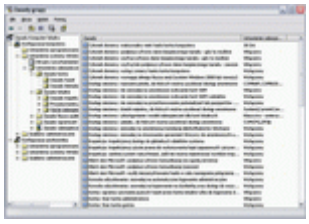
Powtórka z systemów – Windows XP Professional – *życzę przyjemnej lektury!*

Windows XP to system wielozadaniowy, przeznaczony do współużytkowania przez wiele osób. Dysponuje przejrzystym mechanizmem logowania, jasnym podziałem danych poszczególnych osób i bezpiecznym udostępnianiem zasobów. Jednak wcale nie tak łatwo wykorzystać techniczne fundamenty systemu tak, aby każdy miał możliwość wykonywania dokładnie tego, na co chcesz mu zezwolić, pełniąc funkcję administratora peceta. W poniższym materiale staram się uporządkować ten wielki zbiór wiedzy, na który składają się procedury logowania, zasady systemowe, przydziały uprawnień i udostępnienia. Rozpoczynamy od stosunkowo prostych do zrozumienia reguł logowania.

Logowanie i zasady systemowe

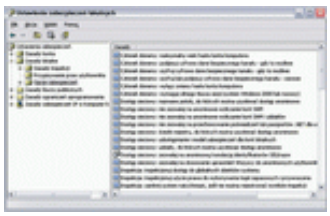


Przystawka GPEDIT.MSC, czyli edytor zasad grup, pozwala m.in. nakładać restrykcje na poszczególne konta użytkowników, a także zmieniać ponad sto innych ustawień dotyczących bezpieczeństwa. Jest dostępna w Windows XP Professional (ze sporymi ograniczeniami również XP Home Edition). Podstawową rolę w zapewnieniu bezpieczeństwa systemu odgrywa system plików NTFS, ale nawet zainstalowane na partycji FAT32 środowisko Windows XP oferuje większe ograniczenia dostępu podczas logowania, podczas zwyczajnej pracy w systemie i podczas wykonywania czynności konserwacyjnych z poziomu konsoli odzyskiwania.

1. Bezpieczeństwo podczas logowania

Okno logowania się użytkowników nie sieciowych, lecz lokalnych nieubłaganie żąda nazwy konta i odpowiedniego hasła. Mechanizm ten zdaje się bezpieczny - i jest, jeśli zastosujesz się do pewnych wskazówek.

Okno powitalne środowiska Windows XP samodzielnie oferuje konta użytkowników zarejestrowanych w systemie. Okazuje się mniej restrykcyjne niż klasyczne okno logowania, w którym trzeba własnoręcznie wpisywać nazwę użytkownika. Swój ulubiony rodzaj logowania możesz wybrać w aplecie Konta użytkowników Panelu sterowania (menu Start | Ustawienia | Panel sterowania).



Narzędzie SECPOL.MSC oferuje niewielki, lecz przejrzysty **zbiór ustawień bezpieczeństwa**. (Start->Uruchom->secpol.msc)

Logowanie w systemie nie jest bezpieczne, jeśli są w nim zdefiniowane konta bez haseł. Brzmi to trywialnie, jednak to złudne wrażenie, bo określone predefiniowane konta nie wymagają podawania haseł, choć nie wie o tym większość użytkowników. W **Windows XP Home Edition konto Administrator nie dysponuje domyślnie hasłem**. W rezultacie każdy ma nieograniczony dostęp do komputera - wystarczy wybrać konto Administrator w trybie awaryjnym lub uruchomić system z poziomu Konsoli odzyskiwania. Koniecznie zamknij tę lukę w zabezpieczeniach. Przywołaj w tym celu okno wiersza poleceń i wpisz:
net user administrator <hasło>
Jeśli ponadto jest uaktywnione konto Gość, każdy może się dostać do systemu bez podawania hasła. Zasadniczo nie ma racjonalnego powodu do uaktywniania (lokalnego) konta Gość. Nawet jeśli chcesz udostępnić pewne zasoby wszystkim użytkownikom w sieci, nie musisz zakładać konta gościa. Anonimowy dostęp przez sieć wymaga tylko złagodzenia określonych restrykcji w zasadach konta Gość, a nie możliwości lokalnego logowania się Gościa w komputerze.

2. Bezpieczeństwo haseł
W odróżnieniu od nazwy kont, które można wpisywać w dowolny sposób (małymi lub wielkimi literami albo różnie), Windows wymaga dokładnego podawania hasła, z rozróżnieniem małych i wielkich liter. Pozostałe wymagania co do haseł można definiować w przystawce **Ustawienia zabezpieczeń lokalnych** (nie dotyczy Windows XP Home Edition). Przywołasz ją, otwierając menu **Start | Uruchom i wpisując secpol.msc**. Rozwiń gałęzie Zasady konta i Zasady haseł. Godne polecenia jest przede wszystkim ustawienie minimalnej długości hasła i zasad złożoności. Oznacza to, że hasło musi spełniać co najmniej trzy z czterech kryteriów - zawierać małe litery, wielkie litery, cyfry i/lub znaki specjalne. Zmiany powyższych zasad nie mają wpływu na dotychczas założone hasła. Tylko podczas modyfikowania hasła lub zakładania nowego system sprawdza, czy wpis odpowiada powyższym ustawieniom.

Zwróć uwagę na to, że wszystkie hasła i zasady systemowe można modyfikować z poziomu każdego konta z uprawnieniami administratora. Zatem im mniej kont administratorskich w systemie, tym większe bezpieczeństwo podczas logowania.

Centrala zabezpieczeń w Windows XP

Wymuszone logowanie w systemie, prawa dostępu NTFS i zasady grup to bardzo skuteczne środki zabezpieczania danych przed nieupoważnionymi i kontrolowanego przekazywania ich we właściwe ręce. Środowisko Windows zapewnia kilka narzędzi do sterowania konfiguracją zabezpieczeń.

CACLS.EXE służy do podglądania i przedefiniowania uprawnień NTFS. Nie dysponuje graficznym interfejsem - działa tylko w oknie wiersza poleceń. Chcąc przydzielić użytkownikowi Gienek pełny dostęp do katalogu C:\DOKUMENTY, wystarczy wpisać:

cacls c:\dokumenty /g Gienek:F

Przyznanie uprawnień umożliwia parametr **/g**. Przełącznikiem **/d** odbiera się użytkownikowi uprawnienia, a przełącznikiem **/p** zmienia jego dotychczasowe prawa dostępu. Pełny opis parametrów i ich znaczenia uzyskasz, wpisując polecenie **cacls /?**.

FSMGMT.MSC - przystawka **Foldery udostępnione wyświetla przejrzyste zestawienie zasobów udostępnionych w sieci.** Przywołując ich właściwości w menu podręcznym, uzyskasz przegląd bieżących praw dostępu do poszczególnych udziałów, a nawet możliwość ich edytowania (patrz również polecenie **net share**).

GPEDIT.MSC (tylko w środowisku Windows 2000 i XP Professional) - **edytor zasad grup** stanowi centralny moduł licznych ustawień rejestru, które dotyczą bezpieczeństwa. Chcąc zmodyfikować lub uaktywnić określoną zasadę, wystarczy kliknąć ją dwukrotnie i dokonać żądanych zmian.

LUSR.MSC - menedżer użytkowników. Wyświetla wszystkich użytkowników i grupy lokalne zarejestrowane w systemie, a także przynależności użytkowników do tychże grup. Oferuje możliwość edytowania, usuwania i zakładania kont użytkowników (patrz również polecenie **net user**).

net localgroup - polecenie działające wyłącznie w trybie tekstowym (podobnie jak CACLS.EXE). Pozwala zakładać (**net localgroup /add <nazwa_grupy>**) i usuwać (**net localgroup /delete <nazwa_grupy>**) grupy użytkowników. Jest dostępne nawet w Windows XP Home Edition.

net share - polecenie do użytku w trybie tekstowym. Wyświetla listę zasobów udostępnionych w sieci, tworzy nowe udostępnienia
(**net share <nazwa_udziału>=<ścieżka>**)
i usuwa dotychczasowe (**net share <nazwa_udziału>/delete**).
Uwaga - do zasobów udostępnionych poleceniem net share mają pełny dostęp (w trybie odczytu i zapisu) wszyscy uwierzytelnieni użytkownicy i goście, jeśli dopuszczają to ich lokalne uprawnienia NTFS.

net user - bardzo funkcjonalna alternatywa przystawki LUSR.MSC (patrz wyżej), działająca w trybie tekstowym. Wyświetla listę kont, pozwala tworzyć nowe konta (parametr **/add**), usuwać dotychczasowe (**/delete**), a nawet wyłączać je i ponownie włączać (**/active:no** i **/active:yes**). Za jego pomocą można zmieniać hasła użytkowników (**net user <nazwa_konta> <hasło>**). Do nieudokumentowanych należy funkcja ograniczania dopuszczalnej pory logowania (np. **net user <nazwa_konta> /times:pn-pt, 14-18**). Ograniczenia te cofa się poleceniem net **user <nazwa_konta> /times:all**.

XCACLS.EXE - narzędzie z zestawu Windows 2000 Resource Kit, działa również w Windows XP. W porównaniu do standardowego CACLS.EXE umożliwia bardziej szczegółowe przydzielanie praw dostępu, a także przejmowanie praw własności do określonych obiektów na dysku.

3. Administratorzy i użytkownicy

Chcąc uprościć przydzielanie uprawnień, wyposażono Windows w hierarchiczną strukturę grup użytkowników. Każde konto w pececie ze środowiskiem Windows jest przypisane do jednej z tych grup. Okno dialogowe apletu Konta użytkowników w Windows XP rozróżnia tylko dwie grupy lokalne - administratorów i użytkowników z ograniczonym dostępem. Stanowi to duże uproszczenie, bo konta obarczone ograniczeniami dzielą się na kolejne podgrupy. Osoba zarządzająca systemem powinna znać co najmniej podział na użytkowników, użytkowników zaawansowanych (zwanych również pełnomocnymi) i gości.

Nieudokumentowane polecenie **control userpasswords2** (Start->Uruchom->cmd->control userpassword2) pozwala dostać się do okna dialogowego Konta użytkowników w Windows XP. Zauważ jednak, że w wersji Home Edition nie ma podziału na użytkowników i użytkowników zaawansowanych.

Jeśli poszczególne konta nie podlegają określonym restrykcjom zdefiniowanym np. w przystawce GPEDIT.MSC lub poprzez uprawnienia NTFS, tylko przynależność do jednej ze wspomnianych grup decyduje o zakresie kompetencji danego użytkownika. Na przykład Administrator może dokładnie tyle, co użytkownik Jacek, jeśli należą do tej samej grupy lokalnej.

Wiele narzędzi do konfigurowania opcji zabezpieczeń jest dostępnych również w trybie tekstowym.
Konta z grupy Administratorzy i konta pozostałych użytkowników mają odmienne uprawnienia globalne, nawet jeśli Windows nie jest zainstalowany na partycji NTFS, która pozwala definiować prawa dostępu do plików. Konta należące do grupy Administratorzy mają zasadniczo nieograniczone uprawnienia - również cofania ewentualnych restrykcji "konkurencyjnych" administratorów. Konta o ograniczonych uprawnieniach, czyli konta użytkowników, nie mają możliwości zakładania ani modyfikowania kont (nie mają dostępu do przystawek GPEDIT.MSC, SECPOL.MSC i LUSRMGR.MSC). Ponadto zabronione im są wszelkie globalne modyfikacje systemu - np. instalowanie sterowników, czcionek i aplikacji (w folderze \Program Files). Nie wolno przestawiać zegara systemowego, dokonywać zmian w rejestrze i usługach systemowych, a także udostępniać zasobów ani cofać takich udostępnień. Zakaz obejmuje także dostęp do przystawki Zarządzanie dyskami, do programu Defragmentator dysków, a nawet do zmiennych środowiskowych czy choćby do ustawień systemowego Kosza.

Członkowie grupy Użytkownicy mogą zmieniać konfigurację własnego profilu. Muszą tylko trzymać się z dala od wszystkich centralek sterowania systemem. Konta grupy Użytkownicy zaawansowani (nie dotyczy XP Home Edition) mają więcej uprawnień. Wolno im np. instalować aplikacje w obrębie całego dysku, zmieniać zegar systemowy, a także ustawienia drukarek i opcje zasilania. Do wykonywania codziennych zadań w systemie wystarcza z powodzeniem konto grupy Użytkownicy zaawansowani, a w wielu wypadkach nawet konto grupy Użytkownicy.

Oprócz apletu Konta użytkowników w Panelu sterowania środowiska Windows XP Professional oferują menedżera użytkowników i grup lokalnych. Aby go przywołać, otwórz menu **Start | Uruchom** i wpisz polecenie **lusrmgr.msc**. Narzędzie to okazuje się wręcz nieodzowne do zakładania nowych grup.

W Windows XP Home Edition brakuje przystawki LUSRMGR.MSC. Chcąc założyć grupę lokalną w tym systemie, musisz otworzyć okno wiersza poleceń i wpisać:

net localgroup /add <nazwa_grupy>

W podobny sposób usuniesz niepotrzebną grupę. Użyj do tego polecenia

net localgroup /delete <nazwa_grupy>

Gdy pozbawisz określone konto członkostwa w danej grupie (za pomocą polecenia net lub przystawki LUSRMGR.MSC), Windows przydzieli mu uprawnienia Użytkownika z ograniczonym dostępem.

Oprócz opisanych powyżej grup zdefiniowanych domyślnie są jeszcze grupy specjalne, m.in. grupa Wszyscy. W jej skład nie wchodzą wszyscy użytkownicy, jak sugeruje nazwa, lecz tylko zbiór użytkowników uwierzytelnionych w danym systemie - łącznie z kontami grupy Goście. Powinieneś mieć to na uwadze, gdy zechcesz udostępnić "wszystkim" określone zasoby na dysku.

4. Systemy na zewnątrz
Po włączeniu komputera można przywołać Konsolę odzyskiwania, która służy do prac

naprawczych i konserwacyjnych. Również tu system wymaga podania hasła administratora. To domyślne zabezpieczenie, lecz dysponując uprawnieniami administratora, można je wyłączyć za pośrednictwem przystawki GPEDIT.MSC. Stosowny parametr - Konsola odzyskiwania: zezwalaj na automatyczne logowanie administracyjne - znajdziesz w obrębie gałęzi Ustawienia systemu Windows | Ustawienia zabezpieczeń | Zasady lokalne | Opcje zabezpieczeń.

Menedżer użytkowników, LUSRMGR.MSC, podaje wykaz użytkowników i grup lokalnych zarejestrowanych w systemie. Pozwala dodawać nowe konta, a także usuwać i modyfikować istniejące. Blokada dostępu do danych zgromadzonych lokalnie w komputerze okazuje się bezużyteczna, gdy ktoś uruchomi system za pośrednictwem nośników zewnętrznych. Aby dostać się do partycji sformatowanych w systemie FAT32, wystarcza zwyczajna dyskietka startowa DOS. Dostęp do partycji NTFS umożliwi startowa płyta Linuksa lub środowisko Windows PE (bezpłatne, dostępne pod adresem http://www.nu2.nu/pebuilder , rozmiar pliku: 2,73 MB). Nawet z poziomu Konsoli odzyskiwania na płycie instalacyjnej Windows 2000 możesz zalogować się bez hasła w systemie Windows XP. Jeśli w komputerze, z którego oprócz ciebie korzystają inni, znajdują się poufne informacje, wyłącz wczytywanie systemu z dyskietki i płyty CD, a także zabezpiecz wejście do BIOS-u hasłem. Jeszcze większy poziom bezpieczeństwa zapewnia szyfrowanie danych w partycjach NTFS (patrz punkt 9).

5. Zasady systemowe

Przystawka GPEDIT.MSC, dostępna w konsoli zarządzania (Microsoft Management Console - MMC.EXE), zawiera trzycyfrową liczbę systemowych zasad bezpieczeństwa. Ponadto jest do dyspozycji przystawka SECPOL.MSC. Znajdziesz tu jednak tylko skromny wybór obszernego zbioru GPEDIT.MSC. Zasady zgromadzone w obrębie gałęzi Szablony administracyjne przystawki Gpedit są zależne od plików szablonów ADM przechowywanych w katalogu %windir%\SYSTEM32\ GROUPPOLICY\ADM. W środowisku Windows XP Home Edition nie przewidziano obu przystawek, o których mowa powyżej. Nie dają się nawet doinstalować.

W edycji XP Professional przywołanie gpedit.msc daje dostęp do setek ustawień globalnych (gałąź Konfiguracja komputera) i indywidualnych (gałąź Konfiguracja użytkownika). Ustawienia, o których mowa, to po prostu wybrane wartości rejestru, a przystawka Zasady grupy stanowi interfejs pozwalający modyfikować je znacznie wygodniej niż za pomocą Edytora rejestru. Ich zakres sięga od konfiguracji pulpitu przez opcje menu Start, zasady kont użytkowników po zakazy obowiązujące w aplikacjach. Nie należy tu zbyt wiele eksperymentować. Zaledwie kilka śmiałych kliknięć może doprowadzić do niezamierzonego zablokowania ważnych składników Windows, wyłączenia niektórych kont użytkowników czy obniżenia poziomu bezpieczeństwa systemu.

Aby uniknąć niepożądanych skutków, wyjątkowo ostrożnie obchodź się z ustawieniami w przystawce Gpedit. Ponadto musisz się zastosować do wskazówek wymienionych poniżej.

- Przystawkę Gpedit uruchamia się wyłącznie z poziomu konta ujętego w grupie Administratorzy.
- Ustawienia dokonywane w przystawce Gpedit są przechowywane w pliku REGISTRY.POL, zapisanym w katalogu %windir%\SYSTEM32\ GROUPPOLICY - w folderze MACHINE, jeśli zmodyfikowano ustawienia globalne (Konfiguracja

komputera), i/lub w folderze USER, jeżeli zmieniono ustawienia indywidualne (Konfiguracja użytkownika).
- W systemie plików NTFS ścieżka %windir%\ SYSTEM32\GROUPPOLICY jest dostępna tylko dla administratorów.
- Ustawienia zgromadzone we wspomnianych plikach REGISTRY.POL z folderów USER i MACHINE obowiązują zasadniczo każdego użytkownika logującego się w systemie.

Powstają zatem dwa problemy - z jednej strony restrykcje powinny obejmować tylko konta użytkowników, a można je definiować wyłącznie z poziomu kont administratorów, z drugiej zaś nie należy rozszerzać ograniczeń z pliku REGISTRY.POL na niewłaściwe konta. Najprostsze jest poniższe rozwiązanie.

1. Zaloguj się w systemie jako administrator lub użytkownik o równorzędnych uprawnieniach. W Windows XP otworzysz to okno dialogowe za pomocą polecenia **control userpasswords2** (wpisuje się je po wybraniu menu Start | Uruchom).
2. Przenieś konto, które ma podlegać restrykcjom, tymczasowo do grupy administratorów.
3. Teraz zaloguj się jako użytkownik, którego uprawnienia chcesz zmodyfikować. Uruchom przystawkę Gpedit, po czym wprowadź żądane ograniczenia konta.
4. Zmień nazwę pliku REGISTRY.POL na <nazwa_konta>.POL. Jest to konieczne, bo w przeciwnym razie restrykcje zostaną przejęte przez pozostałe konta.
5. Następnie zaloguj się ponownie jako administrator i przenieś edytowane uprzednio konto do jego pierwotnej grupy (patrz wyżej - punkt 2).

Nie usuwając plików POL tworzonych za pomocą przystawki Gpedit, lecz przydzielając im tylko nową nazwę, zapewnisz sobie możliwość szybkiego ustawiania ograniczeń konta. Wystarczy niewiele modyfikacji dotychczasowej konfiguracji i nie trzeba ustawiać wszystkiego od nowa.

Nic dziwnego, że koncepcja zabezpieczeń podlega opisanym ograniczeniom. Zasady grup opracowano z myślą o domenach serwerowych. Producent nie przewidział stosowania ich w lokalnym systemie, z którego korzysta kilku użytkowników.

Uprawnienia NTFS!!

Jeśli nie ma poważnych przeciwwskazań, systemom Windows 2000 i XP należy już w momencie instalowania przydzielić partycję NTFS. W przeciwnym razie można przekształcić partycję systemową z FAT32 na NTFS już po zainstalowaniu systemu - pomoże ci w tym program CONVERT.EXE. NTFS oferuje rozmaite możliwości sterowania prawami dostępu poszczególnych użytkowników komputera do folderów, a nawet pojedynczych plików. Wszystkie uprawnienia plików i folderów są osadzone w systemie plików.

6. Przydziały uprawnień na partycjach NTFS

Wymuszanie bezpiecznych haseł - dzięki parametrom, takim jak Minimalna długość hasła i Wymagania co do złożoności uniemożliwisz tworzenie za krótkich lub zbyt prostych do odgadnięcia haseł. Lokalne prawa dostępu do poszczególnych plików lub folderów można przydzielać pojedynczym użytkownikom (na podstawie ich kont) lub całym grupom

użytkowników. Rozróżnia się aż 14 operacji, które można dopuszczać, nie dopuszczać - odmówić lub nie odmawiać. **W wypadku wybrania więcej niż jednej opcji priorytet przysługuje tym, które zawężają uprawnienia.** Przydaje się to, gdy trzeba przydzielić określonemu użytkownikowi odmienne prawa dostępu, niż ma cała grupa. Jeśli na przykład udzielisz grupie Znajomi prawa zapisu w pewnym folderze, a jednocześnie odbierzesz je jednemu z członków tejże grupy, tylko on nie będzie mógł dokonywać zapisu.

Zanim będziesz mógł definiować lokalne prawa dostępu w Windows XP Professional, musisz uaktywnić tę funkcję. **Otwórz w tym celu okno Eksploratora i przywołaj menu Narzędzia | Opcje folderów. Przejdź do karty Widok, po czym usuń zaznaczenie pola wyboru Użyj prostego udostępniania plików. Od tej pory w oknie właściwości pliku lub folderu (kliknij go prawym przyciskiem i wskaż polecenie Właściwości) będzie pojawiać się karta Zabezpieczenia. Na niej znajdziesz opcje praw dostępu.**

Blokada wykonywania - w folderze niedysponującym stosownymi uprawnieniami nie mogą uruchamiać się m.in. szkodliwe programy. Okno właściwości pliku lub folderu zawiera na karcie Zabezpieczenia listę wszystkich kont, które mogą mieć jakikolwiek dostęp do tego obiektu. Są wyszczególnione w rubryce Nazwy grupy lub użytkownika. Konta, których nie wymieniono z nazwy w tym zestawieniu lub figurujące w nim tylko jako członkowie określonej grupy, nie mają żadnego dostępu. Za pomocą przycisków Dodaj i Usuń można przydzielać prawa dodatkowym użytkownikom lub wykluczać ich z kręgu uprawnionych. Windows XP wymaga dwóch kliknięć - przycisków Zaawansowane i Znajdź teraz.

Wróciwszy do karty Zabezpieczenia w oknie dialogowym właściwości, możesz przydzielać lub odbierać uprawnienia kontu (lub grupie) wymienionemu w górnej części okna. **Do uprawnień tych zaliczają się m.in. zapis, odczyt, modyfikacja i wykonywanie plików.** Zaznacz w tym celu żądane konto lub grupę. Następnie zaznacz dozwolone operacje w kolumnie Zezwalaj i niedozwolone w kolumnie Odmów. W ten sposób ustalisz prawa dostępu określonych użytkowników do bieżącego pliku lub folderu.

Jeśli chcesz na przykład dopuścić odczyt plików jednego z folderów grupie Krytycy, a jednocześnie uniemożliwić wgląd do tych dokumentów użytkownikowi Wrogi_Krytyk, który jest członkiem tejże grupy, zaznacz wiersz Krytycy w górnej części okna i zaznacz pole wyboru Zezwalaj w wierszu Odczyt. Potem wskaż użytkownika Wrogi_Krytyk i zaznacz pole wyboru Odmów w wierszu Odczyt. Gdybyś usunął jedynie zaznaczenie pola Zezwalaj (również w wierszu Odczyt), pierwszeństwo uzyskałoby prawo grupy, a Wrogi_Krytyk mógłby bez przeszkód zaglądać do dokumentów.

Czym chata bogata? - Gościnność systemów operacyjnych
Użytkownik Gość nie ma domyślnie prawa do logowania się w systemie. Nie zaleca się zmieniać tego ustawienia, bo konto Gość zezwala na logowanie się bez podawania hasła. Jednak podczas udostępniania zasobów w sieci przydałaby się niekiedy możliwość dopuszczenia wszystkich użytkowników bez zakładania dla każdego z nich oddzielnego konta i przydzielania hasła.

Windows XP Home Edition - w tym środowisku goście mają zasadniczo dostęp do udziałów (patrz ramka "Udostępnienia w XP Home"), nawet jeśli konto Gość jest oznaczone jako wyłączone. Dlatego nie trzeba wprowadzać zmian do predefiniowanej konfiguracji udostępnień globalnych.

Windows XP Professional - dostęp konta Gość do udostępnianych folderów odblokujesz za pośrednictwem zasady Odmowa dostępu do tego komputera z sieci. Okno z wykazem użytkowników zawiera pewne nieścisłości. Podobnie jak w XP Home Edition, konto Gość jest domyślnie wyłączone. Tymczasem ustawienie to dotyczy wyłącznie (braku) prawa do lokalnego logowania się w systemie.

Pamiętaj również o tym, że korzystanie z udostępnionych folderów przez sieć wymaga przydzielenia kontu Gość lokalnego prawa do odczytu zasobów.

Klikając przycisk Zaawansowane i wybierając żądane konto, dostaniesz się do czternastu dodatkowych praw oferowanych przez NTFS (noszą nazwę uprawnień specjalnych), które pozwalają bardziej szczegółowo określać dozwolone i zabronione operacje niż jest to możliwe za pomocą praw podstawowych (zwanych uprawnieniami standardowymi), opisanych powyżej. Dzięki nim możesz na przykład zablokować wykonywanie pliku, a jednocześnie dopuścić jego odczytywanie. Aby uzyskać obszerny opis uprawnień, przywołaj pomoc systemu Windows XP, wpisz uprawnienia specjalne, po czym wskaż łącze Uprawnienia specjalne dla plików i folderów w rubryce Wyniki wyszukiwania.

Oprócz tego powyższe okno pozwala przenosić prawa dostępu na obiekty podrzędne, czyli podfoldery (patrz dziedziczenie - punkt 7).

7. Dziedziczenie i uprawnienia czynne

Po uaktywnieniu dziedziczenia uprawnienia zdefiniowane dla określonego folderu obowiązują również pliki w podfolderach. Funkcję dziedziczenia można włączyć tylko dla folderów, dla plików już nie. Przywołaj właściwości żądanego obiektu - pliku lub folderu - i przejdź do karty Zabezpieczenia. Gdy klikniesz przycisk Zaawansowane, pojawi się kolejne okno dialogowe (Zaawansowane ustawienia zabezpieczeń), a w nim pole wyboru Dziedzicz po obiekcie nadrzędnym wpisy uprawnienia stosowane do obiektów podrzędnych. Uwzględnij je razem z wpisami tutaj zdefiniowanymi (Windows XP Professional). Właśnie nim włącza się bądź wyłącza dziedziczenie praw dostępu. Oprócz tego trzeba określić zakres dziedziczenia. Domyślnie uprawnienia obowiązują w wybranym folderze, wszystkich podfolderach i zawartych w nich plikach. Chcąc ustalić inny zasięg dziedziczenia, kliknij przycisk Edytuj, otwórz pole listy Zastosuj dla i zaznacz stosowną opcję, np. Tylko pliki lub Ten folder i podfoldery. Ponadto możesz ograniczyć dziedziczenie do jednej płaszczyzny podfolderów. Służy do tego pole wyboru Zastosuj te uprawnienia jedynie dla obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera. Zwróć jednak uwagę, że stosując tę funkcję możesz usunąć dotychczasowe uprawnienia obowiązujące w bardziej zagnieżdżonych podfolderach (czyli w folderach na niższych płaszczyznach).

W obliczu tak zawiłych struktur, jak indywidualne pozwolenia i zakazy, przynależności do grup czy dziedziczenie uprawnień, niełatwo ustalić, jakie prawa dostępu do określonych zasobów dyskowych ma dany użytkownik. W środowisku Windows XP Professional służy pomocą karta Czynne uprawnienia. Gdy wybierzesz grupę lub użytkownika, system wyświetli jej/jego bieżące uprawnienia.

8. Na admina nie ma rady

Konta z grupy administratorzy nie podlegają żadnym realnym ograniczeniom. Można, co prawda, zablokować administratorowi dostęp do plików czy folderów, jednak mija się to z

celem. **Każdy administrator ma prawo przejąć na własność dowolny obiekt na dysku i dokonać na nowo podziału uprawnień.**

Aby przejąć prawo własności danego folderu, przywołaj jako administrator okno Zaawansowane ustawienia zabezpieczeń (jw.) i przejdź do karty Właściciel. Następnie zaznacz swe własne konto na liście Zmień właściciela na, po czym potwierdź przyciskiem Zastosuj. W ten sposób odzyskasz pełny dostęp do folderu - wystarczy zamknąć i ponownie otworzyć okno Właściwości, dodać swoje konto na karcie Zabezpieczenia i przydzielić uprawnienie Pełna kontrola.

9. Bezpieczne szyfrowanie

Prawo dziedziczenia - nowy folder otrzymuje uprawnienia obiektów nadrzędnych. W razie potrzeby możesz to zmieniać. Jak wspomniałam w punkcie 4., na nic prawa dostępu, gdy ktoś spróbuje dostać się do danych z poziomu innego systemu operacyjnego. Chcąc się zabezpieczyć przed próbami podglądania i wykradania danych w ten sposób, zaszyfruj zasoby na partycjach NTFS. Jest to możliwe w środowiskach Windows 2000 i XP Professional. Aby zaszyfrować plik lub folder, kliknij go prawym przyciskiem myszy i wskaż polecenie Właściwości. W dalszej kolejności kliknij przycisk Zaawansowane na karcie Ogólne, zaznacz pole wyboru Szyfruj zawartość, aby zabezpieczyć dane i potwierdź przyciskiem OK.

Jeśli często korzystasz z szyfrowania danych, możesz ułatwić sobie dostęp do tej funkcji, umieszczając ją w podręcznym menu folderów i plików. Przywołaj w tym celu Edytor rejestru(Start->Uruchom->regedit i enter) i przejdź do klucza "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advancd ". Utwórz w nim nową wartość DWORD o nazwie "EncryptionContextMenu", po czym przypisz jej cyfrę 1 w polu danych. Zmiany zaczną obowiązywać, gdy zrestartujesz system. Teraz wystarczy kliknąć żądany plik czy folder prawym przyciskiem myszy i wybrać polecenie Szyfruj.

Karta Czynne uprawnienia okaże się bezcenną pomocą, gdy zechcesz ustalić, jakie prawa dostępu ma określony użytkownik. Niezależnie od metody, którą inicjujesz szyfrowanie (przez okno właściwości lub bezpośrednio z menu podręcznego), z zabezpieczonych plików i folderów korzysta się tak samo, jak z niezaszyfrowanych zasobów. Deszyfrowanie jest realizowane w tle bez ingerencji i wiedzy użytkownika. Oprócz ciebie nikt inny (nawet żaden z członków grupy Administratorzy) nie odczyta danych ani nie skopiuje ich na partycję FAT32. Wyjątek stanowi administrator (nie grupa Administratorzy) w środowisku Windows 2000. Dysponuje on kluczem do odzyskiwania danych, który pozwala mu odczytywać wszystkie dane w obrębie systemu.

Pamiętaj, że po przeniesieniu dysku do innego komputera lub zainstalowaniu na nim innego systemu operacyjnego, stracisz dostęp do zaszyfrowanych plików i folderów. Dlatego wyodrębnij zawczasu swój prywatny klucz i umieść jego zapasową kopię w bezpiecznym miejscu. Uruchom przeglądarkę Internet Explorer i otwórz menu Narzędzia | Opcje internetowe. Przejdź do karty Zawartość, po czym kliknij przycisk Certyfikaty. Następnie zaznacz swój klucz. Rozpoznasz go po nazwie - powinna się zgadzać z nazwą, pod którą logujesz się w systemie. Ponadto jego okres ważności ma wynosić aż sto lat, a w rubryce Zamierzone cele certyfikatu powinien widnieć napis System plików szyfrowania. Kliknij przycisk Eksportuj. W kreatorze eksportu certyfikatów wybierz opcję Tak, eksportuj klucz prywatny. Wpisz hasło i zapisz plik z kluczem np. na CD. W nowym systemie (lub

komputerze) zaimportuj klucz - wystarczy przywołać plik dwukrotnym kliknięciem myszy i podać właściwe hasło.

10. Udostępnienia z zabezpieczeniem

Lokalne prawa dostępu do zasobów dyskowych definiuje się na karcie Zabezpieczenia (Windows XP Professional) w oknie właściwości pliku lub folderu. Przechodząc do karty Udostępnianie lub wskazując polecenie Udostępnianie i zabezpieczenia w menu podręcznym folderów, dostaniesz się do funkcji udostępniania zasobów w sieci. Za pośrednictwem tego okna możesz, będąc administratorem, umożliwiać korzystanie z plików i folderów użytkownikom spoza komputera. Wystarczy zaznaczyć opcję Udostępnij ten folder i wpisać dowolną nazwę w pole Nazwa udziału - właśnie pod nią będzie figurował w sieci. Po kliknięciu przycisku Uprawnienia przydzielisz użytkownikom bądź grupom zarejestrowanym w systemie prawa do udostępnianych zasobów. Windows XP dopuszcza tylko użytkowników z własnym kontem w systemie udostępniającym zasoby dyskowe. **Warunkiem udostępniania w Windows XP Professional jest wyłączenie tzw. prostego udostępniania plików i folderów** (sposób wykonania tej czynności opisaliśmy w poradzie 6).

Przystawka FSMGMT.MSC oferuje bardzo przejrzysty podgląd udziałów, bieżących sesji i otwartych plików. Obowiązuje zasada, że zasobom udostępnianym wszystkim użytkownikom sieci należy przyporządkować uprawnienia konta Gość.
Wprawdzie Eksplorator wyróżnia udostępnione foldery specjalną ikoną (dłoń pod żółtym skoroszytem), ale lepszy przegląd udostępnień zapewnia bez wątpienia narzędzie FSMGMT.MSC. Przywołuje się je, klikając menu Start | Uruchom i wpisując polecenie fsmgmt.msc. Przedstawiony program wyświetla przejrzystą listę wszystkich udziałów, bieżących sesji i otwartych w danej chwili plików. Oprócz tego potrafi zatrzymywać udostępnianie i tworzyć nowe udziały.

11. Ukryte udostępnienia

W środowisku Windows XP Professional przystawka FSMGMT.MSC podaje, że każda partycja dysku jest udostępniona w sieci pod nazwą <litera>$. Są to udostępnienia tworzone do celów administracyjnych. Właściciele kont dysponujący uprawnieniami administratora mają dzięki temu dostęp w trybie odczytu i zapisu do wszystkich partycji na twoich dyskach. Symbol dolara ($) na końcu nazwy udziału powoduje, że udostępnienie nie jest widoczne w oknie otoczenia sieciowego (Moje połączenia sieciowe) innych komputerów. Jednak każdy, kto ma prawa administratora, może odwoływać się do udostępnionych zasobów poleceniem \\nazwa_komputera\litera$ (czyli np. \\kowalski\c$). Jeśli sam założyłeś podstawowe konto administratora i konta wszystkich pozostałych członków grupy Administratorzy, nie stanowi to żadnego ryzyka.

Gdybyś mimo to chciał wyłączyć udostępnienia administracyjne, otwórz Edytor rejestru(Start->Uruchom->regedit) i przejdź do klucza "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameter" Załóż w nim wartość DWORD o nazwie "AutoShareWks" i przyporządkuj jej cyfrę 0. Udziały znikną po ponownym uruchomieniu systemu Windows.

Umieszczając symbol dolara na końcu nazwy, możesz zamaskować własne udziały, aby nie były widoczne w oknie środowiska sieciowego w innych komputerach. Kamuflaż działa

jednak tylko w Eksploratorze, dlatego warto zdefiniować prawa dostępu tak, aby wykluczyć podgląd udostępnianych zasobów przez nieupoważnionych użytkowników.

Program MMC, czyli Microsoft Management Console
jest to konsola obsługi narzędzi administracyjnych (przystawek).
Przystawki służą do wykonywania zadań administracyjnych oraz naprawczych.

Aby wywołać określoną przystawkę systemu, w Menu Start --> Uruchom --> wpisz jej nazwę z rozszerzeniem "msc" --> kliknij OK. Przykładowo wpisanie "gpedit.msc" otworzy przystawkę "Zasady grupy". Niektóre przystawki wymagają podniesienia uprawnień. Wtedy należy uruchomić konsolę w trybie administratora.

Obecność przystawki jest zależna od systemu operacyjnego oraz obecności dodatkowego oprogramowania.

Przystawki:
azman.msc ----> Menedżer autoryzacji
certmgr.msc ----> Certyfikaty
certsrv.msc ----> Urząd certyfikacji
certtmpl.msc ----> Szablony certyfikatów
ciadv.msc ----> Usługa indeksowania
comexp.msc ----> Usługi składowe
compmgmt.msc ----> Zarządzanie komputerem
dcpol.msc ----> Domyślne ustawienia zabezpieczeń kontrolera domeny
devmgmt.msc ----> Menadżer urządzeń
dfrg.msc ----> Defragmentator dysków
dfsgui.msc ----> Rozproszony system plików (DFS)
dhcpmgmt.msc ----> Menedżer DHCP
diskmgmt.msc ----> Zarządzanie dyskami
dnsmgmt.msc ----> Menedżer DNS
domain.msc ----> Domeny i relacje zaufania usługi Active Directory
dompol.msc ----> Domyślne ustawienia zabezpieczeń domeny
dsa.msc ----> Użytkownicy i komputery usługi Active Directory
dssite.msc ----> Lokacje i usługi Active Directory
eventvwr.msc ----> Podgląd zdarzeń
fsmgmt.msc ----> Foldery udostępnione
filesvr.msc ----> Zarządzanie serwerem plików
gpedit.msc ----> Zasady grupy
gpmc.msc ----> Zarządzenie zasadami grupy
ias.msc ----> Usługa uwierzytelniania internetowego
iis.msc ----> Menedżer internetowych usług informacyjnych (IIS)
iis6.msc ----> Menedżer internetowych usług informacyjnych (IIS) 6.0
lusrmgr.msc ----> Użytkownicy i grupy lokalne
napclcfg.msc ----> Konfiguracja klienta ochrony dostępu do sieci

ntmsmgr.msc ----> Magazyn wymienny
ntmsoprq.msc ----> Żądania operatora magazynu wymiennego
perfmon.msc ----> Wydajność (Monitor niezawodności i wydajności)
printmanagement.msc ----> Zarządzanie drukowaniem
rrasmgmt.msc ----> Routing i dostęp zdalny
rsop.msc ----> Wynikowy zestaw zasad
secpol.msc ----> Ustawienia zabezpieczeń lokalnych
services.msc ----> Usługi
SQLServerManager.msc ----> SQL Server Configuration Manager
taskschd.msc ----> Harmonogram zadań
tapimgmt.msc ----> Telefonia
tpm.msc ----> Zarządzanie modułem TPM na komputerze lokalnym
tscc.msc ----> Konfiguracja usług terminalowych\Połączenia
tsmmc.msc ----> Pulpity zdalne
wf.msc ----> Zapora systemu Windows z zabezpieczeniami zaawansowanymi
wmimgmt.msc ----> Sterowanie usługą WMI (Windows Management Infrastructure)

Przystawki możesz znaleźć w folderze systemowym Windows na dysku (c:/Windows/system32)