Dědičnosti oprávnění lze zabránit a postup se naučíte dále v této kapitole v části „Přiřazení speciálních oprávnění".

Tip Dobře, pohráli jste si. Upravili jste zabezpečení registru a uspokojili svou zvědavost; co teď? Původní oprávnění můžete snadno obnovit pomocí šablony Setup Security. S postupem se seznámíte v části „Úprava konfigurace počítače" dále v této kapitole.

Přidání uživatelů do seznamů ACL

Do existujícího seznamu ACL můžete přidat uživatele nebo skupiny:

1. V nástroji `Regedit` klepněte na klíč se seznamem ACL, který chcete upravit.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění) a klepněte na tlačítko Add (Přidat).
3. V dialogovém okně Select Users, Computers, Or Groups (Vyberte uživatele, počítače nebo skupiny) vyberte možnost Locations (Umístění) a poté klepněte na počítač, doménu nebo organizační jednotku, kde chcete vyhledat uživatele nebo skupinu pro přidání do seznamu ACL klíče.
4. Do pole Enter The Object Names To Select (Zadejte názvy objektů k výběru) zadejte název uživatele nebo skupiny, které chcete přidat do seznamu ACL klíče, a poté klepněte na tlačítko OK.
5. V seznamu Permissions For (Oprávnění pro) *Název* nastavte označením zaškrtávacího políčka Allow (Povolit) nebo Deny (Odepřít) oprávnění, které chcete přidělit uživateli či skupině.

Tip V kroku 4 zadáte celé jméno nebo část jména uživatele či skupiny pro přidání do seznamu ACL klíče. Neznáte-li jméno, můžete je vyhledat. Pokud je to možné, omezte své vyhledávání nejdříve zvolením umístění podle kroku 3. Poté klepněte na tlačítko Advanced a možnost Find Now. Vyberte název uživatele nebo skupiny pro přidání a klepněte na tlačítko OK. Výsledky můžete ještě více zúžit klepnutím na tlačítko Object Types a následným zrušením označení zaškrtávacího políčka Built-In Security Principals.

Přidání uživatelů do seznamu ACL klíče si dovedu představit jen v jednom skutečném případě, kdy povolíte skupině přístup k registru počítače prostřednictvím sítě (viz část „Zamezení vzdálenému přístupu k registru“ dále v této kapitole). Jinak je přidání uživatele či skupiny do seznamu ACL klíče vhodné pro rychlou opravu, pokud aplikace nemůže přistupovat k nastavení, která potřebuje při spuštění. Obecně řečeno způsobí přidání uživatelů nebo skupin do seznamu ACL klíče jen málo škody, nejste-li však opatrní, můžete otevřít mezery v zabezpečení systému Windows, kterými pak mohou uživatelé a hackeři projít. Jestliže budete muset danou úpravu provést u více než jednoho počítače nebo uživatele, měli byste zvážit její zavedení v podobě šablony zabezpečení. (Viz „Zavedení šablon zabezpečení“ dále v této kapitole.)

Odebrání uživatelů ze seznamů ACL

Uživatele nebo skupinu odeberete ze seznamu ACL klíče následujícím způsobem:

1. V nástroji `Regedit` klepněte na klíč se seznamem ACL, který chcete upravit.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění).
3. Určete uživatele či skupinu pro odebrání a klepněte na tlačítko Remove (Odebrat).

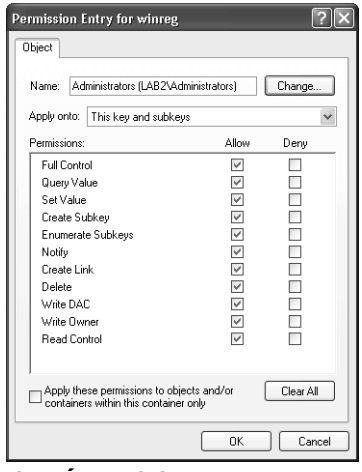
Upozornění Při odebírání skupin ze seznamů ACL klíčů buďte opatrní. Seznamy ACL, které v systému Windows vidíte po instalaci (Setup Security), představují zpravidla minimum vyžadované pro uživatele ke spuštění a používání operačního systému. Odstraníte-li z klíče skupinu Users nebo Power Users, nemohou uživatelé v daných skupinách číst hodnoty klíčů, což pravděpodobně povede k poškození operačního systému nebo aplikace. Pokud se odvážíte odebrat z klíče skupinu Administrators, možná nebudete moci spravovat počítač vůbec. Odebrání jednotlivých uživatelů ze seznamu ACL klíče však nemusí být nezbytně špatné. Systém Windows nepřiděluje oprávnění jednotlivým uživatelům, takže tato oprávnění mohla vzniknout chybně. Nikdy byste ale neměli odebírat uživatele ze seznamů ACL jejich podregistrů profilů. Jestliže tak učiníte, zabráníte jim v přístupu k jejich vlastním nastavením, nad kterými by měli mít úplnou kontrolu.

Přidělení speciálních oprávnění

Speciální oprávnění vám nabízejí větší kontrolu nad seznamem ACL klíče než základní oprávnění Full Control a Read. Uživatelům můžete povolit nebo zakázat schopnost vytvářet podklíče, nastavovat hodnoty, číst hodnoty atd. Můžete být velmi podrobní. Postupujte takto:

1. V nástroji `Regedit` klepněte na klíč se seznamem ACL, který chcete upravit.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění).
3. V seznamu Group Or User Names (Jméno skupiny nebo uživatele) určete uživatele či skupinu pro úpravu oprávnění. V případě potřeby přidejte uživatele nebo skupinu do seznamu. Poté klepněte na tlačítko Advanced (Upřesnit).

4. Poklepejte na skupinu nebo uživatele, kterému chcete přidělit speciální oprávnění. Zobrazí se dialogové okno Permissions For (Oprávnění pro) *Název*, které vidíte na obrázku 8.2.



OBRÁZEK 8.2: Speciální oprávnění vám dávají přesnější kontrolu nad oprávněními uživatele či skupiny. Přidělení speciálních oprávnění je však obvykle zbytečné.

5. V rozbalovacím seznamu Apply Onto (Použít pro) vyberte jednu z následujících možností:
   - **This Key Only (Pouze tento klíč).** Uplatní oprávnění pouze pro vybraný klíč.
   - **This Key And Subkeys (Tento klíč a podklíče).** Uplatní oprávnění pro vybraný klíč a všechny jeho podklíče. Jinými slovy, oprávnění budou použita pro celou větev.
   - **Subkeys Only (Pouze podklíče).** Uplatní oprávnění pro všechny podklíče, ale ne pro samotný klíč.
6. V seznamu Permissions (Oprávnění) označte zaškrtávací políčko Allow (Povolit) nebo Deny (Odepřít) pro každé oprávnění, které chcete povolit nebo zakázat:
   - **Full Control (Úplné řízení).** Všechna následující oprávnění.
   - **Query Value (Hodnota dotazu).** Čtení hodnoty z klíče.
   - **Set Value (Nastavit hodnotu).** Nastavení hodnoty v klíči.
   - **Create Subkey (Vytvořit podklíč).** Vytváření podklíčů v klíči.
   - **Enumerate Subkeys (Vytvářet výčty podklíčů).** Určení podklíčů klíče.
   - **Notify (Oznámit).** Příjem oznámení událostí z klíče.
   - **Create Link (Vytvářet propojení).** Vytváření symbolických odkazů v klíči.
   - **Delete (Odstranit).** Odstranění klíče nebo jeho hodnot.
   - **Write DAC (Zapsat DAC).** Zápis libovolného seznamu ACL klíče.
   - **Write Owner (Zapsat vlastníka).** Změna vlastníka klíče.
   - **Read Control (Řízení čtení).** Čtení libovolného seznamu ACL klíče.

Na tomto místě se musíme zmínit o dědičnosti. Je-li dědičnost povolena, podklíče zdědí oprávnění svých nadřazených klíčů. Jinými slovy, pokud dá klíč skupině úplné řízení, bude mít tato skupina kontrolu i nad všemi podklíči tohoto klíče. Když zobrazíte seznamy ACL podklíčů, je zaškrtávací políčko Allow (Povolit) vedle možnosti Full Control (Úplné řízení) pro danou skupinu neaktivní, protože nemůžete změnit zděděná oprávnění. Pro konfiguraci dědičnosti můžete učinit dvě věci. Můžete zabránit tomu, aby podklíč zdědil oprávnění svého nadřazeného klíče: V dialogovém okně Advanced Security Settings For *Klíč* zrušte označení zaškrtávacího políčka Inheritable Permission (Zděděná oprávnění). Můžete také nahradit seznamy ACL podklíčů, čímž efektivně obnovíte celou větev tak, aby odpovídala seznamu ACL klíče: Označte zaškrtávací políčko Replace Permission Entries On All Child Objects With Entries Shown Here That Apply To Child Objects (**Nahradit položky oprávnění ve všech podřízených objektech zde zobrazenými položkami platnými pro podřízený objekt**).

8.2 Mapování výchozích oprávnění

Seznámení s výchozími oprávněními registru je užitečné, pokud jste IT profesionálem, který nasazuje software. Budete-li vědět, zda členové skupiny Users mohou měnit určitá nastavení, pomůže vám to testovat aplikace před zavedením a zjistit, zda budou s výchozími oprávněními fungovat. Jestliže zjistíte, že aplikace pracuje s výchozími oprávněními správně, je připravena k zavedení. Pokud tomu tak nebude, musíte buď opravit program, nebo změnit příslušná oprávnění klíče. Nejjednodušším způsobem je samozřejmě použití šablon zabezpečení.

Nejdříve musíte znát tři základní skupiny v systému Windows: Users, Power Users a Administrators. Prostřednictvím těchto skupin nabízí systém Windows různé úrovně přístupu v závislosti na potřebách každé ze skupin:

- **Users.** Tato skupina má nejvyšší úroveň zabezpečení, protože její výchozí oprávnění neumožňují členům měnit data operačního systému nebo jiná uživatelská nastavení. Uživatelé v této skupině obecně nemohou měnit nastavení operačního systému a aplikací. Obvykle mezi ně patří programy určené pro systém Windows, které správci nasadí do počítačů uživatelů. Tato skupina také dává svým uživatelům úplnou kontrolu nad vším v uživatelských profilech, včetně podregistrů profilů (`HKCU`). IT profesionálové se často vyhýbají zařazení uživatelů do této skupiny, protože její členové obvykle nemohou spouštět starší aplikace. Než abyste zařazovali uživatele do jiné skupiny, měli byste tento problém řešit uplatněním kompatibilní šablony zabezpečení (viz část „Zavedení šablon zabezpečení“ dále v této kapitole).
- **Power Users.** Tato skupina poskytuje zpětnou kompatibilitu pro spuštěné programy, které nejsou certifikovány pro systém Windows. Výchozí oprávnění dávají této skupině schopnost změnit mnoho nastavení operačního systému a programů. Pokud používáte starší aplikace, které uživatelé nemohou spouštět jako členové skupiny Users, a nechystáte se využít šablony zabezpečení, měli byste uživatele přidat do skupiny Power Users a umožnit tak spouštění aplikací. Tato skupina však má dostatečná oprávnění pro instalaci většiny aplikací; členové nemohou změnit soubory operačního systému nebo instalovat služby.

Oprávnění přidělená členům skupiny Power Users jsou zhruba uprostřed mezi skupinami Users a Administrators. Podobá se skupině Users v systému Microsoft Windows NT 4.0, ovšem členové této skupiny se opravdu nemohou sami přidat do skupiny Administrators.

- **Administrators.** Tato skupina poskytuje úplnou kontrolu nad celým počítačem. Její členové mohou změnit soubory operačního systému a aplikací. Mohou změnit všechna nastavení v registru. Také mohou převzít vlastnictví nad klíči a změnit seznam ACL klíče. IT profesionálové mají často tendence přidat uživatele do této skupiny, aby se vyhnuli potížím při zavedení aplikací, jejichž instalace by jinak byla složitá. To byste však neměli dělat. Protože uživatelé v této skupině mohou na svůj počítač cokoli instalovat nebo změnit libovolné nastavení, mají viry široké pole působnosti a zároveň může dojít k lidské chybě. Abyste zabezpečili počítače v podnikovém prostředí a zkrátili dobu nečinnosti, ponechejte tuto skupinu pro skutečné správce. Přestože jste sami správcem, používejte ze stejných důvodů svůj počítač jako člen skupiny Power Users. Potřebujete-li provést určitý úkol správy, použijte sekundární přihlášení pro spuštění programu jako člen skupiny Administrators: stiskněte klávesu Shift a přitom klepněte pravým tlačítkem myši na zástupce programu, zvolte příkaz `Run As` a poté zadejte jméno a heslo účtu, který chcete použít ke spuštění programu.

Tabulka 8.1 popisuje výchozí oprávnění registru po čisté instalaci systému Windows. (Tato oprávnění neplatí pro řadiče domény serveru Windows 2003 Server.) Nezapomínejte, že výsledná oprávnění se liší v případě, že přecházíte ze starší verze systému Windows na verzi Windows XP nebo Windows Server 2003. Uváděná oprávnění jsou ze šablony zabezpečení, kterou použijete k obnovení systému Windows. Zaměřil jsem se na skupiny Users a Power Users, protože jsou primárním aspektem. Ve většině těchto případů má skupina Administrators úplné řízení, stejně jako vestavěné účty Creator Owner a System. Většinou – ne však vždy – nahrazují oprávnění klíče všechna oprávnění podklíčů. Děje se tak díky dědičnosti, s kterou jste se seznámili v předchozí části.

Když ve sloupci Power Users uvidíte slovo *Special*, znamená to, že skupina má v daném klíči zvláštní oprávnění (a většinou v podklíčích) a obvykle se jedná o schopnost upravovat hodnoty. Skupina Power Users však nezíská oprávnění Full Control (Úplné řízení), Create Link (Vytvořit propojení), Change Permissions (Oprávnění) nebo Take Ownership (Převzít vlastnictví) pro některý z klíčů v registru. Na této tabulce je zajímavé to, že systém Windows dává skupině Users oprávnění Read a skupině Power Users speciální oprávnění pro všechny položky `HKLM\SOFTWARE`. Zbývající údaje v tabulce jsou výjimkou tohoto pravidla, které omezují přístup k určitým klíčům v `HKLM\SOFTWARE`.

TABULKA 8.1: Výchozí oprávnění registru v systému Windows

Větev	Users	Power Users
hklm\software	Read	Special
hklm\software\classes	Read	Special
hklm\software\classes\.hlp	Read	Read
hklm\software\classes\helpfile	Read	Read

Větev	Users	Power Users
hklm\software\microsoft\ads\providers\ldap\extensions	Read	Read
hklm\software\microsoft\ads\providers\nds	Read	Read
hklm\software\microsoft\ads\providers\nwcompat	Read	Read
hklm\software\microsoft\ads\providers\winnt	Read	Read
hklm\software\microsoft\command processor	Read	Read
hklm\software\microsoft\cryptography	Read	Read
hklm\software\microsoft\cryptography\calais	None	None
hklm\software\microsoft\driver signing	Read	Read
hklm\software\microsoft\enterprisecertificates	Read	Read
hklm\software\microsoft\msdtc	None	None
hklm\software\microsoft\netdde	None	None
hklm\software\microsoft\non-driver signing	Read	Read
hklm\software\microsoft\ole	Read	Read
hklm\software\microsoft\protected storage system provider	None	None
hklm\software\microsoft\rpc	Read	Read
hklm\software\microsoft\secure	Read	Read
hklm\software\microsoft\systemcertificates	Read	Read
hklm\software\microsoft\upnp device host	Read	None
hklm\software\microsoft\windows nt\currentversion\accessibility	Read	Read
hklm\software\microsoft\windows nt\currentversion\aedebug	Read	Read
hklm\software\microsoft\windows nt\currentversion\asr\commands	Read	Read
hklm\software\microsoft\windows nt\currentversion\classes	Read	Read
hklm\software\microsoft\windows nt\currentversion\drivers32	Read	Read
hklm\software\microsoft\windows nt\currentversion\efs	Read	Read
hklm\software\microsoft\windows nt\currentversion\font drivers	Read	Read
hklm\software\microsoft\windows nt\currentversion\fontmapper	Read	Read
hklm\software\microsoft\windows nt\currentversion\ image file execution options	Read	Read
hklm\software\microsoft\windows nt\currentversion\inifilemapping	Read	Read
hklm\software\microsoft\windows nt\currentversion\perflib	None	None
hklm\software\microsoft\windows nt\currentversion\perflib\009	None	None
hklm\software\microsoft\windows nt\currentversion\profilelist	Read	Read
hklm\software\microsoft\windows nt\currentversion\secedit	Read	Read
hklm\software\microsoft\windows nt\currentversion\setup\recoveryconsole	Read	Read

Větev	Users	Power Users
hklm\software\microsoft\windows nt\currentversion\svchost	Read	Read
hklm\software\microsoft\windows nt\currentversion\terminal server\install\software\microsoft\windows\currentversion\runonce	Read	Read
hklm\software\microsoft\windows nt\currentversion\time zones	Read	Read
hklm\software\microsoft\windows nt\currentversion\windows	Read	Read
hklm\software\microsoft\windows nt\currentversion\winlogon	Read	Read
hklm\software\microsoft\windows\currentversion\explorer\ user shell folders	Read	Read
hklm\software\microsoft\windows\currentversion\group policy	None	None
hklm\software\microsoft\windows\currentversion\installer	None	None
hklm\software\microsoft\windows\currentversion\policies	None	None
hklm\software\microsoft\windows\currentversion\reliability	Read	Read
hklm\software\microsoft\windows\currentversion\runonce	Read	Read
hklm\software\microsoft\windows\currentversion\runonceex	Read	Read
hklm\software\microsoft\windows\currentversion\telephony	Read	Special
hklm\software\policies	Read	Read
hklm\system	Read	Read
hklm\system\clone	None	None
hklm\system\controlset001	None	None
hklm\system\controlset001\services\dhcp\configurations	Read	Read
hklm\system\controlset001\services\dhcp\parameters	Read	Read
hklm\system\controlset001\services\dhcp\parameters\options	Read	Read
hklm\system\controlset001\services\dnscache\parameters	Read	Read
hklm\system\controlset001\services\mrxdav\encrypteddirectories	None	None
hklm\system\controlset001\services\netbt\parameters	Read	Read
hklm\system\controlset001\services\netbt\parameters\interfaces	Read	Read
hklm\system\controlset001\services\tcpip\linkage	Read	Read
hklm\system\controlset001\services\tcpip\parameters	Read	Read
hklm\system\controlset001\services\tcpip\parameters\adapters	Read	Read
hklm\system\controlset001\services\tcpip\parameters\interfaces	Read	Read
hklm\system\controlset002	None	None
hklm\system\controlset003	None	None
hklm\system\controlset004	None	None
hklm\system\controlset005	None	None
hklm\system\controlset006	None	None

Větev	Users	Power Users
hklm\system\controlset007	None	None
hklm\system\controlset008	None	None
hklm\system\controlset009	None	None
hklm\system\controlset010	None	None
hklm\system\currentcontrolset\control\class	None	None
hklm\system\currentcontrolset\control\keyboard layout	Read	Read
hklm\system\currentcontrolset\control\keyboard layouts	Read	Read
hklm\system\currentcontrolset\control\network	Read	Read
hklm\system\currentcontrolset\control\securepipeservers\winreg	None	None
hklm\system\currentcontrolset\control\session manager\executive	None	Special
hklm\system\currentcontrolset\control\timezoneinformation	None	Special
hklm\system\currentcontrolset\control\wmi\security	None	None
hklm\system\currentcontrolset\enum	None	None
hklm\system\currentcontrolset\hardware profiles	None	None
hklm\system\currentcontrolset\services\appmgmt\security	None	None
hklm\system\currentcontrolset\services\clipsrv\security	None	None
hklm\system\currentcontrolset\services\cryptsvc\security	None	None
hklm\system\currentcontrolset\services\dnscache	Read	Read
hklm\system\currentcontrolset\services\ersvc\security	None	None
hklm\system\currentcontrolset\services\eventlog\security	None	None
hklm\system\currentcontrolset\services\irenum\security	None	None
hklm\system\currentcontrolset\services\netbt	Read	Read
hklm\system\currentcontrolset\services\netdde\security	None	None
hklm\system\currentcontrolset\services\netddedsdm\security	None	None
hklm\system\currentcontrolset\services\remoteaccess	Read	Read
hklm\system\currentcontrolset\services\rpcss\security	None	None
hklm\system\currentcontrolset\services\samss\security	None	None
hklm\system\currentcontrolset\services\scarddrv\security	None	None
hklm\system\currentcontrolset\services\scardsvr\security	None	None
hklm\system\currentcontrolset\services\stisvc\security	None	None
hklm\system\currentcontrolset\services\sysmonlog\log queries	None	None
hklm\system\currentcontrolset\services\tapisrv\security	None	None
hklm\system\currentcontrolset\services\tcpip	Read	Read
hklm\system\currentcontrolset\services\w32time\security	None	None
hklm\system\currentcontrolset\services\wmi\security	None	None

Větev	Users	Power Users
hku\.default	Read	Read
hku\.default\software\microsoft\netdde	None	None
hku\.default\software\microsoft\protected storage system provider	None	None
hku\.default\software\microsoft\systemcertificates\root\protectedroots	None	None

Zjišťování klíčů, které aplikace používá, je částečně věda, ale spíše umění. Někdy jednoduše otevřu binární soubor programu v textovém editoru a vyhledám řetězce vypadající jako klíče. Ke sledování aktivity při spuštění programu nejčastěji používám nástroj, jako je Winternals Registry Monitor (`Regmon`), s nímž se seznámíte v kapitole 10, „Vyhledávání nastavení v registru“. Poté zaznamenám různé klíče, na které program odkazuje, a zjistím, zda pro dané klíče měla požadovaná oprávnění skupina Users nebo Power Users. Dobře fungující aplikace hlásí chyby, když nemohou číst nebo zapisovat hodnotu do registru. Na toto chování bych se však příliš nespoléhal, protože nesprávně pracující programy pokračují ve své činnosti i po zjištění chyby v registru.

8.3 Převzetí vlastnictví klíčů

Systém Windows implicitně přiřazuje vlastnictví k `HKLM` a `HKCU` následujícím způsobem:

- Správci vlastní všechny podklíče v `HKLM`.
- Uživatelé vlastní všechny podklíče ve svých podregistrech profilů, `HKCU`.

Máte-li úplnou kontrolu nad klíčem (což správci obvykle mají), můžete převzít jeho vlastnictví, pokud již nejste vlastníkem:

1. V nástroji `Regedit` klepněte na klíč, jehož vlastnictví chcete převzít.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění); poté klepněte na tlačítko Advanced (Upřesnit).
3. Na kartě Owner (Vlastník) vyberte nového vlastníka a klepněte na tlačítko OK.

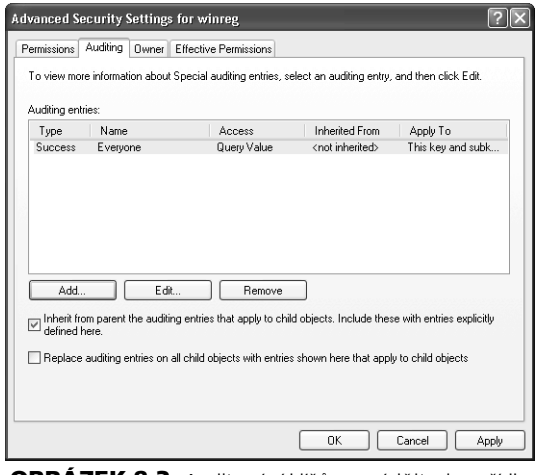
8.4 Auditování přístupu k registru

Auditování přístupu k registru je skvělý způsob sledování nastavení v registru a jde také o jednu z metod, které se budeme věnovat v kapitole 10, „Vyhledávání nastavení v registru“. Můžete tak sledovat přístup k citlivým nastavením. Problémem při auditování registru je to, že musíte příslušný klíč určit velmi specificky nebo obětovat výkon kvůli auditování velké části registru. Je to kompromis mezi získáním potřebných informací a dlouhotrvajícím procházením registru.

Auditování klíče je třífázový proces. Nejdříve musíte povolit možnost Audit Policy. Můžete tak učinit v síti prostřednictvím Group Policy, to však velmi ovlivní výkon. Pokud vám auditování slouží jako nástroj při řešení potíží nebo ke zjišťování nastavení, zapněte možnost Audit Policy místně. V okně Control Panel – Ovládací panely (zobrazení Classic) otevřete složku Administrative Tools (Nástroje pro správu) a spusťte Local Security Policy (Místní zásady zabezpečení). Local Security Policy

nenaleznete na řadiči domény. V levém podokně pod položkou Local Policies (Místní zásady) klepněte na Audit Policy (Zásady auditu). V pravém podokně poklepejte na možnost Audit Object Access (Auditovat činnosti s objekty) a poté označte zaškrtávací políčka Success (Úspěšný) a Failure (Neúspěšný). Poté co povolíte Audit Policy, použijte `Regedit` k auditování jednotlivých klíčů následujícím způsobem:

1. V nástroji `Regedit` klepněte na klíč, který chcete auditovat.
2. V nabídce Edit (Úpravy) zvolte příkaz Permissions (Oprávnění); poté klepněte na tlačítko Advanced (Upřesnit).
3. Na kartě Auditing (viz obrázek 8.3) klepněte na tlačítko Add (Přidat).
4. V dialogovém okně Select Users, Computers, Or Groups (Vyberte uživatele, počítače nebo skupiny) klepněte na možnost Locations (Umístění) a vyberte počítač, doménu nebo organizační jednotku pro vyhledání skupiny nebo uživatele, jehož chcete auditovat.
5. Do pole Enter The Object Names To Select (Zadejte názvy objektů k výběru) zadejte jméno uživatele nebo skupiny pro přidání do seznamu auditování klíče. Potom klepněte na tlačítko OK.



OBRÁZEK 8.3: Auditování klíčů provádějte jen zřídka, protože tím můžete značně ovlivnit výkon.

6. V dialogovém okně Auditing Entry For *Název* označte v seznamu Access obě zaškrtávací políčka Successful a Failed vedle činností, u kterých chcete auditovat úspěšné i neúspěšné pokusy. Tyto možnosti odpovídají oprávněním, s nimiž jste se seznámili v části „Přiřazování speciálních oprávnění“ dříve v této kapitole:
   - Full Control (Úplné řízení)
   - Query Value (Hodnota dotazu)
   - Set Value (Nastavit hodnotu)
   - Create Subkey (Vytvořit podklíč)
   - Enumerate Subkeys (Vytvářet výčty podklíčů)
   - Notify (Oznámit)

- Create Link (Vytvářet propojení)
- Delete (Odstranit)
- Write DAC (Zapsat DAC)
- Write Owner (Zapsat vlastníka)
- Read Control (Řízení čtení)

Když povolíte Audit Policy a auditujete určité klíče, zkontrolujte výsledky pomocí prohlížeče Event Viewer (Prohlížeč událostí). V okně Control Panel (zobrazení Classic) otevřete složku Administrative Tools a spusťte Event Viewer. V levém podokně klepněte na možnost Security. V pravém podokně uvidíte všechny položky, přičemž ty nejnovější jsou v horní části seznamu. Pro zobrazení dalších informací poklepejte na kteroukoli z položek. Dialogové okno Event Properties udává, jaký typ přístupu systém Windows zjistil, typ objektu a proces, který přistoupil ke klíči nebo hodnotě. V kapitole 10, „Vyhledávání nastavení v registru", se dozvíte, jak tyto informace využít ke zjištění, kde systém Windows nebo program ukládá určitá nastavení v registru.

8.5 Zamezení místnímu přístupu k registru

S tématem zabezpečení registru vyvstává nevyhnutelná otázka, jak zabránit uživatelům v přístupu k registru. Není to možné. Nezapomínejte, že registr obsahuje nastavení, která musí být uživateli k dispozici, aby systém Windows pracoval správně. Uživatelé také musí mít úplnou kontrolu nad svými podregistry profilů, aby aplikace a operační systém mohly ukládat jejich nastavení. Nemůžete zabránit přístupu – ani to nechcete. Při nejlepším byste měli doufat, že se podaří omezit možnost uživatelů upravovat registr prostřednictvím nástroje `Regedit` nebo jiných editorů registru.

Nejvhodnějším způsobem zamezení přístupu k nástroji `Regedit` je povolení zásady `Prevent access to registry editing tools`. Když uživatel spustí `Regedit`, uvidí pouze chybovou zprávu s informací „Registry editing has been disabled by your administrator". Problémem této zásady je to, že ne všechny editory registru tuto zásadu respektují. Odhodlanému uživateli nic nezabrání ve stažení a používání sharewarového editoru registru, kterých je k dispozici mnoho. Další možností je využití zásad Software Restriction Policies (Zásady omezení softwaru), o nichž se více dozvíte v nápovědě Help and Support Center. Ani to však nezabrání uživatelům ve spouštění sharewarových editorů registru, pokud nepoužijete zásady Software Restriction Policies, díky kterým lze vytvořit krátký seznam přípustných aplikací.

8.6 Zamezení vzdálenému přístupu k registru

Zabezpečení místního přístupu k registru Windows je jedna věc; zabezpečení vzdáleného přístupu věc druhá. Windows nabízí členům místních skupin Administrators a Backup Operators vzdálený přístup k registru. Protože skupina Domain Admins je členem každé z místních skupin Administrators, mohou se všichni správci domén

připojit k registru kteréhokoli počítače připojeného k doméně. Systém Windows nyní také omezuje vzdálený přístup k registru více než starší verze.

Existuje jen omezený počet případů, kdy budete chtít umožnit vzdálený přístup k registrům počítačů. Například v Active Directory můžete vytvořit skupinu správců pro každou organizační jednotku a umožnit jí úpravu registrů počítačů, které náleží do příslušné organizační jednotky. Chcete-li určité skupině povolit vzdálený přístup k registru, přidejte ji do seznamu ACL klíče `HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`. Problém tohoto postupu spočívá v tom, že ačkoli přidání skupiny do klíče `winreg` umožní vzdálený přístup, seznam ACL každého klíče stále určuje, které klíče může skupina změnit. Abyste tedy povolili vzdálenému uživateli nebo skupině změnit nastavení v počítači, přidejte daného uživatele či skupinu do místní skupiny Users, Power Users nebo Administrators.

Upozornění Kvůli zabezpečení nezpřístupňujte registr všech počítačů neuváženým přidáváním skupin do seznamu ACL klíče winreg. Pokud tak učiníte, způsobíte dostatečný prostor velkému množství virů (tzv. Trojanů), které ohrozí systém Windows a zajistí hackerům přístup do vaší infrastruktury. Nejlepší je omezit vzdálený přístup k registrům pouze na správce domén.

8.7 Zavedení šablon zabezpečení

K vytváření a uplatnění šablon slouží mnoho různých nástrojů. Šablony zabezpečení nejdříve použijete k vytvoření a úpravě šablon. K uplatnění šablon pak použijete konzolu Security Configuration And Analysis nebo Group Policy. Tato část vás provede procesem použití těchto nástrojů, počínaje vytvořením konzoly Microsoft Management Console (MMC), která bude sloužit k úpravám šablon, a konče zavedením šablon v síti.

Začneme vysvětlením různých nastavení zabezpečení v šabloně. Následující seznam uvádí kategorie nastavení, s kterými se setkáte v šabloně zabezpečení. Za jednotlivými kategoriemi naleznete možnosti, které v kategoriích můžete definovat.

- **Account Policies.** Password Policy, Account Lockout Policy a Kerberos Policy (Zásady účtů – Zásady hesel, Zásady uzamčení účtů, Zásady modulu Kerberos)
- **Local Policies.** Audit Policy, User Rights Assignment a Security Options (Místní zásady – Zásady auditu, Přiřazení uživatelských práv, Možnosti zabezpečení)
- **Event Log.** Nastavení Application, System a Security Event Log (Protokol událostí – Aplikace, Systém, Zabezpečení)
- **Restricted Groups.** Členství ve skupinách citlivých na zabezpečení (Skupiny s omezeným členstvím)
- **System Services.** Spouštění a oprávnění pro systémové služby (Služby systému)
- **Registry.** Oprávnění pro klíče registru (téma této části)
- **File System.** Oprávnění pro soubory a složky (Souborový systém)

Šablony zabezpečení nejsou ničím jiným než textovými soubory s příponou `.inf`. Můžete je kopírovat, upravovat atd. Soubor INF se podobá souboru INI. Můžete vytvořit vlastní šablony zabezpečení, což vám však nedoporučuji, protože je to náročná práce s velkým rizikem. Máte také možnost upravit jednu z předdefinovaných šablon, které

jsou k dispozici v systému Windows. Tento druhý postup je rozhodně vhodnější, protože je pro vaši práci téměř vše připraveno. Pamatujte si, že oprávnění měnit výchozí šablonu zabezpečení (`%SystemRoot%\Security\Templates`) má pouze skupina Administrators, a jen správci tedy mohou upravovat a uplatňovat šablony zabezpečení.

Další informace Ke skriptování změn v zabezpečení registru můžete použít nástroj `Regini.exe` dodávaný společně se systémem Windows. Jeho použití je snadné a někdy užitečné k provedení změn v seznamech ACL klíčů z přihlašovacích skriptů. Jde o starší nástroj, který však postupně nahrazují výkonnější funkce zabezpečení v systému Windows. Více informací o nástroji `Regini.exe` naleznete na internetových adresách `http://support.microsoft.com/kb/264584` a `http://support.microsoft.com/?kbid=237607`.

Vytvoření konzoly pro správu zabezpečení

Abyste si usnadnili práci, vytvořte konzolu MMC, která nabízí všechny nástroje potřebné pro upravování, analýzy a uplatnění šablon zabezpečení:

1. Klepněte na tlačítko Start a zvolte příkaz `Run`; poté zadejte `mmc` a klepněte na tlačítko OK.
2. V nabídce File (Soubor) zvolte příkaz Add/Remove Snap-in (Přidat nebo odebrat modul snap-in).
3. V dialogovém okně Add/Remove Snap-in (Přidat nebo odebrat modul snap-in) klepněte na tlačítko Add (Přidat).
4. V dialogovém okně Add Standalone Snap-in (Přidat samostatný modul snap-in) vyberte možnost Security Templates (Šablony zabezpečení) a klepněte na tlačítko Add (Přidat).
5. Zvolte položku Configuration And Analysis (Konfigurace a analýzy) a klepněte na tlačítko Add (Přidat).
6. Klepněte na tlačítko Close (Zavřít) a poté na tlačítko OK.

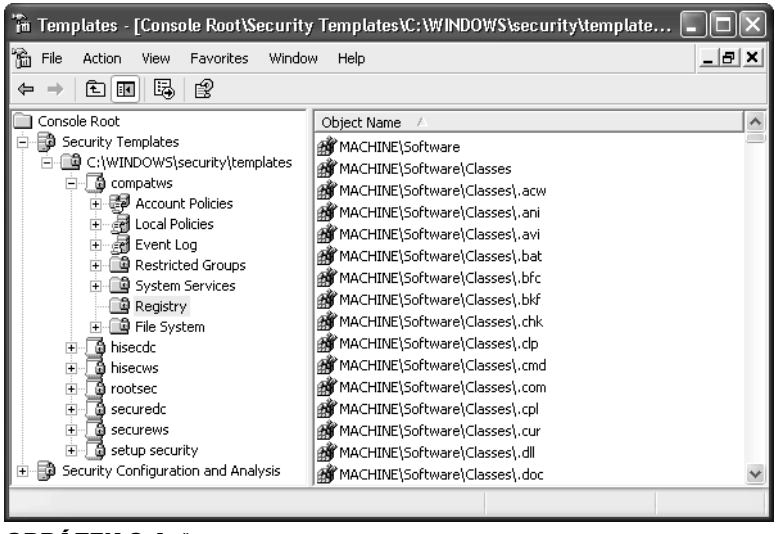
Po vytvoření uložte konzolu do souboru pro rychlý přístup. V nabídce File zvolte příkaz Save. Soubor můžete nazvat například `Templates.msc`. MMC uloží váš soubor do složky Administrative Tools. Budete-li chtít soubor rychle otevřít, klepnete na tlačítko Start, přejdete na All Programs, Administrative Tools a poté zvolíte položku Templates (podle vámi zvoleného názvu). Obrázek 8.4 ukazuje konzolu vytvořenou podle popisu v této části.

Výběr předdefinované šablony zabezpečení

V systému Windows je k dispozici několik předdefinovaných šablon zabezpečení. Téměř nikdy nemusíte vytvářet novou šablonu, protože obvykle stačí upravit jednu z těchto předdefinovaných šablon a uložit ji do jiného souboru. Slouží jako výchozí bod pro uplatňování zásad zabezpečení v různých případech, ať již se to týká jednoho, stovky nebo tisíce počítačů. Následující předdefinované zásady zabezpečení implicitně naleznete ve složce `%SystemRoot%\Security\Templates`:

- **Default security (Setup security.inf).** Tato šablona obsahuje výchozí nastavení zabezpečení, která jsou uplatněna při instalaci systému Windows. Patří sem také oprávnění pro systém souborů a registr. Potřebujete-li informace o výchozích oprávněních operačního systému, naleznete je zde. Tuto šablonu můžete

použít k obnovení původních nastavení zabezpečení Windows prostřednictvím Security Configuration And Analysis, nenasazujte ji však pomocí Group Policy.



OBRÁZEK 8.4: Šablony vytváříte v SecurityTemplates a poté je analyzujete prostřednictvím Security Configuration And Analysis

- **Compatible (Compatws.inf).** Tato šablona obsahuje nastavení zabezpečení, která uvolňují omezení pro skupinu Users tak, aby uživatelé mohli spouštět starší aplikace. Jde o vhodnější postup než přeřazení uživatelů ze skupiny Users do skupiny Power Users, nebo dokonce Administrators. Tato šablona změní oprávnění pro systém souborů a registr přidělená skupině Users tak, že jsou konzistentní se staršími a jinými aplikacemi, které nejsou certifikované pro systém Windows. Šablona také předpokládá, že správce nechce zařazovat uživatele do skupiny Power Users, a proto přemisťuje uživatele ze skupiny Power Users do skupiny Users. Tato šablona je určena pouze pro pracovní stanice a neměli byste ji uplatňovat pro servery.
- **DC Security (DC Security.inf).** Tato šablona se vytvoří, když je server povýšen na řadič domény. Odráží výchozí nastavení zabezpečení souborů, registru a systémových služeb. Pokud tuto šablonu znovu uplatníte, nastavení se vrátí na původní hodnoty. Šablona však může potlačit oprávnění u nových souborů, klíčů registru a systémových služeb vytvořených jinými programy.
- **Secure (Secure*.inf).** Tyto šablony jsou spojeny s nastaveními zabezpečení, která nejméně ovlivňují kompatibilitu aplikací. Šablona `Securedc.inf` je určena pro řadiče domén a šablona `Securews.inf` se používá pro pracovní stanice. Uplatňuje například nastavení využívání hesel, uzamčení a auditování. Omezuje také uživatele ověřovacích protokolů LAN Manager a Windows NT LAN Manager (NTLM) konfigurací systému Windows tak, aby odesílal pouze odpovědi NTLM version 2 (NTLMv2), a konfigurací serverů, aby odmítaly odpovědi protokolu LAN Manager. Tato šablona zabraňuje anonymním uživatelům, aby zjišťovali názvy účtů, sdílené položky a překládali identifikátory SID (Security

Identifier) (viz kapitola 1, „Základy registru“). Před zavedením tuto šablonu pečlivě otestujte.

- **Highly Secure (Hisec*.inf).** Tyto šablony jsou nadřazené všem předchozím šablonám a uplatňují ještě více omezení. Šablona `Hisecdc.inf` je určena pro řadiče domény a šablona `Hisecws.inf` pro pracovní stanice. Tato šablona například nastavuje úrovně šifrování a podepisování, které systém Windows vyžaduje pro ověřování a přemisťování dat prostřednictvím zabezpečených kanálů. Vyžaduje výkonné šifrování a podepisování. Odebírá členy ze skupin Power Users a zajišťuje, aby ke členům místní skupiny Administrators patřily pouze skupiny Domain Admins a Administrators. Otestujte šablony, abyste zajistili kompatibilitu s vaší infrastrukturou a aplikacemi, protože po uplatnění této šablony bude pravděpodobně možné spouštět pouze certifikované aplikace.
- **System root security (Rootsec.inf).** Tato šablona definuje kořenová oprávnění pro systém souborů Windows. Neobsahuje žádná oprávnění registru. Uplatňuje oprávnění pro kořenovou jednotku `%SystemDrive%`. Tuto šablonu můžete použít k obnovení těchto oprávnění kořenové jednotky systému nebo k uplatnění stejných oprávnění na dalších svazcích.
- **No Terminal Server user SID (Notssid.inf).** Tato šablona odebírá nepotřebné identifikátory Terminal Server SID ze systému souborů a registru, pokud je spuštěn Terminal Server v kompatibilním režimu aplikací. Je-li to možné, spusťte Terminal Server raději v režimu úplného zabezpečení, ve kterém není identifikátor Terminal Server SID použit vůbec.

Tyto šablony zabezpečení jsou většinou přírůstkové. Upravují výchozí nebo existující nastavení zabezpečení v počítači, jsou-li tato nastavení již nakonfigurovaná. Na rozdíl od šablony Setup Security nekonfigurují výchozí nastavení zabezpečení před změnou konfigurace zabezpečení počítače. Šablony zabezpečení také nelze použít k zabezpečení systému Windows v případě, že používáte systém souborů FAT.

Šablony tohoto typu můžete zobrazit v konzole MMC. V levém podokně poklepejte na šablonu zabezpečení, čímž ji otevřete. Šablony jsou implicitně uloženy ve složce `C:\Windows\Security\Templates`, jak je vidět v uzlu Security Templates v konzole. Můžete jim však přidělit jinou cestu. Klepněte pravým tlačítkem myši na šablonu Security Templates a zvolte příkaz New Template Search Path. V oblasti Security Templates uvidíte předchozí i novou cestu. Chcete-li odebrat cestu ze složky Security Templates, klepněte na ni pravým tlačítkem myši a vyberte příkaz Delete.

Vytvoření vlastní šablony zabezpečení

Vlastní šablonu zabezpečení můžete vytvořit složitým postupem:

1. Ve složce Security Templates (Šablony zabezpečení) klepněte pravým tlačítkem myši na složku, ve které chcete vytvořit novou šablonu, a zvolte příkaz New Template (Název šablony).
2. Do pole New Template (Název šablony) zadejte název nové šablony a do pole Description (Popis) napište stručný, ale užitečný popis nové šablony. Poté klepněte na tlačítko OK.

3. V levém podokně poklepejte na novou šablonu zabezpečení pro její otevření. Vyberte oblast zabezpečení, například Registry, a v pravém podokně nakonfigurujte nastavení zabezpečení dané oblasti.

Tento postup však podle mého názoru není vhodný. Především je příliš náročný na laboratorní testování a navíc je náchylný k chybám. Nejlepším způsobem vytvoření šablony zabezpečení je využít jednu z předdefinovaných šablon, uložit ji do nového souboru a poté ji upravit – opatrně. Při své práci jsem většinou začínal souborem šablony `Compatws.inf` a upravil ji podle potřeby, aby i starší aplikace měly dostatek prostoru ke své práci. Postupujte takto:

1. Ve složce Security Templates poklepejte na položku `C:\Windows\Security\Templates`.
2. Pravým tlačítkem myši klepněte na předdefinovanou šablonu, kterou chcete upravit. Klepněte na tlačítko Save As, zadejte nový název pro šablonu zabezpečení a klepněte na tlačítko Save.
3. V levém podokně poklepejte na novou šablonu zabezpečení pro její otevření. Vyberte oblast zabezpečení, například Registry, a v pravém podokně nakonfigurujte nastavení zabezpečení dané oblasti.

Protože tato kniha pojednává o registru, měli byste se dozvědět podrobnější informace o konfiguraci zabezpečení registru v šabloně. V levém podokně Security Templates poklepejte na svou šablonu a poté zvolte možnost Registry. V pravém podokně se zobrazí seznam klíčů registru. Pro přidání klíče do seznamu klepněte pravým tlačítkem myši na Registry a zvolte příkaz Add Key. Protože jsou v seznamu uvedeny všechny klíče `HKLM`, přidejte výjimky k nastavení, která šablona definuje pro `HKLM\SOFTWARE` a `HKLM\SYSTEM`. Při úpravě nastavení poklepejte na klíč a vyberte jednu z následujících možností:

- **Configure This Key Then (Zkonfigurovat tento klíč a provést následující akci).** Po výběru této položky vyberte jednu z následujících možností:
  - **Propagate Inheritable Permissions To All Subkeys (Použít zděděná oprávnění na všechny podklíče).** Podklíče zdědí nastavení zabezpečení klíče za předpokladu, že nastavení zabezpečení podklíčů neblokují dědičnost. V případě konfliktu potlačí oprávnění podklíče zděděná oprávnění od nadřazeného klíče.
  - **Replace Existing Permissions On All Subkeys With Inheritable Permissions (Nahradit existující oprávnění ke všem souborům a podsložkám dědičnými oprávněními).** Oprávnění klíče potlačí oprávnění všech podklíčů. Jinými slovy, oprávnění každého z podklíčů budou identická s oprávněními nadřazeného klíče. Zvolíte-li tuto možnost a uplatníte šablonu, změna je trvalá, pokud ji nezměníte prostřednictvím jiné šablony v registru.
  - **Do Not Allow Permissions On This Key To Be Replaced (Nepovolit přepis oprávnění k tomuto klíči).** Tuto možnost vyberte, pokud nechcete konfigurovat oprávnění klíče nebo jeho podklíčů.

Chcete-li upravit oprávnění, která má šablona uplatnit v klíči, klepněte na Edit Security. Můžete tak učinit ve stejném dialogovém okně Security For *Název*, které jste viděli dříve v této kapitole. Máte možnost přidávat a odebírat skupiny. Můžete po-

volit nebo zakázat oprávnění pro různé uživatele a skupiny k provádění různých úkolů. Lze také auditovat přístup uživatelů a skupin ke klíči. Můžete změnit vlastnictví klíče. Když uplatníte šablonu pro počítač nebo ji nasadíte prostřednictvím Group Policy, klíč obdrží oprávnění definovaná v tomto dialogovém okně.

Analýza konfigurace počítače

Jakmile máte připravenou vlastní šablonu, můžete ji použít k analýze konfigurace zabezpečení počítače. Nástroj Security Configuration And Analysis (Konfigurace a analýza zabezpečení) vám umožňuje porovnat aktuální stav konfigurace zabezpečení počítače s nastaveními definovanými v šabloně. Tento nástroj můžete použít k provedení okamžitých změn v konfiguraci počítače, například při řešení potíží. Může také sloužit ke sledování a zajištění určité úrovně zabezpečení jako součást programu rizikového řízení podniku prostřednictvím zjišťování vzniklých mezer v zabezpečení.

Nástroj Security Configuration And Analysis můžete k analýze zabezpečení počítače použít následujícím způsobem:

1. Pravým tlačítkem myši klepněte na nástroj Security Configuration And Analysis, který jste přidali do konzoly v části s názvem „Vytvoření konzoly pro správu zabezpečení“ dříve v této kapitole, a klepněte na tlačítko Open Database.
2. V dialogovém okně Open Database máte dvě možnosti:
   - Pro vytvoření nové databáze pro analýzu zadejte do pole File Name název nové databáze a klepněte na tlačítko Open. V dialogovém okně Import Template vyberte šablonu a klepněte na tlačítko Open.
   - Pro otevření existující databáze pro analýzu zadejte do pole File Name název existující databáze a klepněte na tlačítko Open.
3. Pravým tlačítkem myši klepněte na nástroj Security Configuration And Analysis, zvolte příkaz Analyze Computer Now a poté přijměte výchozí cestu souboru protokolu nebo určete jinou.

Nástroj Security Configuration And Analysis porovná aktuální zabezpečení počítače s databází pro analýzu. Pokud do databáze importujete více šablon (klepnutím pravým tlačítkem myši na nástroj Security Configuration And Analysis a zvolením příkazu Import Template), nástroj sloučí všechny šablony do jedné. Jestliže zjistí konflikt, má přednost šablona, kterou jste načetli jako poslední. Poté co nástroj Security Configuration And Analysis provede analýzu počítače, zobrazí výsledky, kterými můžete procházet. Uspořádání těchto výsledků je stejné jako v šablonách zabezpečení. Rozdíl spočívá v tom, že nástroj Security Configuration And Analysis zobrazuje následující indikátory, které ukazují, zda aktuální nastavení odpovídá nebo je nekonzistentní s nastavením definovaným v šabloně:

- **Červené X.** Nastavení je v databázi pro analýzu a v počítači, tyto dvě verze se však neshodují. Projděte nastaveními, u kterých je červené X, abyste určili rozsah daného problému.
- **Zelené zaškrtnutí.** Nastavení je v databázi pro analýzu a v počítači a tyto verze se shodují.

- **Otazník.** Nastavení není v databázi pro analýzu a nebylo analyzováno. To může také znamenat, že uživatel, který spustil nástroj Security Configuration And Analysis, k tomu neměl potřebné oprávnění.
- **Vykřičník.** Nastavení je v databázi pro analýzu, přitom však není v počítači. Klíč registru může existovat v databázi, ale ne v počítači.
- **Bez indikátoru.** Nastavení není v databázi nebo v počítači.

Co udělat s nesrovnalostmi zjištěnými mezi nastaveními v databázi pro analýzu a v počítači? Nejdříve můžete provést aktualizaci databáze poklepáním na problémové nastavení registru a následným klepnutím na tlačítko Edit Security (viz obrázek 8.5). Tím však aktualizujete databázi a ne šablonu. Nezmění se také nastavení počítače. Postup při změně nastavení počítače naleznete v následující části. Do počítače můžete také importovat vhodnější šablonu nebo aktualizovat šablonu v databázi a poté znovu spustit analýzu. Abyste se vyhnuli potížím vzniklým sloučením šablon v případě použití nové nebo aktualizované šablony, zvažte vytvoření nové databáze.

Úprava konfigurace počítače

Po vytvoření šablony zabezpečení a jejím následném ověření prostřednictvím analýzy počítačů pomocí nástroje Security Configuration And Analysis můžete šablonu uplatnit:

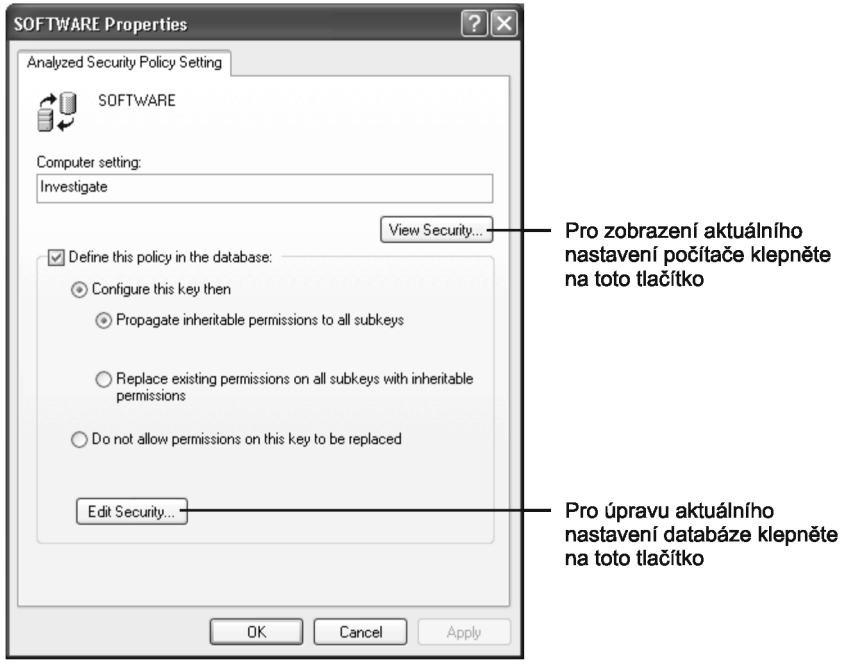
1. Pravým tlačítkem myši klepněte na nástroj Security Configuration And Analysis a zvolte příkaz Open Database.
2. V dialogovém okně Open Database máte dvě možnosti:
   - Pro vytvoření nové databáze zadejte do pole File Name název nové databáze a klepněte na tlačítko Open. V dialogovém okně Import Template vyberte šablonu a klepněte na tlačítko Open.
   - Pro otevření existující databáze zadejte do pole File Name název existující databáze a klepněte na tlačítko Open. Pokud jste upravili databázi bez aktualizace šablony, na které je založena, otevřete existující databázi.
3. Pravým tlačítkem myši klepněte na nástroj Security Configuration And Analysis, zvolte příkaz Configure Computer Now a přijměte výchozí cestu souboru protokolu nebo určete jinou.

Zavedení šablon zabezpečení v síti

V předchozí části, „Úprava konfigurace počítače“, jste se naučili, jak uplatnit šablonu zabezpečení v počítači ručně. Tento postup je vhodný pro jednorázové akce, nejde však o způsob zavedení šablon zabezpečení ve více počítačích v síti. Chcete-li nasadit šablony v síti, použijte Group Policy: vytvořte nový objekt GPO a poté jej upravte. V editoru Group Policy Editor klepněte pravým tlačítkem myši na položku Security Settings a zvolte příkaz Import Policy. Vyberte šablonu, kterou chcete použít, a klepněte na tlačítko Open.

Zní to jednoduše, ale neměli byste tuto metodu brát na lehkou váhu – zavedení šablon zabezpečení v síti vyžaduje pečlivé plánování. Nejdříve musíte určit šablony vyžadované ve vaší síti. Poté musíte stanovit, které organizační jednotky získají příslušné šablony zabezpečení. Pokud například obchodní oddělení používá starší

aplikace vyžadující, aby skupina Users měla úplnou kontrolu nad určitými klíči registru, zdokumentujte a otestujte šablonu zabezpečení a následně ji importujte do objektu GPO, který přiřadíte organizační jednotce obchodního oddělení. V ideálním případě budete se šablonami zabezpečení počítat již v procesu plánování zavedení. Často se stává, že se IT profesionálové snaží prostřednictvím šablon zabezpečení řešit potíže vzniklé chybějící předvídavostí a nedostatečným pečlivým plánováním.



OBRÁZEK 8.5: V dialogovém okně Properties si můžete prohlédnout a upravovat nastavení.

8.8 Konfigurace nových funkcí zabezpečení

V opravném balíčku Microsoft Windows XP SP2 jsou k dispozici nová rozšíření zdokonalující správu a možnosti zabezpečení klíčů v osobních počítačích. K těmto rozšířením patří následující:

- Nová funkce Windows Security Center (Centrum zabezpečení Windows) vám oznamuje stav třech hlavních součástí zabezpečení: Windows Firewall, Automatic Updates a Virus Protection (Brána Firewall systému Windows, Automatické inovace, Antivirová ochrana).
- Windows Security Center určuje, zda jsou funkce zabezpečení klíčů zapnuté a aktuální. Windows Security Center vám oznamuje, že je nutná aktualizace nebo musíte provést další kroky pro zdokonalení zabezpečení počítače.
- Správu Windows Security Center můžete provádět prostřednictvím nastavení Active Directory Group Policy. Nástroj Windows Security Center je v doménových prostředích implicitně vypnutý.

Následující části popisují způsob konfigurace funkcí zabezpečení Windows XP SP2 a Windows Server 2003 SP1. K těmto funkcím patří Windows Security Center (Windows XP) a Windows Firewall. Od vydání opravného balíčku SP2 jsem byl často tázán, jak lze tyto dvě funkce konfigurovat.

Výstrahy nástroje Security Center

Nástroj Windows Security Center zobrazuje výstrahy v překryvných oknech v případě, že konfigurace brány firewall, zjišťování virů nebo funkce Automatic Updates není správná (nebo je neaktuální). Tyto výstrahy se zobrazují v oznamovací oblasti na hlavním panelu. Výstrahy můžete vypnout pomocí registru. Tabulka 8.2 popisuje hodnoty `REG_DWORD` pro každý typ výstrahy. Hodnoty nastavujete v klíči `HKLM\SOFTWARE\Microsoft\Security Center`. (Pokud v registru neexistuje, vytvořte klíč a nastavení.) Chcete-li například zabránit zobrazování výstrah nástroje Windows Security Center, když není povolena brána Windows Firewall (konfigurace, kterou společnost Microsoft nedoporučuje), nastavte `FirewallDisableNotify` na `0x01`.

Windows Firewall

V opravných balíčcích Windows XP SP2 a Windows Server 2003 SP1 je k dispozici nová brána Windows Firewall. Většina společností a mnoho nadšenců bude chtít upravit bránu Windows Firewall během instalace. Společnost Microsoft k tomu nabízí tři metody. Nejlepším způsobem správy nastavení Windows Firewall v podnikovém prostředí je použití nových nastavení Windows Firewall Group Policy. Tento postup vyžaduje adresářovou službu Active Directory s řadiči domén Windows 2000 nebo Windows Server 2003. Více informací naleznete na internetové adrese `http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/depfwset/wfsp2wgp.mspx`.

TABULKA 8.2: Nastavení nástroje Security Center

Název	Typ	Hodnoty
AntiVirusDisableNotify	REG_DWORD	0x00 – Zakázat výstrahy antivirového programu. 0x01 – Zobrazovat výstrahy antivirového programu.
AntiVirusOverride	REG_DWORD	0x00 – Windows Security Center sleduje antivirový program. 0x01 – Windows Security Center nesleduje antivirový program.
FirewallDisableNotify	REG_DWORD	0x00 – Zakázat výstrahy brány firewall. 0x01 – Zobrazovat výstrahy brány firewall.
FirewallOverride	REG_DWORD	0x00 – Windows Security Center sleduje bránu firewall. 0x01 – Windows Security Center nesleduje bránu firewall.
UpdatesDisableNotify	REG_DWORD	0x00 – Zakázat výstrahy funkce Automatic Update. 0x01 – Zobrazovat výstrahy funkce Automatic Update.

Následující seznam popisuje metody, které nevyžadují Group Policy:

- **Soubor unattend.txt.** Soubor `unattend.txt` pro Windows XP SP2 nabízí možnosti ke konfiguraci nastavení Windows Firewall při spuštění bezobslužné instalace opravného balíčku Windows XP SP2.
- **Soubor Netfw.inf.** Soubor `Netfw.inf` pro Windows XP SP2 může konfigurovat bránu Windows Firewall určením sady nastavení registru shodující se s možnostmi dostupnými v součásti Windows Firewall v okně Control Panel a prostřednictvím nastavení Windows Firewall Group Policy, když uživatel provádí interaktivní instalaci opravného balíčku Windows XP SP2.
- **Skript Netsh.** Po instalaci opravného balíčku SP2 v systému Windows XP může být nutné, aby uživatelé spustili soubor skriptu, jako je například soubor `.BAT` nebo `.CMD`, který obsahuje řadu příkazů `Netsh.exe` ke konfiguraci operačního režimu, povolených programů, povolených portů atd. v bráně Windows Firewall.
- **Vlastní konfigurační programy.** Po instalaci opravného balíčku SP2 v systému Windows XP může být nutné, aby uživatelé spustili vlastní konfigurační program, který používá nové konfigurace API brány Windows Firewall ke konfiguraci operačního režimu, povolených programů, povolených portů a dalších nastavení.

Další informace o těchto možnostech naleznete na internetové adrese `http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/depfwset/wfsp2ngp.mspx`.

Windows Firewall můžete zakázat prostřednictvím registru. Nastavení jsou v klíči `HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall`. (Pokud klíč a hodnoty v registru nejsou, vytvořte je.) V tomto klíči jsou dva podklíče: `DomainProfile` a `StandardProfile`. Nastavení v podklíči `DomainProfile` se uplatňují v případě, že je počítač aktuálně připojený k doméně. Nastavení v podklíči `StandardProfile` se uplatňují, když počítač není aktuálně připojený k doméně (například odpojený přenosný počítač). V obou těchto klíčích vytvořte hodnotu `EnableFirewall`. Chcete-li bránu firewall zakázat, nastavte tuto hodnotu na `0x00`, v opačném případě nastavte `0x01`.

8.9 Nastavení utajení osobních údajů v prohlížeči Internet Explorer

Od verze prohlížeče Microsoft Internet Explorer 6 je k dispozici karta Privacy, která uživatelům dává větší kontrolu nad soubory cookie. V zóně Internet existují různé úrovně soukromí, které jsou v registru uloženy tam kde zóny zabezpečení.

Můžete také přidat webový server, u kterého povolíte nebo zablokujete soubory cookie, bez ohledu na zásady soukromí na webovém serveru. Klíče registru se ukládají do klíče `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History`. V tomto klíči vidíte domény, které byly přidány jako spravované weby. Tyto domény jsou nastaveny na jednu z následujících hodnot:

- `0x00000005`. Vždy blokovat
- `0x00000001`. Vždy povolit

8.10 Zóny zabezpečení v prohlížeči Internet Explorer

Nastavení zón zabezpečení prohlížeče Internet Explorer se ukládají do klíčů `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings` a `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`. Nastavení zón zabezpečení se implicitně ukládají do `HKCU`. Nastavení pro jednoho uživatele neovlivňují nastavení pro jiného uživatele. Klíč `Internet Settings` obsahuje následující podklíče:

- `TemplatePolicies`
- `ZoneMap`
- `Zones`

Je-li v Group Policy povoleno nastavení `Security Zones: Use only machine settings` nebo je v klíči `HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings` přítomna hodnota `REG_DWORD` s názvem `Security_HKLM_only`, jsou použita pouze nastavení místního počítače a všichni uživatelé mají stejná nastavení zabezpečení. Pokud je povolena zásada `Security_HKLM_only`, bude prohlížeč Internet Explorer používat hodnoty `HKLM`, hodnoty `HKCU` však budou přesto zobrazeny v nastavení zón na kartě Security v prohlížeči Internet Explorer. Jestliže v Group Policy není povoleno nastavení `Security Zones: Use only machine settings` nebo neexistuje hodnota `REG_DWORD` s názvem `Security_HKLM_only`, případně je nastavena na `0`, jsou použita nastavení počítače spolu s uživatelskými nastaveními. V okně Internet Options se však zobrazí pouze uživatelská nastavení. Pokud například tato hodnota `REG_DWORD` neexistuje nebo je nastavena na 0, jsou čtena nastavení `HKLM` spolu s `HKCU`, v okně Internet Options se však zobrazí pouze nastavení `HKCU`.

TemplatePolicies

Klíč `TemplatePolicies` určuje nastavení výchozích úrovní zón zabezpečení (Low, Medium Low, Medium a Hight). Výchozí nastavení úrovně zabezpečení můžete změnit. Nemůžete však přidávat žádné další úrovně zabezpečení. Klíče obsahují hodnoty, které stanovují nastavení pro zónu zabezpečení. Každý klíč obsahuje řetězcové hodnoty `Description` a `Display Name`, jež určují text zobrazený na kartě Security pro každou z úrovní zabezpečení.

ZoneMap

Klíč `ZoneMap` obsahuje následující klíče:

- **Domains.** Klíč `Domains` obsahuje domény a protokoly, které byly přidány pro změnu chování z výchozího nastavení. Po přidání domény se do klíče `Domains` přidá klíč. Poddomény se zobrazují jako klíče pod doménou, ke které náleží. Každý klíč uvádějící doménu obsahuje hodnotu `REG_DWORD` s názvem příslušného protokolu. Hodnota `REG_DWORD` se shoduje s číselnou hodnotou zóny zabezpečení, do níž je doména přidána.
- **ProtocolDefaults.** Klíč `ProtocolDefaults` definuje výchozí zónu zabezpečení použitou pro konkrétní protokol (ftp, http nebo https). Chcete-li změnit výchozí nastavení, můžete buď přidat protokol do zóny zabezpečení klepnutím na tla-

čítko Sites na kartě Security nebo přidat hodnotu REG_DWORD do klíče Domains. Název hodnoty REG_DWORD se musí shodovat s názvem protokolu a nesmí obsahovat žádné dvojtečky (:) nebo lomítka (/).

Klíč ProtocolDefaults obsahuje také hodnoty REG_DWORD, které definují výchozí zóny zabezpečení, v kterých je použit protokol. Ke změně těchto hodnot nelze použít ovládací prvky na kartě Security. Toto nastavení se používá v případě, že určitý webový server nespadá do zóny zabezpečení.

- **Ranges.** Klíč Ranges obsahuje rozsahy adres TCP/IP. Každý definovaný rozsah TCP/IP se zobrazí v libovolně nazvaném klíči. Tento klíč obsahuje řetězcovou hodnotu (:Range) s určeným rozsahem TCP/IP. Pro každý protokol je přidána hodnota REG_DWORD obsahující číselnou hodnotu zóny zabezpečení pro stanovený rozsah IP.

  Když soubor Urlmon.dll použije veřejnou funkci MapUrlToZone k překladu určité adresy URL na zónu zabezpečení, provede tak prostřednictvím jedné z následujících metod:

  - Pokud URL-adresa obsahuje úplný název domény (FQDN), je zpracován klíč Domains. V této metodě potlačí přesná shoda webu částečnou shodu.
  - Jestliže URL-adresa obsahuje adresu IP, je zpracován klíč Ranges. Adresa IP adresy URL je porovnána s hodnotou :Range, která je součástí každého libovolně nazvaného klíče v klíči Ranges.

Poznámka Protože jsou klíče s libovolnými názvy zpracovávány v pořadí, v jakém byly přidány, může tato metoda najít dříve částečnou shodu než přesnou shodu. Pokud se tak stane, může být URL-adresa použita v jiné zóně zabezpečení, než do které je běžně přiřazena.

Zones

Klíč Zones obsahuje klíče, které představují jednotlivé zóny zabezpečení definované pro počítač. Implicitně je stanoveno následujících pět zón (číslovaných od nuly do čtyřky):

- 0. My Computer
- 1. Local Intranet Zone
- 2. Trusted Sites Zone
- 3. Internet Zone
- 4. Restricted Sites Zone

Poznámka Zóna My Computer (Tento počítač) se implicitně nezobrazuje v poli Zone na kartě Security.

Každý z těchto klíčů obsahuje následující hodnoty REG_DWORD, které představují odpovídající nastavení na vlastní kartě Security:

- 1001. Download signed ActiveX controls (Stahovat podepsané ovládací prvky Active X)

- 1004. Download unsigned ActiveX controls (Stahovat nepodepsané ovládací prvky Active X)
- 1200. Run ActiveX controls and plug-ins (Spouštět ovládací prvky Active X a moduly plug-in)

  Hodnota Run ActiveX controls and plug-ins (1200) má zvláštní nastavení s názvem Administrator approved. Je-li toto nastavení zapnuto, hodnota REG_DWORD je 0x00010000 a v klíči HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\AllowedControls je vyhledán seznam schválených ovládacích prvků.
- 1201. Initialize and script ActiveX controls not marked as safe (Skriptovat ovládací prvky Active X neoznačené jako bezpečné)
- 1206. Allow scripting of Internet Explorer Webbrowser control (Povolit skriptování ovládacího prvku WebBrowser aplikace Internet Explorer)
- 1400. Active scripting (Aktivní skriptování)
- 1402. Scripting of Java applets (Skriptování apletů v jazyce Java)
- 1405. Script ActiveX controls marked as safe for scripting (Skriptování ovládacích prvků Active X označených jako bezpečné)
- 1406. Access data sources across domains (Přístup ke zdrojům dat v jiných doménách)
- 1407. Allow paste operations via script (Povolit operace vkládání prostřednictvím skriptů)
- 1601. Submit non-encrypted form data (Odesílat nezašifrovaná formulářová data)
- 1604. Font download (Stažení písma)
- 1605. Run Java (Spouštět jazyk Java)
- 1606. Userdata persistence (Trvalost uživatelských dat)
- 1607. Navigate sub-frames across different domains (Navigace dílčími rámci mezi různými doménami)
- 1608. Allow META REFRESH (Povolit parametry META REFRESH)
- 1609. Display mixed content (Zobrazit smíšený obsah)
- 1800. Installation of desktop items (Instalace součástí pracovní plochy)
- 1802. Drag and drop or copy and paste files (Přetahování nebo kopírování a vkládání souborů)
- 1803. File Download (Stahování souborů)

  Pro hodnotu File Download (1803) neexistuje nastavení výzvy, protože tato hodnota buď je, nebo není povolena.
- 1804. Launching programs and files in an IFRAME (Spouštění programů a souborů v sekci IFRAME)
- 1805. Launching programs and files in webview (Spouštění programů a souborů v zobrazení web)

- 1806. Launching applications and unsafe files (Spouštění aplikací a nezabezpečených souborů)
- 1807. Reserved (Rezervováno)
- 1808. Reserved (Rezervováno)
- 1809. Use Pop-up Blocker (Blokovat automaticky otevíraná okna)
- 1A00. Logon (Přihlašování)

  Nastavení Logon (1A00) může mít jednu z následujících hodnot:

  - 0x00000000. Automatically logon with current username and password (Automatické přihlášení pod aktuálním uživatelským jménem a heslem)
  - 0x00010000. Prompt for user name and password (Požadovat uživatelské jméno a heslo)
  - 0x00020000. Automatic logon only in the Intranet zone (Automatické přihlášení pouze do zóny sítě intranet)
  - 0x00030000. Anonymous logon (Anonymní přihlášení)
- 1A02. Allow persistent cookies that are stored on your computer (Povolení ukládání souborů cookies na tento počítač)
- 1A03. Allow per-session cookies (not stored) (Povolení souborů cookies v této relaci – bez ukládání)
- 1A04. Don't prompt for client certificate selection when no certificates or only one certificate exists (Nezobrazovat výzvu k výběru klientského certifikátu, jestliže je k dispozici pouze jeden nebo žádný certifikát)
- 1A05. Allow 3rd party persistent cookies (Povolit trvalé soubory cookies od dodavatelů třetích stran)
- 1A06. Allow 3rd party session cookies (Povolit dočasné soubory cookies od dodavatelů třetích stran)
- 1A10. Privacy Settings (Osobní údaje)

  Nastavení Privacy Settings (1A10) používá jezdec na kartě Privacy. Hodnoty REG_DWORD jsou následující:

  - 00000003. Block All Cookies (Všechny soubory cookies budou blokovány)
  - 00000001. High (Vysoká)
  - 00000001. Medium High (Vyšší)
  - 00000001. Medium (Střední)
  - 00000001. Low (Nízká)
- 00000000. Accept All Cookies (Povolit všechny soubory cookies)
- 1C00. Java Permissions

  Nastavení Java Permissions (1C00) může mít následujících pět binárních hodnot REG_BINARY:

  - 00 00 00 00. Disable Java (Zakázat jazyk Java)
  - 00 00 01 00. High safety (Vysoké zabezpečení)

- 00 00 02 00. Medium safety (Střední zabezpečení)
- 00 00 03 00. Low safety (Nízké zabezpečení)
- 00 00 80 00. Custom (Volitelné zabezpečení)

- 1E05. Software channel permissions (Oprávnění programových kanálů)

  Nastavení Software channel permissions (1E05) má tři různé hodnoty:

  - 00010000. High (Vysoká)
  - 00020000. Medium (Střední)
  - 00030000. Low (Nízká)
- 1F00. Reserved (Rezervováno)
- 2000. Binary and script behaviors (Chování skriptů a binárních souborů)
- 2001. Run .NET components signed with Authenticode (Spouštět .NET komponenty podepsané Authenticode)
- 2004. Run .NET components not signed with Authenticode (Spouštět .NET komponenty nepodepsané Authenticode)
- 2100. Open files based on content, not file extension (Otevírat soubory podle jejich obsahu, nikoli podle jejich přípony)
- 2101. Web sites in less privileged Web content zone can navigate into this zone (Povolení navigace do této zóny pro webové stránky z nižších zón oprávnění)
- 2102. Allow script-initiated windows without size or position constraints (Povolit skriptová okna bez omezení velikosti i umístění)
- 2200. Automatic prompting for file downloads (Automatická výzva ke stahování souborů)
- 2201. Automatic prompting for ActiveX controls (Automatická výzva ovládacích prvků ActiveX)
- 2300. Allow Web pages to use restricted protocols for active content (Povolit webovým stránkám použití v aktivním obsahu chráněných protokolů)
- {AEBA21FA-782A-4A90-978D-B72164C80120} First Party Cookie
- {A8A88C49-5EB2-4990-A1A2-0876022C854F} Third Party Cookie

Pokud není uvedeno jinak, můžete každou z hodnot REG_DWORD nastavit na nulu, jedničku nebo trojku. Nastavení na nulu obvykle znamená povolení určité činnosti, jednička zajistí zobrazení výzvy a trojka znamená nepovolení určité činnosti.

Každá zóna zabezpečení obsahuje také řetězcové hodnoty Description a Display Name. Text těchto hodnot se zobrazí na kartě Security, když klepnete na zónu v poli Zone. Je zde také řetězcová hodnota Icon, která nastavuje ikonu pro jednotlivé zóny. Kromě zóny My Computer obsahuje každá zóna hodnoty REG_DWORD s názvem CurrentLevel, MinLevel a ReccommendedLevel. Hodnota MinLevel představuje nejnižší nastavení, které lze použít, než se zobrazí varovná zpráva. Hodnota CurrentLevel je aktuální nastavení pro zónu a hodnota RecommendedLevel je doporučovaná úroveň pro zónu. Následující seznam popisuje nastavení pro tyto hodnoty:

- 0x00010000. Low Security

- `0x00010500`. Medium Low Security
- `0x00011000`. Medium Security
- `0x00012000`. High Security

Hodnota `REG_DWORD` s názvem `Flags` určuje, zda uživatel může upravovat vlastnosti zóny zabezpečení. Pro stanovení hodnoty `Flags` sloučíte čísla příslušných nastavení. K dispozici jsou tyto hodnoty `Flags`:

- `1`. Povolit změny vlastních nastavení
- `2`. Uživatel může přidávat webové servery do této zóny
- `4`. Vyžadovat ověřené webové servery (protokol https)
- `8`. Zahrnout webové servery, které neprocházejí přes server proxy
- `16`. Zahrnout webové servery, které nejsou uvedeny v jiných zónách
- `32`. Nezobrazovat zónu zabezpečení v dialogovém okně Internet Properties (výchozí nastavení pro zónu My Computer)
- `64`. Zobrazovat dialogové okno Requires Server Verification
- `128`. S připojeními Universal Naming Connections (UNCs) pracovat podobně jako s připojeními k intranetu