

Przewodnik bezpieczeństwa Microsoft Windows XP

Operational Network Evaluations Division of the Systems and Network Attack Center (SNAC)

Operacyjna sieciowa jednostka centrum oceny ataków systemowych i sieciowych

Autorzy:

R. Bickel
M. Cook
J. Haney
M. Kerr, DISA
CT01 T. Parker, USN
H. Parkes

Tłumaczenie dla

Jama Mastaha
(infojama.pl)

WCF Translate TEAM

Alfik | TheCrow | Wyrwa



Zaktualizowane:

Październik 30, 2002
Wersja: 1.0

Przetłumaczone

:
30 Styczeń 2003
Wersja: 1.0

National Security Agency – Agencja Bezpieczeństwa Narodowego
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704
XPGuides@nsa.gov

Ta strona celowo jest pusta

Informacja

SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE

Podziękowania

Autorzy pragną podziękować autorom "Przewodnika bezpieczeństwa Microsoft Windows 2000.

Autorzy pragną również podziękować Sherri Bavis za przeglądnięcie tego dokumentu i wszystkie działania uczestniczące w testowaniu tego przewodnika. Twoje komentarze i sugestie były nieocenione.

Informacje dotyczące znaków towarowych

Microsoft, MS-DOS, Windows, Windows XP, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups i Windows 3.1 są zarejestrowanymi znakami towarowymi firmy Microsoft Corporation w USA i wszystkich pozostałych państwach.

Wszystkie pozostałe nazwy są zarejestrowanymi znakami towarowymi szanowanych firm.

Pewne części tego dokumentu zostały zaciągnięte z materiałów opublikowanych przez Microsoft za ich zgodą

Spis treści

Spis treści	vi
Spis rysunków	x
Spis tabel	xi
Rozdział 1 Istotne informacje dotyczące użytkowania tego przewodnika	1
<i>Założenia</i>	1
<i>Ostrzeżenia przed rozpoczęciem używania przewodnika</i>	2
<i>Konwencje i powszechnie używane terminy</i>	2
Użytkownicy i użytkownicy zautentykowani (autentyczni)	2
Zmienne systemowe	3
Lokalizacja narzędzi administracyjnych	3
<i>O przewodniku bezpieczeństwa Microsoft Windows XP</i>	3
Rozdział 2 Co nowego w bezpieczeństwie Windows XP	7
<i>Zmiany cech bezpieczeństwa</i>	7
Członek grupy Wszyscy	7
Zarządzanie własnością	7
Instalacja drukarek	7
Restrykcje pustego hasła	7
Zmiany	8
Podsystemy	8
System kodowania	8
<i>Nowe cechy bezpieczeństwa</i>	8
Zasady ograniczania oprogramowania	8
Nazwy przechowywanych użytkowników i haseł	9
Nowe konta usług	9
Konto Lokalnego Systemu	9
Konto lokalne sieci	9
Konto lokalnych usług	10
Rozdział 3 Wprowadzenie do menadżera narzędzi konfigurowania bezpieczeństwa	11
<i>Funkcjonalność konfigurowalności bezpieczeństwa</i>	12
Graficzny Interfejs Użytkownika konfiguracji bezpieczeństwa	12
Narzędzia Wiersza Poleceń konfiguracji bezpieczeństwa	12
<i>Szablony bezpieczeństwa</i>	13
Ładowanie szablonów zakładek bezpieczeństwa do MMC	13
Podgląd Tekstu Szablonów Bezpieczeństwa	14
Pliki konfiguracji bezpieczeństwa	14
Domyślne szablony bezpieczeństwa	15
Dostarczone przez Microsoft szablony	15
Szablony bezpieczeństwa publikowane przez NSA	15
<i>Zanim dokonasz zmian bezpieczeństwa</i>	15
<i>Lista kontrolna dla aktualizacji rekomendacji tego przewodnika</i>	15
Rozdział 4 Modyfikacja zasady ustawień kont przy pomocy szablonów bezpieczeństwa	19
<i>Zasady haseł</i>	19
<i>Zasady kont</i>	22
<i>Zasady Kerberos</i>	23

Rozdział 5 Modyfikacja ustawień Zasady Lokalnej przy użyciu szablonów bezpieczeństwa	
<i>Zasady audytu</i>	25
<i>Obowiązkowe prawa użytkowników</i>	25
<i>Opcje bezpieczeństwa</i>	28
<i>Dodawanie pozycji do opcji bezpieczeństwa</i>	32
Usuwanie przerobionych opcji	47
Rozdział 6 Modyfikacja ustawień Dziennika Zdarzeń przy użyciu szablonów bezpieczeństwa	48
<i>Ustawienia dziennika zdarzeń</i>	49
<i>Zarządzanie zapisami zdarzeń</i>	50
Zapisywanie i czyszczenie zapisów audytu	50
Resetowanie ustawień pliku zdarzeń audytu po zatrzymaniu systemu	51
Rozdział 7 Zarządzanie Grupami Restrykcji przy użyciu szablonów bezpieczeństwa	53
<i>Modyfikacja Grup Restrykcji poprzez zakładki szablonów bezpieczeństwa</i>	53
Rozdział 8 Zarządzanie usługami systemowymi przy użyciu szablonów bezpieczeństwa	55
<i>Modyfikacja usług systemowych poprzez zakładki szablonów bezpieczeństwa</i>	55
<i>Bezpieczeństwo usług systemowych</i>	57
Rozdział 9 Modyfikacja ustawień bezpieczeństwa rejestru przy użyciu szablonów bezpieczeństwa	59
<i>Model dziedziczenia</i>	59
<i>Zezwolenia rejestru</i>	59
Efektywne prawa	61
<i>Modyfikacja ustawień rejestru poprzez zakładki szablonów bezpieczeństwa</i>	61
Modyfikacja zezwoleń na kluczu rejestru	61
Dodawanie klucza rejestru do konfiguracji bezpieczeństwa	64
Wyłączanie klucza rejestru z konfiguracji bezpieczeństwa	65
<i>Rekomendowane zezwolenia klucza rejestru</i>	65
Rozdział 10 Modyfikacja ustawień bezpieczeństwa systemu plików przy użyciu szablonów bezpieczeństwa	73
<i>Konwersja do NTFS</i>	73
<i>Prawa dostępu plików i folderów</i>	74
Podstawy zezwoleń	74
Prawa dostępu folderów	75
Prawa dostępu plików	76
Efektywne prawa	76
<i>Modyfikacja ustawień systemu plików poprzez zakładki szablonów bezpieczeństwa</i>	76
Modyfikacja praw dostępu na pliku lub folderze	77
Dodawanie plików lub folderów do konfiguracji bezpieczeństwa	79
Wyłączanie plików lub folderów z konfiguracji bezpieczeństwa	79
<i>Rekomendowane prawa dostępu plików i folderów</i>	80
Rozdział 11 Konfiguracja bezpieczeństwa i analizy	91
<i>Ładowanie konfiguracji bezpieczeństwa i zakładek Analizy do MMC</i>	91
<i>Baza konfiguracji bezpieczeństwa</i>	91
<i>Opcje wiersza poleceń</i>	93
<i>Optymalizacja analizy bezpieczeństwa</i>	94
Optymalizacja analizy bezpieczeństwa przy pomocy wiersza poleceń	94
Optymalizacja analizy bezpieczeństwa przy pomocy graficznego interfejsu użytkownika	94
<i>Konfigurowanie systemu</i>	95

Konfiguracja Systemu poprzez Wiersz Poleceń	95
Konfiguracja Systemu poprzez Graficzny Interfejs Użytkownika	96
Rozdział 12 Uaktywnianie zasady grup Windows XP Group Policy w domenie Windows 2000	97
<i>Wprowadzenie</i>	97
<i>Rozszerzenia ustawień bezpieczeństwa</i>	97
<i>Tworzenie Zasady Grupy w Windows XP</i>	98
<i>Importowanie Szablону bezpieczeństwa do Zasady Grupy</i>	98
<i>Zarządzanie Windows XP GPO z kontrolera domeny Windows</i>	99
<i>Obiekty lokalnej zasady grupy</i>	100
<i>Uaktualnianie zasady grupy</i>	100
<i>Podgląd rezultatów ustawień zasady</i>	100
Zakładka RsoP	100
Gpresult.exe	101
<i>Znane sprawy</i>	101
Restrykcja na ustawienia użytkownika anonymous I “użytkownik musi zmienić hasło przy następnym logowaniu”	101
Rozdział 13 Zdalna pomoc/konfiguracja pulpitu	103
<i>Zdalna pomoc</i>	103
Zabieganie o zdalną pomoc	103
Możliwości zdalnej pomocy	104
<i>Połączenia zdalnego pulpitu</i>	105
<i>Zasady grupy – Szablony administracyjne</i>	107
Usługi terminalowe	107
<i>Rekomendacje ustawień sieciowych</i>	110
Rozdział 14 Konfiguracja Firewall dla połączenia Internetowego	111
<i>Rekomendowane użycie</i>	111
<i>Cechy</i>	111
Pełna inspekcja pakietów	111
Protekcja przed skanowaniem portów	111
Zapis zdarzeń bezpieczeństwa	112
Czego nie dostarcza	112
<i>Uaktywnianie ICF</i>	112
<i>Podsumowanie</i>	117
Rozdział 15 Dodatkowe ustawienia bezpieczeństwa	119
<i>Rekomendacje dotyczące kont administratorów</i>	119
Dodatkowe konta Administratora	119
Użycie konta administratora I komendy uruchom jako	120
<i>Prawa do udostępnionych zasobów</i>	120
Ustawianie praw zasobów	121
Rekomendacje bezpieczeństwa udostępnianych zasobów	121
<i>Usuwanie klucza rejestru POSIX</i>	122
<i>Dodatkowe ustawienia zasady grupy</i>	122
Wyłączanie zdalnej pomocy / pulpitu	122
Inicjalizacja sieciowa	123
Wyłączanie automatycznego odtwarzania mediów	124
<i>Blokowanie pakietów NetBIOS w ustawieniach sieci</i>	124

Rozdział 16 Modyfikacje Microsoft Windows XP w domenie Windows NT	125
<i>Brak zasady grupy</i>	125
<i>Ustawienia NTLM I menedżera</i>	125
<i>Mocny klucz sesji</i>	125
<i>Autozapisywanie</i>	126
Dodatek A Przykładowy banner logowania Dodatek B Referencje	127

Tabela rysunków

Rysunek 1 Zakładka szablonów bezpieczeństwa	14
Rysunek 2 Rekomendacje zasady haseł	20
Rysunek 3 Rekomendacje zasady Audytu	26
Rysunek 4 System Services	57
Rysunek 5 Opcje zezwoleń modyfikacji konfiguracji rejestru	62
Rysunek 6 Zawansowane ustawienia bezpieczeństwa	63
Rysunek 7 Okno zezwoleń dla klucza rejestru	64
Rysunek 8 Opcje konfiguracji praw pliku	78
Rysunek 9 Okno zezwoleń dla plików i folderów	79
Rysunek 10 Konfiguracja sekcji plików	92
Rysunek 11 Rezultaty analizy bezpieczeństwa	95
Rysunek 12 Rozszerzone ustawienia bezpieczeństwa GPO	99
Rysunek 13 Zakładka RsoP	101
Rysunek 14 Uaktywnianie ICF	113
Rysunek 15 Tabela usług	114
Rysunek 16 Przykładowe ustawienia usług	115
Rysunek 17 Tabela zdarzeń bezpieczeństwa	116
Rysunek 18 Tabela ICMP	117

Spis Tabel

Tabela 1 Opcje zasady haseł	22
Tabela 2 Opcje dotyczące kont	23
Tabela 3 Opcje zasady Kerberos	24
Tabela 4 Opcje zasady audytu	28
Tabela 5 Opcje praw użytkowników	32
Tabela 6 Opcje bezpieczeństwa	46
Tabela 7 Opcje dziennika zdarzeń	50
Tabela 8 Opis I prawa rejestru	60
Tabela 9 Opcje zezwoleń rejestru	60
Tabela 10 Rekomendowane zezwolenia rejestru	71
Tabela 11 Opis I prawa dostępu plików	74
Tabela 12 Opcje praw folderów	75
Tabela 13 Opcje praw plików	76
Tabela 14 Rekomendowane prawa folderów i plików	90
Tabela 15 Parametry wiersza poleceń	94
Tabela 16 Opcje zasady usług terminalowych	109

Ta strona celowo jest pusta

Istotne informacje na temat używania przewodnika

Celem tego dokumentu jest poinformowanie czytelników o rekomendowanych ustawieniach zabezpieczeń w systemie Microsoft Windows XP Professional. Ustawienia bezpieczeństwa mogą być ustawione dzięki Menedżerowi Konfiguracji Bezpieczeństwa, poprzez Zasady Grupy, a także poprzez ustawienia ręczne.

Windows XP Professional jest systemem przeznaczonym dla klienta. Odpowiednik systemu przeznaczony do zastosowań serwerowych nie został jeszcze wydany. Dlatego też, ten dokument będzie przeznaczony dla Windows XP w połączeniu z domeną Windows 2000 i aktywną usługą Active Directory i Zasady Grupy. Dodatkowe informacje o Obiektach Zasady Grupy są adresowane jako dodatkowe do Przewodnika bezpieczeństwa Zasady Grupy Windows 2000, który powinien być przeczytany przed rozpoczęciem korzystania z niniejszego przewodnika.



Uwaga: Przewodnik ten nie jest adresowany w kontekście bezpieczeństwa Windows XP Home Edition lub wolnostojącej (nie podpiętej do domeny) wersji Windows XP Professional

Pomimo faktu, iż podstawowymi założeniami przewodnika jest opis bezpieczeństwa Windows XP w domenie Windows 2000, rozdział 16 omawia rekomendowane ustawienia bezpieczeństwa w sytuacji występowania Windows XP w domenie Windows NT 4.0

Wraz z przewodnikiem został dołączony szablon bezpieczeństwa winxp_workstation.inf. Cel i użycie tego szablonu zostało umówione w dalszej części tego dokumentu. Dokument ten przeznaczony jest dla administratorów sieci Windows, ale może być również wykorzystany przez każdą osobę zaangażowaną i zainteresowaną Windows XP lub bezpieczeństwem sieciowym

Założenia

Następujące zasadnicze założenia zostały poczynione by zminimalizować obszerność tego dokumentu: W sieci znajdują się jedynie komputery z uruchomionym systemem Windows 2000 i Microsoft Windows XP Professional (wersja instalacyjna pełna, nie upgrade)



Uwaga: Rozdział 16 omawia sprawy zaangażowane w proces dodawania Windows XP do domeny Windows NT 4.0

Komputery Windows XP używają zapisu na dyskach w systemie plików NT (NTFS). Kontrolery domeny są komputerami z zainstalowanymi Windows 2000 Domain z uruchomionymi usługami Active Directory



Uwaga: Rozdział 16 omawia sprawy zaangażowane w proces dodawania Windows XP do domeny Windows NT 4.0.

Zostały zainstalowane ostatnie service pack'i oraz htfix'y na systemy. By uzyskać najnowsze informacje o krytycznych aktualizacjach należy udać się na stronę <http://windowsupdate.microsoft.com> lub przeglądać w poszukiwaniu najnowszych aktualizacji pod względem bezpieczeństwa przeglądając Biuletyn Bezpieczeństwa Technet: <http://www.microsoft.com/technet/security/current.asp>.

Wszystkie komputery działające w sieci oparte są o architekturę i platformę Intel'a. Aplikacje są kompatybilne z Windows XP. Użytkownicy niniejszego podręcznika posiadają wiedzę z zakresu instalacji Windows XP i Windows 2000 oraz podstawowych czynności administracyjnych.

Ostrzeżenia przed rozpoczęciem korzystania z Przewodnika

Użytkownik powinien przeczytać i zaakceptować następujące ostrzeżenia przed rozpoczęciem konfiguracji sieci zgodnie z rekomendacjami przewodnika:

- Nie wdrażaj żadnych ustawień z tego przewodnika bez wcześniejszego przetestowania ich w środowisku nieprodukcyjnym
- Ten dokument zawiera tylko przewodnik zawierający rekomendowane ustawienia bezpieczeństwa. Nie oznacza to, że należy zastąpić dobrze zorganizowanej aktualnej zasady bezpieczeństwa. Ponadto, przewodnik nie jest zaadresowany do specyficznych wymogów stawianych pewnym konfiguracjom. Szczególną uwagę należy zachować podczas implementacji przewodnika w systemach z zainstalowanymi pozostałymi produktami takimi jak Microsoft Exchange, IIS i SMS.
- Zmiany bezpieczeństwa opisywane w dokumencie odnoszą się jedynie do Microsoft Windows XP Professional i nie powinny być implementowane na innych systemach Windows
- Windows XP może zostać poważnie osłabiony lub wyłączony implementując niewłaściwe zmiany używając programów (np.: Menedżer Konfiguracji Bezpieczeństwa, Regedit.exe) do zmiany konfiguracji systemu. Dlatego też, niezmiernie ważne staje się przetestowanie wszystkich rekomendowanych ustawień z tego przewodnika przed wdrożeniem ich na środowisko produkcyjne.

Uwaga: W Windows XP, regedt32.exe jest nazwany jako regedit.exe.

- Obecnie nie istnieją funkcje "Cofnij" dla operacji usunięcia wpisów w rejestrze. Edytor rejestru (Regedit.exe) prosi o potwierdzenie operacji usunięcia. Kiedy klucz rejestru ma zostać usunięty pojawia się stosowny komunikat nie zawierający jednak nazwy klucza. Sprawdź dokładnie zaznaczony obszar przed wykonaniem jakiegokolwiek usuwania.

Konwencje i często używane zwroty, pojęcia

Użytkownicy i użytkownicy autentykowani

Dla Kontrolnej Listy Dostępu (ACLs) w Windows XP, Microsoft stworzył szeroki użytek z grup użytkowników. Standardowo grupy użytkowników zawierają grupę użytkowników autentykowanych – lokalnych oraz członków domeny Członkowie grup użytkowników mogą być kontrolowani przez administratorów, co jest powodem Microsoft'u dla użycia tych grup w ACLs. Obejrzyj standardowy schemat bezpieczeństwa dla stemów typu workstation (więcej informacji znajduje się w następnym rozdziale)

grupa użytkowników jest używana w prawach dostępu do plików i rejestru tak jak przyznane użytkownikom odpowiednie prawa.

Ten przewodnik przyjął następujące konwencje nazewnictwa Microsoft. Nie mogą zostać utracone ustawienia bezpieczeństwa jeśli wybierze się zastąpienie grupy użytkowników grupom użytkowników autentykowanych na stacji roboczej.

Zmienne Systemowe

Następujące zmienne systemowe zostały wykorzystane w niniejszym dokumencie:

- %SystemDrive% - litera napędu na którym został zainstalowany Windows XP. Zwykle będzie do C:\
- %SystemRoot% - Główny folder zawierający systemu Windows XP
- Zwykle zapis ten wygląda jako: %SystemDrive%\WINDOWS.
- %SystemDirectory% - %SystemRoot%\system32
- %ProgramFiles% - Folder, w którym większość aplikacji jest instalowana Zwykle wygląda on tak: usually %SystemDrive%\Program Files .
- %AllusersProfile% - Folder, w którym przechowywany jest profil All Users Zwykle jest to: %SystemDrive%\Documents and Settings\All Users.

Lokalizacja Narzędzi Administracyjnych

Domyślnie, menu Narzędzi Administracyjnych nie pojawia się w Windows XP w Start menu. By zobaczyć menu Narzędzi Administracyjnych w Start menu należy:

- Kliknąć prawym klawiszem myszki na pasku zadań (zwykle na dole okneanu)
- wybierz właściwości w rozwijanym menu
- wybierz zakładkę Menu Start
- kliknij na przycisku Dostosuj
- wybierz zakładkę zaawansowane
- pod sekcją Elementy Menu Start znajdź sekcję Systemowe Narzędzia Administracyjne
- wybierz Wyświetl w menu wszystkie programy lub Wyświetl w menu wszystkie programy I w menu start

Przewodnik ten pozwolił by Narzędzia Administracyjne były dostępne z menu wszystkie programy.

O przewodniku bezpieczeństwa Microsoft Windows XP

Niniejszy dokument zawiera następujące rozdziały:

Rozdział 1, "Istotne informacje o używaniu przewodnika" dostarcza ważnych informacji I ostrzeżeń, które powinny zostać przeczytane przed użyciem przewodnika.

Rozdział 2, "Co nowego w bezpieczeństwie Windows XP" daje krótki przegląd nowych cech bezpieczeństwa Windows XP.

Rozdział 3, "Wstęp do Menedżera narzędzi konfiguracji bezpieczeństwa" dostarcza przeglądu ustawień wymienionych narzędzie oraz opisuje jak używać szablonów bezpieczeństwa razem z Konsolą Zarządzania Microsoft - Microsoft Management Console (MMC). Omawia jak, implementować, edytować oraz tworzyć nowe pliki konfiguracji bezpieczeństwa. Rozdział opisuje także detale dotyczące pliku konfiguracji bezpieczeństwa dołączonego do tego dokumentu.

Rozdział 4, "Modyfikacja Zasad ustawień kont używając szablonów bezpieczeństwa," wyjaśnia jak ustawić zasady kont w domenie przy użyciu szablonów bezpieczeństwa. Sekcja ta również porusza tematykę zasad haseł, zasad blokowania kont oraz zasad Kerberos.

Rozdział 5, "Modyfikacja ustawień lokalnych zadań przy użyciu szablonów bezpieczeństwa" pokazuje jak używać zakładki szablonów bezpieczeństwa do implementacji i modyfikacji ustawień lokalnych zasad. Opisane zostały sugerowane zasady dla audytu, praw użytkownika oraz atrybutów bezpieczeństwa.

Rozdział 6, "Modyfikacja ustawień dziennika zdarzeń przy użyciu szablonów bezpieczeństwa," wyjaśnia jak przechwytywać, przeglądać, i przechowywać zdarzenia krytyczne, które występuje na sieci przez modyfikację ustawień dziennika zdarzeń.

Rozdział 7, "Zarządzanie restrykcjami grup przy pomocy szablonów bezpieczeństwa," opisuje jak zarządzać członkami grup przy użyciu opcji restrykcji grup.

Rozdział 8, "Zarządzanie usługami systemowymi przy pomocy szablonów bezpieczeństwa," pokazuje jak zarządzać ustawieniami usług systemowych takich jak modele startowe, lista dostępu przy pomocy szablonów bezpieczeństwa. Sekcja ta opisuje jak ustawienia są uaktywniane, jakie są prawa kontroli użytkowników i grup oraz opcje wykonywania, zapisu, usuwania, zatrzymywania, wstrzymywania usługi.

Rozdział 9, "Modyfikacja ustawień bezpieczeństwa rejestru przy użyciu szablonów bezpieczeństwa," omawia jak konfigurować listę dostępu do Kluczy Rejestru. Omówione zostały także ustawienia rekomendowane.

Rozdział 10, "Modyfikacja ustawień bezpieczeństwa systemu plików przy użyciu szablonów bezpieczeństwa," prowadzi czytelników przez czynności konieczne do modyfikacji praw dostępu do plików i folderów przy użyciu zakładki szablonów bezpieczeństwa. Dodatkowa sekcja ta opisuje rekomendowane ustawienia praw dostępu.

Rozdział 11, "Konfiguracja bezpieczeństwa I Analiza," wyjaśnia jak optymalizować analizę bezpieczeństwa poprzez konfigurację zakładki konfiguracji bezpieczeństwa I analizy lub poprzez narzędzia wiersza poleceń, gdy dokonano zmian w ustawieniach.

Rozdział 12, "Uaktywnianie Zasad Grupy Windows XP w domenie Windows 2000," omawia jak wymuszać zasady grupy w klientach Windows XP działających w oparciu o domenę Windows 2000.

Rozdział 13, "Zdalna Pomoc / Konfiguracja Pulpitu," daje rekomendacje dla użycia I konfiguracji bezpieczeństwa dla Zdalnej Pomocy I Zdalnego Pulpitu w Windows XP.

Rozdział 14, "Konfiguracja wbudowanego Firewall dla połączenia z Internetem," omawia użycie tego narzędzia dla użytkownika Windows XP.

Rozdział 15, "Dodatkowe ustawienia bezpieczeństwa," opisuje inne rekomendacje bezpieczeństwa, takie jak użycie konta administratora czy prawa do udostępnionych zasobów.

Rozdział 16, "Modyfikacje dla Windows XP działającego w domenie Windows NT," opisuje kilka zalecanych ustawień bezpieczeństwa w Windows XP jako członka domeny Windows NT.

Ta strona celowo jest pusta

Co nowego w bezpieczeństwie Windows XP

Windows XP posiada zmodyfikowane ustawienia bezpieczeństwa Windows 2000, jak również zupełnie nowe cechy. Rozdział ten przedstawia pewne cechy, które są istotne z punktu widzenia Windows XP działającego w środowisku domeny. Cechy unikatowe dla pojedynczych komputerów z Windows XP nie zostały omówione w tym dokumencie

Zmiany cech bezpieczeństwa

Następujące cechy zostały zmodyfikowane w stosunku do Windows 2000.

Należność do grupy **Wszyscy**

W Windows NT i Windows 2000, wbudowana grupa **Wszyscy** obejmowała użytkowników anonymous (puste połączenie). Oznaczało to, że użytkownik ten miał dostęp do wszystkich zasobów co pozostali członkowie grupy **Wszyscy**. Standardowo w Windows XP grupa **Wszyscy** nie obejmuje tych użytkowników (anonymous).

Własność dla grupy **Administratorzy**

W Windows NT i Windows 2000 każdy obiekt stworzony przez członka grupy **Administratorzy** automatycznie został przypisywany do całej grupy, jako do właścicieli. W Windows XP członek grupy **Administratorzy** tworzący obiekt staje się jego jedynym właścicielem.

Instalacja drukarek

W Windows XP użytkownik musi należeć do grupy **Użytkowników Zaawansowanych** lub **Administratorów** by zainstalować drukarkę lokalną. Dodatkowo użytkownik musi posiadać prawa do ładowania / wyładowania sterowników urządzenia.



Informacja: Administratorzy standardowo posiadają prawo ładowania / wyładowywania sterowników urządzenia

Restrykcje związane z pustym hasłem

Lokalne konta użytkowników nie posiadające hasła mogą być jedynie używane do logowania na konsoli i pracy na stanowisku bez korzystania z zasobów sieci.



INFORMACJA: Restrykcje te nie dotyczą logowań użytkowników domeny, a także konta Gość. Jeśli konto Gość jest aktywne i posiada puste hasło, może zostać użyte do logowania do zagwarantowanych zasobów.

Convert.exe

W Windows NT i Windows 2000 użycie convert.exe do konwersji partycji typu FAT lub FAT32 na NTFS dawało pełne prawa grupie Wszyscy do konwertowanego wolumenu. W Windows XP convert.exe ustawia podczas konwersji domyślne prawa do wolumenu.

Podsystemy

Windows NT i Windows 2000 dostarcza wsparcie dla systemów OS/2 i POSIX subsystems. Jednakże, Windows XP nie zawiera podsystemów wspierających. Wsparcie dla POSIX stało się teraz częścią Microsoft Windows Interix 2.2. Więcej informacji znajduje się na <http://www.microsoft.com/windows2000/Interix>.

System Szyfrowania Plików

System Szyfrowania Plików pozwala użytkownikom na szyfrowanie plików, folderów i całych napędów z danymi. Windows XP posiada kilka nowych cech:

- Inni użytkownicy mogą być autoryzowani do dostępu zaszyfrowanych danych
- Pliki off-line mogą być szyfrowane
- Agenci odtwarzania danych są możliwi do utworzenia
- Potrójny DES (3DES) – algorytm kodowania – może zostać wykorzystany
- Hasło do kodowania dysku może zostać użyte jako hasło użytkownika
- Szyfrowane pliki mogą być przechowywane w folderach sieci web

Nowe cechy bezpieczeństwa

Sekcja ta opisuje pewne nowe cechy bezpieczeństwa Windows XP

Zasady restrykcyjne oprogramowania

Wzrastająca liczba “niewykrywalnych” programów przenoszonych poprzez Internet i pocztę elektroniczną w formie robaków i wirusów wykorzystuje fakt nieświadomości użytkowników przy kradzieży danych lub siania spustoszenia na zainstalowanych systemach. Windows XP dostarcza teraz mechanizmy dla administratorów do klasyfikacji aplikacji na zaufane i nie zaufane.

Przez zasady restrykcji oprogramowania, oprogramowanie może być chronione przed uruchamianiem bazując na następujących zasadach:

- Ścieżka – aplikacje dozwolone lub nie dozwolone na podstawie ścieżki pliku lub folderu. Zasada ścieżki może zawierać specjalne znaki. Na przykład, wszystkie skrypty Visual Basic’a mogą być dezaktywowane przez określenie ich jako *.vbs.

Hash – aplikacje mogą być dozwolone lub zabronione bazując na użyciu znaków Hash (#) w kontekście pliku. Opiera się on na pliku i jego unikatowości.. Jeśli jednak nastąpi zmiana aplikacji hash również ulegnie zmianie.

- **Certyfikat** – aplikacje mogą być dozwolone lub zabronione bazując na cyfrowym certyfikacie skojarzonym z aplikacją.
- **Strefa internetowa** – aplikacje mogą być dozwolone lub zabronione bazując na strefie internetowej z której zostały ściągnięte. Można określić następujące strefy: Internet, Intranet, Niedozwolone adresy, Zaufane strony, Mój komputer. Zasady te działają z plikami instalacyjnymi dla Windows
- **Egzekwowanie właściwości** – ustalenia czy pliki bibliotek oprogramowania (pliki zawierające główne zmienne I definicje funkcji) są zawarte w polityce restrykcyjnej oprogramowania. Także ta opcja może być użyta do ochrony restrykcji oprogramowania przed zmianami przez lokalnych administratorów.
- **Wyznaczenie typu plików** – pozwala na dodawanie lub usuwanie typów plików z listy tych, które mogą zawierać wykonywalny kod.
- **Zaufaniu publikatorzy** – określa którzy użytkownicy mogą wybierać zaufane aplikacje do publikacji.

Więcej informacji znajduje się w Księdze Wiedzy Microsoft'u w artykule numer Q310791 " Opis zasady restrykcji oprogramowania w Windows XP " na stronie <http://support.microsoft.com/default.asp?scid=kb:EN=US:q310791>.

Przechowywanie nazw użytkowników i haseł

Nazwy użytkowników I referencje potrzebne do dostępu do sieci lub zasobów Internetu przechowywane są w systemie. Do czasu późniejszego omówienia mechanizmów przechowywania nie istnieje potrzeba dalszego opisu w tym momencie.

Nowe konta usług

Dwa nowe konta usług, Usługa Sieciowe oraz Usługa Lokalna, zastąpiły konto Usługi Lokalnego Systemu, jako konta usług dla głównych usług systemu. Sekcja ta opisuje wszystkie trzy konta usług.

Konto LocalSystem

Konto LocalSystem jest zdefiniowanym kontem z kompletem przywilejów na lokalnym komputerze. Konto nie jest powiązane z żadnym regularnym kontem użytkownika i nie posiada referencji jak nazwa użytkownika czy hasło. Konto to może otwierać klucz rejestru HKLM\Security. Kiedy LocalSystem posiada dostęp do zasobów sieciowych, działa również jak konto domeny.

Przykładami takich usług, które są uruchamiane pod właścicielstwem konta LocalSystem są: WindowsUpdate Client, Clipbook, Com+, DHCP Client, Messenger Service, Task Scheduler, Server Service, Workstation Service, and Windows Installer.

Konto Network Service

Konto Network Service Account jest zdefiniowanym lokalnym kontem z ograniczonymi przywilejami na lokalnym komputerze. Posiada prawa dostępu do zasobów sieciowych jako komputer. Usługi, które uruchamiane są pod tym kontem reprezentują referencje komputera do zdalnych systemów. Konto to generalnie

posiada dostęp do zasobów, którym Access Control Lists (ACLs) pozwala na dostęp poprzez Usługi Sieciowe, grupę Wszyscy lub Użytkowników Zautentykowanych.

Przykładami takich usług, które uruchamiane są jako Network Service są: Distributed Transaction Coordinator, DNS Client, Performance Logs and Alerts, and RPC Locator.

Konto Usługa Lokalna

Konto Usługa Lokalna jest zdefiniowanym kontem posiadającym minimum przywilejów ma lokalnym komputerze i reprezentuje referencje typu anonymous przy aktywności sieciowej. Konto to generalnie posiada dostęp do zasobów, którym ACLs pozwala na dostęp przez Usługi Lokalne, grupę Wszyscy lub Użytkowników Zautentykowanych.

Przykładami takich usług, które uruchamiane są jako Usługa Lokalna są: Alerter, Remote Registry, Smart Card, SSDP, and WebClient.

Konfiguracji Bezpieczeństwa

Windows XP zawiera wsparcie dla Menedżera Konfiguracji Bezpieczeństwa - Security Configuration Manager (SCM). Narzędzia SCM ustawiają zezwolenia administratorom systemu na konsolidację wielu ustawień bezpieczeństwa systemu w jeden prosty plik konfiguracji (nazwany szablonem lub plikiem typu inf w tym przewodniku ze względu na rozszerzenie .inf). Możliwe jest warstwowanie pliku konfiguracji bezpieczeństwa do modyfikacji różnych aplikacji i ustawień bezpieczeństwa. Te ustawienia bezpieczeństwa mogą być wtedy adoptowane na wielu komputerach z Windows XP jako część Zasady Obiektów Grupy lub przez lokalne konfiguracje komputerów.

Kilka narzędzie, które umożliwiają konfigurację ustawień bezpieczeństwa w Windows XP:

- Zasady Lokalnego Bezpieczeństwa
- Rozszerzenia Ustawień Bezpieczeństwa dla Zasady Grupy
- Menedżer Konfiguracji Bezpieczeństwa, który zawiera:
 - Zakładki Szablonów Bezpieczeństwa
 - Zakładki Konfiguracji Bezpieczeństwa i Analiz
 - Secedit.exe – narzędzie wiersza poleceń

Te komponenty pozwalają na analizę i konfigurację obszarów bezpieczeństwa:

- **Zasady Dostępu** – zawiera Zasady Hasel, zasady blokowania kont, Zasady Kerberos
- **Zasady Lokalną** – zawiera Zasady Audytu, określenia praw użytkowników i opcji bezpieczeństwa
- **Dziennik Zdarzeń** – zawiera ustawienia dla Dziennika Zdarzeń
- **Grupy Restrykcji** – zawiera ustawienia członkostwa w grupach
- **Usługi Systemowe** – zawiera konfiguracje dla usług systemowych
- **Rejestr** - zawiera ustawienia praw dostępu klucza rejestru Discretionary Access Control List (DACL)
- **System Plików** – zawiera pliki ustawienia praw plików i folderów NTFS

Rozdziały 4 - 10 opisują rekomendowane ustawienia i sposoby optymalizacji szablonów, a rozdział 11 opisuje jak zachowywać konfiguracje i ustawienia bezpieczeństwa. Więcej informacji o Menedżerze Konfiguracji Bezpieczeństwa oraz Przewodnik Krok po Kroku jak używać narzędzi konfiguracji bezpieczeństwa znajduje się na stronie: www.microsoft.com/windows2000/techinfo/planning/security/secconfsteps.asp.

Funkcjonalność Konfiguracji Bezpieczeństwa

Menedżer narzędzi konfiguracji bezpieczeństwa wspomaga obie metody: używanie graficznego interfejsu użytkownika (GUI) oraz narzędzia wiersza poleceń..

Konfiguracja bezpieczeństwa przez Graficzny Interfejs Użytkownika GUI

Graficzny interfejs użytkownika jest dostarczony przez Konsolę Zarządzania Microsoft'u (MMC). MMC jest kontenerem na narzędzia administracyjne i jest używany rozlegle w Windows XP. Narzędzia są importowane do MMC poprzez „zakładki” („zatrzaski”) - "snap-ins.". Obecnie Menedżer Konfiguracji Bezpieczeństwa zawiera dwie zakładki do MMC: Szablony Bezpieczeństwa oraz Analiza i Konfiguracja Bezpieczeństwa. Obie zakładki będą omówione w detalach w tym i 11 rozdziale.

Menedżer konfiguracji bezpieczeństwa pozwala administratorom na:

- Kreowanie lub edycję szablonów konfiguracji bezpieczeństwa
- Optymalizację analizy bezpieczeństwa
- Graficzne przedstawienie wyników analizy
- Uaktywnianie konfiguracji bezpieczeństwa na systemie

Graficzny Interfejs Użytkownika dostarcza możliwość różnych kolorów, fontów, ikon, by podkreślać różnice pomiędzy podstawowymi informacjami i aktualnymi ustawieniami systemu. Kiedy analiza lub konfiguracja zostaje zmieniona – zoptymalizowana, wszystkie obszary bezpieczeństwa z szablonami bezpieczeństwa udostępnione są do analizy.

Narzędzia konfiguracji bezpieczeństwa wiersza poleceń

Narzędzie konfiguracji bezpieczeństwa wiersza poleceń (secedit. exe) umożliwia:

- Optymalizację analizy bezpieczeństwa
- Uaktywnianie konfiguracji bezpieczeństwa na systemie Windows XP

Opcje wiersza poleceń pozwalają na analizę poszczególnych obszarów bezpieczeństwa w porównaniu do konfiguracji całego pliku. Również wyniki analiz mogą być przekierowane do pliku w celu późniejszych porównań. Narzędzie wiersza poleceń jest także użyteczne przy innych dystrybucjach narzędzi zarządzania systemem

Szablony Bezpieczeństwa

Szablony bezpieczeństwa są plikami zawierającymi ustawienia konfiguracji bezpieczeństwa. Szablony dostarczają łatwego sposobu na standaryzację bezpieczeństwa na wszystkich komputerach w domenie. Mogą być uaktywniane na komputerach z Windows XP lub importowane do Obiektów Zasady Grupy lub być aplikowane bezpośrednio do komputera lokalnego poprzez Menedżera Konfiguracji Bezpieczeństwa.

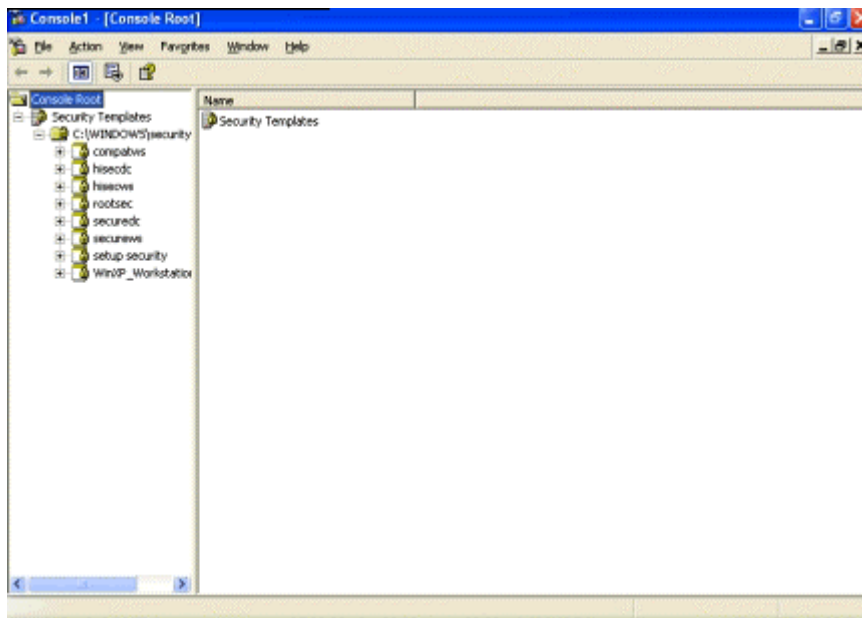
Sekcja ta dostarcza opisu zakładek i opisuje pliki konfiguracji bezpieczeństwa zawarte w narzędziach.

Ładowanie zakładek (Snap – in) szablonów bezpieczeństwa do MMC

Zakładki szablonów bezpieczeństwa muszą być załadowane do Konsoli Zarządzania Microsoft (MMC). MMC jest zainstalowana standardowo na komputerach z Windows XP. By załadować zakładki bezpieczeństwa należy:

- Uruchomić Konsolę Zarządzania MMC (mmc.exe)
- Wybrać Plik -> Dodaj / Usuń Zakładkę (Snap-in)
- Kliknąć DODAJ
- Wybrać szablony bezpieczeństwa
- Kliknąć Dodaj
- Kliknąć Zamknij
- Kliknąć OK

Rysunek 1 pokazuje załadowane zakładki szablonów bezpieczeństwa do MMC



Rysunek 1 Zakładki Szablonów Bezpieczeństwa

By uniknąć problemu ładowania za każdym razem do MMC zakładek należy zapisać aktualne ustawienia konsoli wykonując następujące czynności:

- w menu konsoli wybrać **Zapisz**. Standardowo zapis odbędzie się w menu narzędzi administracyjnych dla profilu aktualnie zalogowanego użytkownika.
- wprowadź nazwę pod którą mają być zapisane aktualne ustawienia konsoli I kliknij **Zapisz**

Od teraz konsola będzie dostępna z **Start -> Wszystkie Programy -> Narzędzia Administracyjne** tak długo jak profil użytkownika będzie skonfigurowany do wyświetlania tego menu w menu Start.

Przeglądanie tekstu szablonów bezpieczeństwa

Mimo, że jest to nie rekomendowane, szablony bezpieczeństwa mogą być podglądnięte poprzez edytor tekstowy, na przykład notepad.exe. Sekcja adresowania szablonu oraz kontroli dostępu do rejestru może wydawać się na początku zakodowana. Jest to zdefiniowany język zwany Security Descriptor Definition Language (SDDL). Artykuł opisujący owy język znajduje się w artykule Microsoft SDK dostępnym na stronie: http://msdn.microsoft.com/library/en-us/securitv/Securitv/security_descriptor_definition_language.asp.

Pliki konfiguracji bezpieczeństwa

Sekcja ta opisuje standardowe oraz dostarczone przez NSA szablony bezpieczeństwa dostępne w zakładkach szablonów bezpieczeństwa.

Standardowe Szablony Bezpieczeństwa

Istnieje szablon bezpieczeństwa, który zawiera standardowe ustawienia bezpieczeństwa, który jest uaktywniany na świeżo zainstalowanym systemie Windows XP. Jest on szczególnie użyteczny, gdy chcemy powrócić do oryginalnych ustawień systemu.

Szablon, który jest aktualnie aktywny jest przechowywany w: %SystemRoot%\security\templates 3S "setup security.inf."



Informacja: "Setup security.inf" nigdy nie powinien być uaktywniany poprzez Zasady Grupy z kontrolera domyślnego I powinien być uaktywniany tylko z lokalnego komputera poprzez Konfigurację Bezpieczeństwa I Analiz – secedit.exe. Spowodowane jest to faktem iż każdy setup szablonów bezpieczeństwa jest dopasowywany do konkretnego komputera. Także szablony zawierające dużą liczbę konfiguracji i mogą obniżyć wydajność połączeń sieciowych jeśli zostały by one uaktywnione z pozycji Zasady Grupy

Szablony dostarczane przez Microsoft

Wraz z zakładkami szablonów bezpieczeństwa Microsoft dostarcza kilka wzorów przeznaczonych dla różnych poziomów bezpieczeństwa. Pomiędzy nimi istnieją compatws.inf, securews.inf, oraz hisecws.inf. W związku z faktami iż rekomendowanymi szablony stały się te dostarczone przez NSA detale dotyczące szablonów dostarczonych przez Microsoft nie będą więcej opisywane.

Szablony Bezpieczeństwa NSA

Dokument ten dostarczany jest z plikiem konfiguracji bezpieczeństwa .inf, który zawiera rekomendowane ustawienia opisywane w przewodniku. Szablony bezpieczeństwa można również odnaleźć na stronie [http://nsa1 .www.conxion.com/](http://nsa1.www.conxion.com/).

Zanim dokonasz zmian bezpieczeństwa

Jeśli pojawią się problemy po wprowadzeniu nowych szablonów bezpieczeństwa rozwiązanie ich będzie trudne jeżeli została wprowadzona duża liczba zmian na raz. Pierwsze i najważniejsze to testowanie ustawień na środowisku testowym zanim zostaną one wprowadzone do sieci produkcyjnej. Należy starać się dokonywać zmian w jednej sekcji szablonów za jednym razem i w jednym czasie z wierszem poleceń i narzędziem secedit.exe (opisanym w rozdziale 11) lub przez izolowanie specyficznych ustawień sekcji do poszczególnych osobnych plików .inf. Metoda ta pozwala na uaktywnianie jednej części szablonów (na przykład tylko Zasady Kont lub Plików System) i wtedy testowania systemu na okoliczność występowania problemów by unikać ich przy przejściu do następnej grupy opcji

Najpewniejszym sposobem przywrócenia systemu do jego oryginalnej konfiguracji jest jego odtworzenie z kopii bezpieczeństwa (backup'u). Plik security.inf" (wspomniany wcześniej w tym rozdziale) może zostać użyty do zresetowania większości wartości ustawień. Jednakże wszelkie ustawienia, określone jako niezdefiniowane w standardowym szablonie nie będą zmienione dla konfiguracji pierwotnej i konfiguracji rekomendowanej przez NSA.

Lista kontrolna dla uaktywnienia rekomendacji z przewodnika

Sekcja ta dostarcza listę kontrolną kroków, które zoptymalizują szablony bezpieczeństwa zawartych w dokumencie.

- Przeglądnij I zrozum ostrzeżenia z rozdziału 1. Nie jest rekomendowane by szablony bezpieczeństwa dostarczone przez NSA były uaktywniane bez przeglądu I wykonania funkcji zawartych w rozdziałach 4-10.
- Wykonaj kopie bezpieczeństwa - backup twojego systemu. Jest to najpewniejszy sposób przywrócenia konfiguracji systemu.
- Ściągnij odpowiedni plik konfiguracji do folderu szablonów (%Systemroot%\security\Templates), lub dodać inną ścieżkę poszukiwania szablonów do miejsca, gdzie są one przechowywane
- Sugeruje się by dokonać kopii bezpieczeństwa plików szablonów pod innymi nazwami, jeśli planuje się ich modyfikację w stosunku do rekomendowanych ustawień. Można to wykonać poprzez funkcję Zapisz jako przed modyfikacją szablonu w MMC.
- Kilka nowych opcji bezpieczeństwa zostało dodanych do szablonów bezpieczeństwa NSA. By uaktywnić te opcje należy ściągnąć plik sceregvi.inf ze strony NSA do folderu %systemRoot%\inf. Należy przemianować owy plik na inny, by mieć możliwość powrotu do pierwotnych ustawień w nim zapisanych.
- By zarejestrować nowe opcje bezpieczeństwa z wiersza poleceń należy uruchomić regsvr32 scecli.dll, po umieszczeniu pliku sceregvi.inf w folderze %SystemRoot%\inf. Koniec rozdziału 5 omawia jak inne opcje bezpieczeństwa mogą być dodane do szablonów bezpieczeństwa.
- Przeglądnij rekomendowane ustawienia z rozdziałów 4 - 10. Poprzez zakładki MMC szablonów bezpieczeństwa, modyfikuj pliki szablonów bezpieczeństwa optymalizując do potrzeb Twojej sieci. Należy zwrócić szczególną uwagę na notatki, uwagi powiązane z poszczególnymi ustawieniami. By zmodyfikować szablon należy:
 - W MMC, kliknąć dwukrotnie na szablon bezpieczeństwa w lewym panelu
 - Kliknij dwukrotnie na standardowym folderze plików (%Systemroot%\Security\Templates). Lista dostępnych plików zostanie przedstawiona.



Informacja: Pliki szablonów z innych folderów mogą zostać wczytane przez kliknięciem prawym klawiszem myszy na szablonie bezpieczeństwa I wybranie opcji szukania ścieżki nowych szablonów.

- Podwójne kliknięcie na określonym pliku konfiguracji
- Podwójne kliknięcie na określonym obszarze bezpieczeństwa
- Podwójne kliknięcie na obiekcie bezpieczeństwa w prawym panelu
- Ustawienie opcji zgodnie z specyficznym środowiskiem
- by zapisać zmieniony plik konfiguracji pod nową nazwą pliku (by uchronić przed nadgraniem na dostarczony szablon) prawym klawiszem myszy kliknąć na plik w lewym panelu I wybrać Zapisz jako, określić nazwę dla zmodyfikowanego szablonu

Kilka ustawień bezpieczeństwa jest rekomendowanych, ale nie zdefiniowanych w szablonach, ponieważ są one specyficzne dla konfiguracji środowiska. Należy zdecydować o wartościach dla konfiguracji. Wśród tych ustawień znajdują się te opisane w rozdziale 5:

- Konta: Zmiana nazwy konta Administratora

- Konta: Zmiana nazwy konta Gość
- Logowanie interaktywne: Wiadomość tekstowa dla użytkowników próbujących się zalogować
- Logowanie interaktywne: Tytuł wiadomości dla użytkowników próbujących się zalogować

Raz zmienione szablony pod kątem optymalizacji dla danego środowiska należy zapisać, by uaktywnić szablony. Jeśli szablony zostaną uaktywnione lokalnie, zobacz rozdział 11 by uzyskać informacje o opcjach konfiguracji poprzez zakładkę Konfiguracji Bezpieczeństwa i Analizę lub narzędzie wiersza poleceń `secedit .exe`. Jeśli szablon zostanie zaimportowany do Obiektów Zasady Grupy, należy przejść do rozdziału 12.

Optymalizacja dodatkowych konfiguracji bezpieczeństwa opisują rozdział 13-16

Ta strona celowo jest pusta

Modyfikacja Ustawień Zasady Kont przy Użyciu Szablonów

Kluczowy komponent kontroli ochrony w systemie to właściwe ustawienia zasady kont. Zależnie od typu systemu (np. kontroler domeny, stacja robocza, serwer członkowski), konfiguracja zasady kont będzie miała różny wpływ na sieć. W domenach Windows 2000, zasady kont jest ustawiana i wymuszana przez zasady grup domen. Próby konfiguracji zasady grup domen w innych GPO są ignorowane. Konfigurowanie zasady kont bezpośrednio na stacjach roboczych i zasady blokowania kont na komputerze.

Do zapewnienia zgodności hasła i zasady blokad, przez cały czas zasady zarówno dla lokalnych jak i domenowych logowań powinna być taka sama, jak ta ustawiona na kontrolerach domen (przez GPO domeny), i przez Zasady Bezpieczeństwa Lokalnego na serwerach członkowskich, a także stacjach roboczych XP. Aby uzyskać więcej informacji na temat ważnych szablonów zabezpieczeń, należy sięgnąć do właściwych rozdziałów *Guide to Securing Microsoft Windows 2000 Group Policy*.

Żeby zobaczyć ustawienia zasady kont szablonu zabezpieczeń, kliknąć w MMC:

- **Szablony Zabezpieczeń**
- Katalog standardowego pliku konfiguracji
- (%SystemRoot%\Security\Templates)
- Określ plik konfiguracji a **Zasady kont**
-



Informacja: Po jakichkolwiek modyfikacjach w konfiguracji, upewnij się, że zapisałeś zmiany i sprawdź je przed zainstalowaniem ich na środowisku produkcyjnym.

Zasady haseł

Przed wprowadzeniem zmian w oknie dialogowym Zasady Kont sprawdź zasady bezpieczeństwa zapisywania haseł w swojej organizacji. Zmiany poczynione w oknie dialogowym Zasady Kont powinny być zgodne z zapisanym hasłem zasady. Użytkownicy powinni przeczytać i potwierdzić znajomość zasady organizacyjnej.

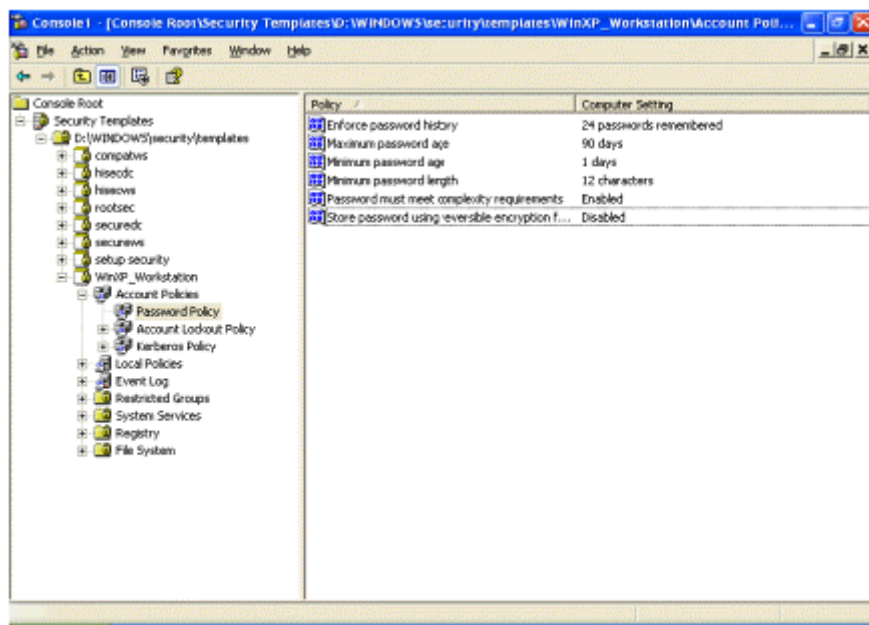
- Zalecenia zasady haseł zawierają:
- Użytkownicy nigdy nie powinni zapisywać haseł

- Hasła powinny być trudne do odgadnięcia włączając małe, duże znaki (np. znaki interpunkcyjne i rozszerzenia), i znaki numeryczne. Nie powinno się używać słów ze słownika.
- Użytkownicy nie powinni przysyłać haseł w formie otwartego tekstu.

Aby zmienić ustawienia zasady haseł przez zakładkę Szablonów Zabezpieczeń kliknij :

Zasady Kont -Zasady haseł -określona opcja do sprawdzenia albo zmiany odpowiednich ustawień

Tabela 1 zalecane ustawienia zasady haseł i 2 jak zasady haseł jest widziana w MMC



Rysunek 2 Zalecenia Zasady Haseł

Opcje Zasady Haseł	Zalecane Ustawienia
<p><u>Wprowadzanie historii haseł</u> Zabezpieczenia przed możliwością wprowadzania przez użytkowników ich ulubionych haseł i zmniejszanie szans na to, że hacker haseł odkryje hasło. Jeśli ta opcja ustawiona jest na 0, użytkownicy nie mogą wrócić powrotem do hasła, którego używali poprzednio. Jest możliwość zmiany zakresu od 0 (brak historii haseł) do 24 zapamiętywanych haseł</p>	24 hasła
<p><u>Maksymalny wiek hasła</u> Okres czasu w którym użytkownikowi wolno mieć dane hasło do czasu jego wymaganej zmiany. Możliwe wartości łącznie z zerem (hasło nigdy nie traci ważności) do 1-999 dni. Maksymalny wiek hasła powinien być ustawiony na mniej niż 90 dni w bardziej zabezpieczonych środowiskach</p>	90 dniowe
<p><u>Minimalny wiek hasła</u> Minimalne ustawienia wieku hasła określają jak długo trzeba czekać po zmianie hasła przed jego kolejną zmianą. Standardowo użytkownicy mogą zmieniać hasła w dowolnym czasie. Zatem użytkownik mógłby zmienić hasło i potem znów je zmienić, na takie jak było wcześniej. Możliwe wartości to 0 (hasło może być zmienione natychmiast) lub w czasie 1-988 dni</p>	1 dzień
<p><u>Minimalna długość hasła</u> Uwaga: Aktualnie, Windows 2000 i XP wspierają hasła do 127 znaków. Hasło dłuższe niż 14 znaków ma wyraźną przewagę w sytuacjach środowisk sieciowych, gdyż hasło nie może być już łamane za pomocą tradycyjnego oprogramowania do tego celu. Niestety interfejs szablonów bezpieczeństwa nie pozwala na ustawienie wymagania hasła dłuższego niż 14 znaków. Również, jeśli w sieci znajdują się komputery z Windows 95 lub NT, maksymalna długość hasła nie może przekraczać 14 znaków, gdyż owe systemy nie wspierają haseł dłuższych niż 14 znaków przy procedurach logowania do ich interfejsów. Informacja: Rekomenduje się, by uprzywilejowani użytkownicy (tacy jak Administratorzy) posiadali hasła dłuższe niż 12 znaków. Wzmocnieniem trudności hasła dla kont administratorów może być użycie znaków, które nie są domyślnymi (litery i cyfry). Na przykład można użyć znaków Unicode pomiędzy 0128 a 0159. Użycie ich daje dwie korzyści: (1) w sieciach ich rozpoznawalność maleje (2) nie znajdują się na liście znaków przetwarzanych przez programy łamiące hasła. Należy uważać przy stosowaniu znaków Unicode. Wprowadzanie znaków Unicode dokonuje się poprzez naciśnięcie klawisza ALT + numer znaku. W przypadku korzystania z Notebook'ów należy również posłużyć się klawiszem FN.</p>	12 znaków

Opcje Zasady Hasel	Rekomendowane ustawienia
<p><u>Hasło musi spełniać wszystkie kryteria</u></p> <p>Wygazekwowanie mocnego hasła dla wszystkich użytkowników. Mocne hasła dostarczają pewnych aspektów obrony przez zgadywaniem hasel i sprawdzaniem ich metoda słownikową przez zewnętrznych intruzów. Hasło musi zawierać 3 z 4 warunków: małe litery, duże litery, cyfy, znaki specjalne (na przykład znaki punktowe). Również hasła nie mogą być takie same jak nazwy użytkowników. Wymagalność tych parametrów będzie wymuszona na użytkownika podczas jego następnego. Istniejące hasła nie podlegają tym założeniom.</p> <p><i>Informacja:</i> NSA dostarcza rozszerzony filter sprawdzania wymogów hasła, ENPASFLT.DLL, który powinien zostać podmieniony (taki sam używany jest w agencjach rządowych)</p> <p>Filtr ten wymusza hasła dłuższe niż 8 znaków zawierające 4 typy znaków. Również użycie pełnego nazwiska lub imienia użytkownika nie jest dozwolone. Więcej informacji o ENPASFLT znajduje się w dokumentacji łącznie z procedurą instalacji i wyłączenia filtra..</p> <p><i>Informacja:</i> By dowiedzieć się jak tworzyć własne filtry sprawdzające hasła należy zapoznać się z: Microsoft Knowledge Base article _Q151082 "HOWTO: Password hange Filtering and Notification in Windows NT" nas stronie: http://suDDort.microsoft.com/default.asD?scid=kb:EN=US:a151082.</p>	Włączone
<p>Przechowywanie hasła przy użyciu odwracalnego kodowania dla wszystkich użytkowników domeny</p> <p>Opcja ta umożliwia poznanie hasła (jego przepływ) bezpośrednio przez główne aplikacje..</p>	Wyłączone

Tabela 1 Opcje Zasady Hasel

Zasady blokowania kont

Blokowanie kont powinno odbywać się po trzech próbach logowania zakończonych nie powodzeniem. Ustawienie to utrudnia i zwalnia ataki „słownikowe”, w których testowane są tysiące powszechnie używanych hasel. Jeśli nastąpi taka blokada haker musi czekać, aż do ponownego uaktywnienia konta. Jeśli konto takie zostało zablokowane administrator może je uaktywnić lub zresetować używając Active **Directory Users and Computers** dla kont odmeny lub **Zarządzanie komputerem** lokalnych kont w celu przerwania czasu ustalonego na automatyczne odblokowanie konta.



Informacja: Wbudowane konto administratora może być zablokowane zgodnie z Zasadami Blokowania Kont Istnieje możliwość zablokowania zdalnego logowania na konto administratorów, lecz lokalna możliwość logowania administratora pozostaje nadal

By zmodyfikować ustawienia zasady blokowania kont w zakładce szablonów bezpieczeństwa należy dwukrotnie kliknąć według następującej ścieżki::

Zasady kont -> Zasady Blokowania Konta -> określić ustawienia do podglądu lub zmiany

Tabela 2 Lista rekomendowanych ustawień zasady blokowania kont.

Opcja Zasady Blokowania Kont	Rekomendowane ustawienia
<p><u>Okres blokowania konta</u> Ustaw liczbę minut dla ilu konto będzie zablokowane. Akceptowane wartości są od 0 (opcja ta blokuje konto na stałe – aż do odblokowania przez administratora) lub pomiędzy 1 a 99999 minut. OSTRZEŻENIE: Ustawienie tej wartości na 0 (aż do momentu odblokowania przez administratora) może być początkiem ataków denial of service.. Istotne jest, że konto wbudowane Administrator nie może zostać zablokowane na stałe na lokalnym komputerze</p>	15 minut
<p><u>Próg blokowania kont</u> Ochrona system przed brutalnymi metodami “słownikowymi” łamania haseł dla lokalnych kont. Opcja ta określa liczbę nieudanych prób logowania po których nastąpi zablokowanie konta. Dozwolonymi wartościami: od 0 (konto nie zostanie zablokowane) do 999 prób Chociaż 3 nieudane próby to wartość rekomendowana, to ustawienie pomiędzy 3 – 5 daje właściwy poziom ochrony Informacja: Nieudane próby logowania na maszynie, której konsola została zablokowana przez CTRL-ALT-DEL lub wygaszacz ekranu z chroniącym hasłem nie zaliczają się do nieudanych prób logowania</p>	3 nieudane próby logowania
<p><u>Resetuj liczbę nieudanych prób logowania</u> Ustawienie liczby minut, po których licznik nieudanych prób zalogowania będzie automatycznie wyzerowany. Dostępne wartości: od 1 do 99999 minut</p>	15 minut

Tabela 2 Opcje Blokowania Kont

Zasady Kerberos

Kerberos jest domyślną metodą autentykacji używaną w Windows 2000 i Active Directory. Od kiedy Active Directory jest konieczne dla autentykacji metodą Kerberos, zasady Kerberos ma tylko znaczenie w GPO (Group Policy Object) domen Windows 2000. Dlatego też, w dokumencie kierowanym do stanowiskowych instalacji Windows XP będą umieszczone tylko informacje ogólne.

By zmodyfikować ustawienia Kerberos poprzez zakładkę Szablonów Bezpieczeństwa należy kliknąć dwukrotnie zgodnie z następującą ścieżką:

Zasady Kont -> Zasady Kerberos ->określić opcje do podglądu lub edycji

Tabela 3 Lista opcji Zasady Kerberos, które powinny być uaktywnione na poziomie **domain group policy Zasady Grupy w Domenie**

Opcje Zasady Kerberos	Rekomendowane ustawienia
<p><u>Egzekwowanie restrykcji logowania użytkowników</u> Wymuszanie Klucza Centrum Dystrybucji - Key Distribution Center (KDC) to sprawdzenia czy użytkownik posiada bilet do zalogowania się tylko na lokalnej maszynie czy posiada możliwość dostępu do systemu poprzez sieć. Jeśli użytkownik nie posiada odpowiednich praw usługa klucza nie zostanie wydana. Uruchomienie takiej zasady podnosi poziom bezpieczeństwa, może jednak zwolnić dostęp do serwerów poprzez sieć.</p>	Włączone
<p><u>Maksymalna długość życia dla usługi biletu</u> Określanie liczby minut dla usługi biletu Kerberos. Wartość musi być pomiędzy 10 minut a maksymalną czyli 600 minut (domyślne ustawienie GPO). Informacja: Wygaśnięta usługa klucza, jest tylko odnawiana podczas łączenia do serwera. Jeśli nastąpi to podczas trwania połączenia, sesja ta jest podtrzymywana.</p>	600 minut
<p><u>Maksymalny czas na używanie klucza</u> Określa liczbę godzin w których Kerberos ticket-granting ticket (TGT) jest dostępny. Po wygaśnięciu trzeba uzyskać nowy lub odnowić stary. 10 godzin jest wartością domyślną dla GPO domeny.</p>	10 godzin
<p>Maksymalny czas na odnowienie TGT dla użytkownika Określa maksymalną liczbę dni, w których TGT użytkownika może zostać odnowione.</p>	7 dni
<p>Maksymalna rozbieżność w synchronizacji stanowiska i serwera Określa maksymalną liczbę minut różnicy pomiędzy KDC a komputerem klienta Kerberos posiada pewność, udzielania autentykacji i chroni system przed możliwymi powtarzanymi atakami. Ważne jest więc by różnice w czasie były minimalne – maksymalnie GPO domeny.</p>	5 minut

Tabela 3 Opcje Zasady Kerberos

Modyfikacja ustawień Zasady Lokalnej przy użyciu Szablonów Bezpieczeństwa

Sekcja Zasady Lokalnej w Szablonach Bezpieczeństwa określa atrybuty bezpieczeństwa dla Zasady Audytu, wyznaczenia praw użytkowników oraz opcji bezpieczeństwa dla centralnej lokalizacji i łatwości administrowania bezpieczeństwem. By zobaczyć Ustawienia Zasady Lokalnej w zakładkach Szablonów Bezpieczeństwa należy dwukrotnie kliknąć według schematu w MMC:

- Szablony Bezpieczeństwa
- Domyślna lokalizacja folderu (%SystemRoot%\Security\Templates)
- Określić plik konfiguracji
- Zasady Lokalna



Informacja: Zanim wykonasz jakiegokolwiek zmiany upewnij się, że zostały zapisane poprzednie ustawienia i dokonano testów na środowisku nie produkcyjnym

Zasady Audytu

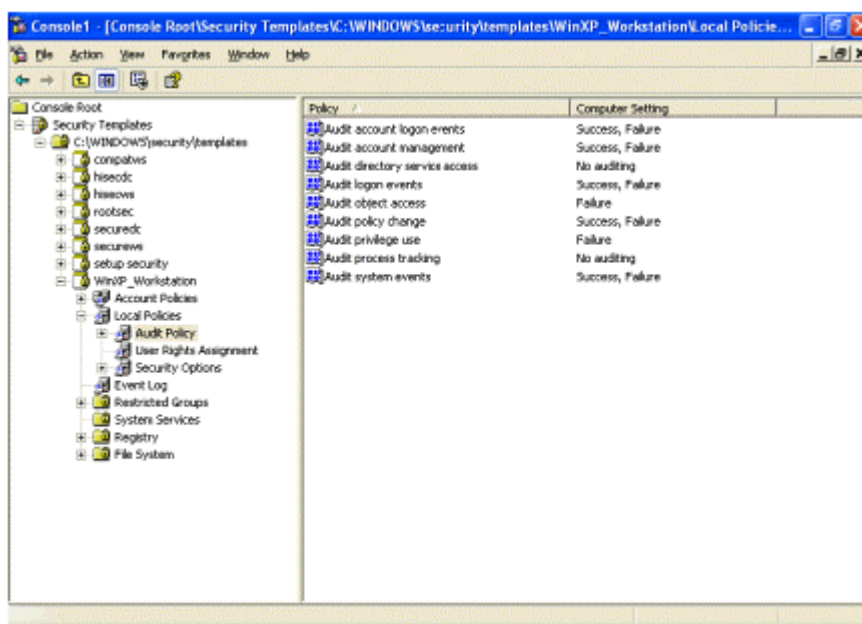
Audyt jest niezwykle istotny dla zarządzania bezpieczeństwem w domenie. W Windows XP audyt nie jest włączony jako domyślny. Każdy system Windows XP zawiera cechy audytu potrzebne do zgromadzenia informacji na temat indywidualnego użycia systemu. Logi zawierają informacje o zdarzeniach aplikacji, systemu i bezpieczeństwa. Każde zdarzenie, które jest poddane audytu według zasady audytu jest rejestrowane w logach, które mogą być podglądane w dzienniku zdarzeń.

OSTRZEŻENIE: Audyt może zabrać dużą liczbę czasu procesora oraz miejsca na dysku. Rekomenduje się, by administratorzy sprawdzali, zapisywali i czyścili logi audytu w systemie dziennym lub tygodniowym, by zredukować szansę degradacji systemu lub zapisywać logi na osobny komputer. Rekomenduje się również by pliki logów były przechowywane na osobnej partycji

By zmodyfikować ustawienia zasady audytu poprzez zakładki szablonów bezpieczeństwa należy dwukrotnie kliknąć według schematu:

- **Zasady Lokalna -> Zasady Audytu**
- Prawym klawiszem kliknąć na określonej opcji by wybrać ją do podglądu lub edycji

Rysunek 3 i Tabela 4 pokazuje rekomendowane ustawienia Zasady Audytu dla Windows XP Professional. Rekomendowane ustawienia dla serwerów członkowskich oraz kontrolerów domeny Windows 2000 zostały omówione w: *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*.



Rysunek 3 Rekomendowana Zasady Audytu

Opcje Zasady Audytu	Rekomendowane ustawienia
<p><u>Audyt zdarzeń logowania konta</u> Śledzenie zdarzeń logowania i wylogowywania na innych komputerach do których lokalny komputer został wykorzystany do autentykacji konta</p>	Sukces, Porażka
<p><u>Audyt zarządzania kontem</u> Śledzi zmiany w bazie bezpieczeństwa kont (na przykład kiedy konto zostało stworzone, zmienione lub skasowane).</p>	Sukces, Porażka
<p><u>Audyt dostępu usług katalogowych</u> Audytuje dostęp użytkowników do obiektów Active Directory które zostały zdefiniowane przez Systemową Listę Kontrolną (SACL) . Opcja ta jest podobna do Audytu Dostępu Obiektów tyle tylko, że dotyczy obiektów Active Directory objects. Od momentu aktywacji tej funkcji system staje się serwerem członkowskim domeny.</p>	Bez audytu
<p><u>Audyt zdarzeń logowania</u> Śledzi użytkowników , którzy się logowali lub wylogowywali lub korzystali z połączeń. Rejestrowane są także żądania (interaktywne, sieciowe, usług). Opcja ta różni się od "Audytu zdarzeń logowania konta" w sposobie interpretacji logowania, w celu ochrony przed niepowołanym logowaniem do systemu. Informacja: Audyt zdarzeń logowania z sukcesem lub z porażką generuje log o dużym rozmiarze. Wszystkie logowania są zapisywane. Audyt pozytywnych logowań ma znaczenie przy śledzeniu potencjalnych włamywaczy. Jeśli jednak rozmiar pliku ma być optymalny należy zapisywać jedynie niepowodzenia.</p>	Sukces, Porażka
<p><u>Audyt dostępu do obiektów</u> Śledzi niepowodzenia w dostępie do określonych obiektów (na przykład katalogi, pliki, drukarki) . Indywidualny.</p>	Porażka
<p><u>Audyt zmian zasady</u> Śledzi zmiany w polityce bezpieczeństwa, takie jak przyznawanie przywilejów lub zmiany zasady audytu. Informacje: Istnieje problem z udytem pomyślnie wykonanych zmian zasady audytu. Pierwszy problem dotyczy restartu i "wykonania nagłego restartu" (CrashOnAuditFail) opcja bezpieczeństwa aktywna. System może nawet doprowadzić się do zawieszenia i "blue – screen'a" Drugi problem to restart komputera z sukcesem, ale zapis tylko w logach administratora. Administrator musi wtedy zmienić wartość w rejestrze CrashOnAuditFail z 2 na 0 lub 1. Sytuacja ta nie występuje jeśli logowanie to jest wyłączone.</p>	Success, Failure
<p><u>Audyt uprzywilejowanego użycia</u> Śledzi porażki w użyciu przywilejów użytkowników. Śledzi wszystkie prawa użytkowników prócz pewnych przypadkach takich jak programy debugujące, Tworzenie Obiektów typu Token, generowanie audytu bezpieczeństwa. Tworzenie backupu lub przywracanie ustawień opcji bezpieczeństwa prowadzi do audytu praw użytkownika z wyłączeniem tego. Jednakże informacja zostanie uzupełniona w dzienniku zdarzeń tak szybko jak to jest możliwe.</p>	Sukces

<p><u>Audyt śledzenia procesów</u> Śledzenie z detalami informacji o zdarzeniach takich jak aktywacja programów i ich zakończenie. Ta opcja jest przydatna do zapisu specyficznych wydarzeń w systemie, które mogą wyglądać na atak.</p>	Bez Audytu
<p><u>Audyt zdarzeń systemu</u> Śledzenie zdarzeń, które nastąpiły po wejściu do systemu lub logu audytu. Zapisywane są takie zdarzenia jak zamykanie systemu, restart.</p>	Sukces, Porażka

Tabela 4 Opcje Zasady Audytu

Zadania Praw Użytkowników

Zadania praw użytkowników określają, jakie działania grupy lub użytkowników są dozwolone do wykonania. Wyraźnie zagwarantowane prawa użytkowników są uzupełniane przez udział w prawach użytkownika lub grupy. Rekomendowane prawa użytkownika są pokazane i opisane w tabeli 5. Zaawansowane prawa użytkownika są przypisane do Administratorów I zaufanych grup, które mają możliwość uruchamiania narzędzi administracyjnych, instalacji paczek serwisowych, tworzenia drukarek i instalacji sterowników urządzeń. Administratorzy nie są opisani w Tabeli 5 dla praw użytkowników, którzy mieliby wpływ na domyślną grupę ustawień dla użytkowników. Na przykład Operatorzy kopii zapasowej (Backup Operators) i administratorzy mają prawa wykonywania kopii (backup'u) plików i folderów, jednak zaleca się, by jedynie administratorzy mieli takie prawa



Informacja: Bazując na polityce sieci, pewne grupy użytkowników być może będą musiały być dodane lub usunięte z rekomendowanych praw użytkowników

By zmodyfikować ustawienia praw użytkowników poprzez zakładki Szablonów Bezpieczeństwa, podwójnym kliknięciem należy:

- **Zasady Lokalna -> Prawa użytkowników**
- Podwójne kliknięcie na edytowanych atrybutach w prawej ramce.
- By dodać użytkownika bądź grupę należy wybrać, **Dodaj użytkownika lub grupę** -> wprowadź nazwę -> Dodaj -> OK -> OK
- By usunąć użytkownika lub grupę wybierz użytkownika lub grupę i -> **Usuń** -> **OK**.

Prawa Użytkowników	Rekomendowane ustawienia
<u>Dostęp do komputera poprzez sieć</u> Pozwala użytkownikom na dostęp do tego komputera poprzez sieć	Administratorzy
<u>Działa jak część systemu operacyjnego</u> Pozwala na optymalizację bezpieczeństwa, dostęp do zaufanych części jest zagwarantowany	(Nikt)
<u>Dodawania stacji roboczej do domeny</u> Pozwala użytkownikowi na dodanie stacji roboczej do właściwej domeny. To prawo ma jedynie znaczenie dla kontrolerów domeny. Administratorzy lub Operatorzy Kont mają możliwość dodawania stacji roboczych do domeny i nie mają wyraźnego prawa na to	(Nikt)
<u>Przypisywanie ograniczeń pamięci na proces</u> Określa, które kono może użyć procesu z właściwościami dostępu zapisu do innych procesów w celu zwiększenia priorytetu dla tego procesu.	Administratorzy Usługi Sieciowe Usługi Lokalne
<u>Pozwala na logowanie poprzez usługi terminalowe</u> Określa, którzy użytkownicy lub grupy mają prawo do logowania się poprzez klienta usług terminalowych. Te prawa konieczne są dla użytkowników zdalnych pulpitów. Jeśli zdalny asystent jest używany, jedynie administratorzy używający nowych cech powinni mieć prawa do nich dostępu .	(Nikt)
<u>Tworzenie kopii bezpieczeństwa plików i folderów</u> Pozwala użytkownikom na tworzenie kopii bezpieczeństwa plików i folderów. To prawo musi być logicznie powiązane z prawami do danych plików i folderów Informacja: Jeśli w sieci znajdują się Operatorzy Kopii Zapasowych, prawo należy również dodać do grupy. Należy pamiętać by użytkownicy Ci mieli prawa dostępu do ACL. W przeciwnym razie Audyt Przywilejów ukatyni wpisywanie błędu.	Administratorzy
<u>Omijanie przemierzania sprawdzania</u> Pozwala użytkownikom na zmianę katalogu i dostęp do plików i podkatalogów, nawet jeśli nie mają oni praw do katalogu nadrzędnego.	Użytkownicy
<u>Zmiana czasu systemu</u> Pozwala użytkownikom na zmianę czasu w międzynarodowym zegarze.	Administratorzy
<u>Tworzenie pliku stronicowania</u> Pozwala użytkownikom na tworzenie pliku stronicowania dla wirtualnej pamięci oraz zmianę jego rozmiaru.	Administratorzy
<u>Tworzenie obiektu tokena</u> Pozwala na proces tworzenia tokenu, którym spowodować dostęp do lokalnych zasobów. Jedyne Lokalny Autorytet Bezpieczeństwa powinien mieć możliwość kreowania tego obiektu.	(Nikt)
<u>Tworzenie trwale udostępnionych obiektów</u> Pozwala użytkownikom na tworzenie specjalnych trwałych obiektów, takich jak \\Device, które są używa przez menedżera obiektów Windows XP.	(Nikt)
<u>Programy debugujące</u> Pozwalają użytkownikom na debugowanie zmiennych na niskim poziomie obiektu, takim jak wątki Informacja: Deweloperzy oprogramowania pracujący na systemie mogą potrzebować praw do uruchamiania programów debugujących. Należy je przydzielać tylko wtedy kiedy jest to konieczne.	(Nikt)

Prawa użytkowników	Rekomendowane ustawienia
<p><u>Odmów dostępu do tego komputera z sieci</u> Chroni określonych użytkowników lub grupy przed dostępem do zasobów z sieci. Ustawienia te wzmacniają „Dostęp do komputera poprzez sieć”, jeśli konta posiada współbieżne zasady</p>	(Nie zdefiniowane)
<p><u>Zabrania logowania jako praca wsadowa</u> Chroni specyficznych użytkowników lub grupy przed logowaniem wywołanym jako praca wsadowa. Ustawienie to wzmacnia „Logowanie jako praca wsadowa”, jeśli ich zasady są zgodne.</p>	(Nikt)
<p><u>Zabrania logowania jako usługa</u> Chroni specyficzne konta usług przez rejestracją procesu jako usługi. To ustawienie wzmacnia „Logowanie jako usługa” pod warunkiem, że zasady są zgodne.</p>	(Nikt)
<p><u>Zabran lokalnego logowania</u> Chroni określoną grupę użytkowników lub grup przed logowaniem prosto do komputera. Ustawienie to wzmacnia „logowania lokalnego” pod warunkiem, że są zgodne.</p>	(Nie zdefiniowane)
<p><u>Zabron logowania poprzez usługi terminalowe</u> Określa, którzy użytkownicy i grupy mają zabronione logowanie do systemu poprzez klientów usług terminalowych. Te ustawienia dotyczą szczególnie użytkowników zdalnych pulpitów Informacja: Jeśli usługi terminalowe funkcjonują na tym systemie należy wszystkich usunąć z tej grupy</p>	Wszyscy
<p>Włącza komputery użytkowników by byli zaufani do delegowania Pozwala użytkownikom ustawić opcje “Zaufane do delegacji” na użytkownikowi lub na obiekcie komputerów.. Użytkownik taki musi mieć zapewnione prawa do dostępu do flagi kontroli kont na komputerze lub obiekcie komputera.</p>	(No one)
<p><u>Wymuszaj zamknięcie systemu ze zdalnego połączenia</u> Pozwala użytkownikom na zamknięcie systemu Windows XP ze zdalnej lokalizacji w sieci..</p>	Administratorzy
<p><u>Generowanie audytów bezpieczeństwa</u> Pozwala na process generowania pliku bezpieczeństwa audytu.</p>	Usługa Lokalna Usługa Sieciowa
<p><u>Zwiększenie priorytetu zaplanowanych działań</u> Pozwala użytkownikom na przyspieszanie wykonywania priorytetów procesów. Może zostać to dokonane w Menedżerze Zadań.</p>	Administratorzy
<p><u>Ladowanie i odładowywanie sterowników urządzeń</u> Pozwala użytkownikom na instalowanie i odinstalowywanie sterowników urządzeń. Jest to niezbędne dla instalacji urządzeń Plug and Play</p>	Administratorzy
<p><u>Blokowanie stron pamięci</u> Pozwala użytkownikom na blokowanie stron pamięci, które nie mogą być przenoszone do wirtualnej pamięci na dysku.</p>	(Nikt)
<p><u>Logowanie jako praca wsadowa</u> Pozwala użytkownikom na logowanie jako zestaw parametrów działania wsadowego. W Windows XP menedżer Zaplanowanych Działań gwarantuje takie prawa.</p>	(Nikt)

Prawa użytkowników	Rekomendowane ustawienia
<p><u>Logowanie jako usługa</u> Pozwala na proces, który będzie zarejestrowany w systemie jako usługa</p> <p>Informacja: Pewne aplikacje, takie jak Microsoft Exchange wymagają użycia kont usługi, które powinny mieć takie prawo. Należy przeglądać użytkowników i grupy oraz nadać priorytety umożliwiające takie prawa tylko jeśli to konieczne.</p> <p>OSTRZEŻENIE: Dostarczane pliki tymczasowe zostaną usunięte (z wyjątkiem usług sieciowych) z praw, chyba, że zostanie to zmodyfikowane</p>	Usługa sieciowa
<p><u>Logowanie lokalne</u> Pozwala na logowanie użytkowników do konsoli systemu.</p> <p>Informacja: Jeśli w sieci istnieją Operatorzy Kopii Bezpieczeństwa należy ich również dodać do tej grupy.</p>	Administratorzy Użytkownicy
<p><u>Zarządzanie logiem audytu i bezpieczeństwa</u> Pozwala użytkownikom na oglądanie i czyszczenie pliku logu bezpieczeństwa i określenie typów dostęp do obiektów (jak pliki, klucze rejestru), które mają podlegać audytowi. Użytkownicy z prawami mogą włączyć audyt dla określonych obiektów przez edycję opcji audytu w zakładce bezpieczeństwa lub oknie dialogowym właściwości obiektu. Członkowie grupy administratorów zawsze mają możliwość tych praw.</p>	Administratorzy
<p><u>Modyfikacja zmiennych środowiskowych</u> Pozwala użytkownikom na modyfikacje zmiennych środowiska systemowego przechowywanych nie w RAM, co wspiera typ konfiguracji.</p>	Administratorzy
<p><u>Optymalizacja zadań zarządzania wolumenem</u> Pozwala użytkownikom na uruchamianie zadań zarządzania wolumenem, takich jak oczyszczanie dysku czy defragmentacja.</p>	Administratorzy
<p><u>Profil pojedynczego procesu</u> Pozwala użytkownikom na optymalizację profili (optymalizacje próbek) na procesie.</p> <p>Informacja: Deweloperzy oprogramowania pracujący na systemie mogą potrzebować takich praw, należy im je przydzielić</p>	Administratorzy
<p><u>Profil wydajnościowy systemu</u> Pozwala użytkownikom na optymalizację profili systemowych.</p>	Administratorzy
<p><u>Wyjmowanie komputera ze stacji dokującej</u> Pozwala użytkownikom na odblokowanie i wyjęcie notebooka ze stacji dokującej.</p>	Administratorzy Użytkownicy
<p><u>Zastąpienie tokeny poziomu procesu</u> Pozwala użytkownikom na modyfikację tokena bezpieczeństwa dostępu procesu. Jest to prawo używane tylko przez system.</p>	Usługa lokalna Usługa sieciowa

Prawa użytkownika	Rekomendowane ustawienia
<p><u>Przywracanie plików lub folderów</u> Pozwala użytkownikom na przywrócenie z wykonanych kopii plików lub folderów To prawo jest powiązane z prawami do plików i folderów Informacja: Jeśli istnieją operatory kopi w sieci to im również należy nadać odpowiednie uprawnienia</p>	Administratorzy
<p><u>Zamykanie systemu</u> Umożliwia użytkownikom zamknięcie systemu Windows XP</p>	Administratorzy Użytkownicy
<p><u>Synchronizacja danych usług katalogowych</u> Pozwala użytkownikom / grupom na synchronizację danych usług katalogowych, zwaną również Synchronizacją Active Directory</p>	(Nikt)
<p><u>Przejmowanie własności plików i obiektów</u> Pozwala użytkownikom na przejmowanie własności nad plikami, folderami, drukarkami, i innymi obiektami w systemie. Uprawnienia te są mocniejsze od praw protekcji obiektów.</p>	Administratorzy

Tabela 5 Opcje praw użytkowników

Opcje Bezpieczeństwa

Sekcja Opcji bezpieczeństwa szablonów bezpieczeństwa zawiera wiele parametrów bezpieczeństwa, które mogą być łatwo skonfigurowane przez dodawanie lub zmianę wartości kluczy rejestru. Rekomendowane ustawienia opcji bezpieczeństwa zostały przedstawione w tabeli numer 6. Dopasowywane opcje bezpieczeństwa dodane w szablonach NSA zostały zaznaczone na szaro.

OSTRZEŻENIE: Używanie narzędzi konfiguracji bezpieczeństwa jest szczególnie nie bezpieczne, dlatego zaleca się szczególną ostrożność podczas modyfikacji klucza rejestru, gdyż nie sprawdzone, błędne zmiany mogą doprowadzić nawet do konieczności reinstalacji systemu



Informacja: Większość ustawień bezpieczeństwa dokonuje się poprzez modyfikację klucza rejestru. Wszelkie ustawienia mają swoje odnośniki w odpowiednich kluczach rejestru. Ich modyfikacja nie wymaga odnoszenia do poprzez API

Atrybut Bezpieczeństwa	Rekomendowane ustawienia
<p><u>Konta: Status kont Administratorów</u> Kontrola statusu konta lokalnego domyślnego Administratora podczas normalnych operacji. Konto Administratora jest zawsze włączone w Trybie Awaryjnym bez względu na ustawienia</p>	Włączone
<p><u>Konta: Status konta Gość</u> Kontroluje status konta Gość. Jest ono domyślnie wyłączone Informacja: Jeśli konto Gość jest wyłączone I opcja bezpieczeństwa Dostęp sieciowy: Udostępnianie I ochrona dla lokalnych kont jest ustawiona tylko dla Gości usługi logowania sieciowego mogą zawieść</p>	Wyłączone
<p><u>Konta: Limitowanie kont używających pustych haseł do logowania tylko do konsoli systemu</u> Kontroluje czy lokalne konta z pustymi hasłami mogą być używane do logowania do sieci. Jeśli ustawienie jest włączone lokalne konta z pustymi hasłami nie mogą być użyte do połączenia z systemem poprzez usługi sieciowe, włączając w to Windows Network i Usługi Terminalowe Informacja: Ustawienie to dotyczy tylko kont lokalnych , a nie dotyczy kont w domenie HKM\System\CurrentControlSet\Control\Lsa\ LimitBlankPasswordUse = 1</p>	Włączone
<p><u>Konta: Zmiana nazwy konta Administratora</u> Konto Administratora stworzone domyślnie podczas instalacji systemu Windows XP skojarzone z konkretnym SID'empo zmianie nazwy może utrudnić potencjalnym włamywaczom próby zalogowania na to konto. Podczas wybierania nowej nazwy konta należy unikać nazw takich jak „admin”, „root”, które mogłyby sugerować znaczenie konta. Zaleca się, bo zmianie nazwy również dokonać zmiany opisu konta Informacja: Dostarczone szablony nie posiadają wzorów ani gotowych rozwiązań zmiany nazwy konta. Zaleca się jednak wykonanie tej czynności Informacja: Jeśli konto anonymous jest nie ograniczone dla numerowanej liczny użytkowników to sama zmiana nazwy konta administratora będzie miała ograniczone korzyści. Jeśli konto anonymous jest chronione przed dostarczaniem informacji o kontach, zmiana nazwy konta administratora przynosi więcej korzyści. Zobacz opcje bezpieczeństwa dotyczące przywilejów konta anonymous w sekcji dostępu sieciowego</p>	<lokalnie ustawione>

Atrybuty Bezpieczeństwa	Rekomendowane ustawienia
<p><u>Konta: Zmiana nazwy konta Gość</u> Konto Gość stworzone jest domyślnie podczas instalacji Windows XP, ale jest ono wyłączone. Połączony z kontem Gość SID z inną nazwą może utrudnić działania potencjalnym włamywaczom, którzy chcą wykorzystać konto Gość. Po zmianie nazwy zaleca się by opis konta został zmieniony lub skasowany. Informacja: Dołączony szablon nie posiada zdefiniowanych ustawień środowiska pod kontekstem takiej zmiany, jednakże zaleca się wykonanie tej czynności.</p>	<p>Konfigurowane lokalnie</p>
<p><u>Audyt: Audyt dostępu globalnych elementów systemu</u> Kontrola możliwości audytu globalnych elementów systemu. Kiedy jest włączone obiekty systemu takie jak zdarzenia, urządzenia są tworzone przez domyślną listę kontroli systemu (SACL).</p> <p>OSTRZEŻENIE: Włączenie tej opcji z dużą ilością zdarzeń zmusza do ciągłego zapisu w logach bezpieczeństwa. W związku z tym zaleca się by opcja ta była włączona tylko jeśli to jest niezbędne</p> <p>Informacja: BY audyt dostępu do obiektów był możliwy (Audit object access) zasady audytu muszą być włączone. HKLM\System\CurrentControlSet\Control\Lsa\AuditBaseObjects</p>	<p>Nie zdefiniowane</p>
<p><u>Audyt: Audyt używania przywileju tworzenia kopi (Backup'u)</u> Kontrola możliwości audytu użycia przywilejów użycia opcji Backup'u i przywracania (Restore). Jeśli zasada jest wyłączona pewne prawa użytkowników nie będą audytowane, nawet jeśli audyt uprzywilejowanego użycia będzie włączony.</p> <p>OSTRZEŻENIE: Włączenie tej opcji z dużą ilością zdarzeń zmusza do ciągłego zapisu w logach bezpieczeństwa. W związku z tym zaleca się by opcja ta była włączona tylko jeśli to jest niezbędne</p> <p>Informacja: By audyt praw użytkowników "Audit privilege use" był możliwy zasada audytu musi być włączona. HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing</p>	<p>Nie zdefiniowane</p>

Atrybuty Bezpieczeństwa	Rekomendowane ustawienia
<p><u>Audyt: Zamknięcie systemu bezwzględnie, jeśli nie można załadować audytu bezpieczeństwa</u></p> <p>Jeśli zdarzenie nie może zostać zapisane do dziennika zdarzeń następuje zatrzymanie systemu co objawia się błędem: STOP: C0000244 {Audit Failed} An attempt to generate a security audit failed.</p> <p>Jeśli zatrzymanie systemu zostanie spowodowane przepełnieniem pliku logu bezpieczeństwa administrator musi go wyczyścić</p> <p>Informacja: Generalnie rekomenduje się by to ustawienie było włączone, jednakże z powodów problemów, jakie mogą wystąpić w przypadku pozytywnego wystąpienia audytu można opcję tą wyłączyć. Można to rozwiązać poprzez ustawienie czynności, które ma wykonać system przy pierwszym wystąpieniu tego problemu – restart systemu. Jednakże może to także doprowadzić do sytuacji ciągłych restartów i blue – screen’ów czy powieszenia się systemu. Załogować w konsekwencji będą mogli tylko administratorzy, którzy będą musieli zmienić wartość klucza rejestru CrashOnAuditFail z 2 na 0 lub 1 by przywrócić system do użytku dla użytkowników. Zachowanie takie nie występuje jeżeli zmiana zasad audytu jest nie włączona.</p> <p>Ostrzeżenie: Włączenie tej opcji doprowadzi do niemożności połączenia do systemu aż do momentu wyczyszczenia logów. Należy wziąć to pod uwagę, jeśli opcja ta będzie włączana na systemie produkcyjnym. Również włączenie tej opcji na wielu stacjach roboczych w sieci, może przynieść podobny efekt jeśli logi się zapelniają. Również rejestracja ciągła tego typu zdarzeń – niepomyślnie przeprowadzanych ataków doprowadzi do zapelnienia log dużą ilością śmieci.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail =0</p>	Wyłączone
<p>Kontroluje fakt czy użytkownicy mogą wyciągnąć komputer ze stacji dokującej bez zalogowania. Wyłączenie tej opcji zmusza użytkowników do zalogowania przed żądanie odblokowania. Użytkownicy muszą mieć prawo wyłączenie komputera ze stacji dokującej (Remove computer from docking station)</p> <p>Informacja: Ustawienia te dotyczą tylko kontrolera odblokowywania, gdzie odpowiednia usługa jest stopowana gdy komputer jest odblokowywany. Nie ma nic co by chroniło przed atakami polegającymi na fizycznym odłączeniu komputera.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon = 0</p>	Wyłączone
<p>Urządzenia: Pozwolenie na format i wyjęcie przenośnych nośników. Determinuje kto jest upoważniony do formatowania i wyjmowania przenośnych nośników NTFS</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD = 0</p>	Administratorzy

Atrybuty Bezpieczeństwa	Rekomendowane ustawienia
<p><u>Urządzenia: Zapobiegaj</u> Ustawienia te określają kto ma prawa do instalacji sterowników do drukarek podczas procesu dodawania drukarki. Sterowniki drukarki, jako sterowniki niskiego poziomu mają dostęp do ograniczonych zasobów systemu. Sterowniki takie mogą wykonywać działania, które nie są dozwolone dla zwykłych użytkowników. Administratorzy powinni zainstalować wszystkie sterowniki, które są przetestowane i zoptymalizowane. Ustawienie to pomaga w ograniczeniu prawa instalowania sterowników, które nie są zweryfikowane. Informacja: Jeśli sterownik drukarki istnieje w systemie użytkownicy dodający drukarki mogą wykonać tą czynność nawet jeśli jest włączona ta opcja. HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers = 1</p>	Włączone
<p><u>Urządzenie: Ograniczenie dostępu do CD - Rom jedynie dla lokalnie zalogowanych użytkowników</u> Domyślnie programy mogą mieć dostęp do CD-ROM, by doczytywać dane. Ustawienie to określa czy CD-ROM jest dostępny I dla użytkowników lokalnych I zdalnych. Jeśli włączone tylko użytkownicy zalogowani mają dostęp do CD-ROM. Jeśli nikt nie jest zalogowany wtedy CD-ROM może być dostępny przez sieć. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms = 1</p>	Włączone
<p><u>Urządzenie: Ograniczenie dostępu do stacji dyskietek jedynie dla lokalnie zalogowanych użytkowników</u> Domyślnie programy mogą mieć dostęp do stacji dyskietek, by doczytywać dane. Ustawienie to określa czy stacji dyskietek jest dostępny I dla użytkowników lokalnych I zdalnych. Jeśli włączone tylko użytkownicy zalogowani mają dostęp do stacji dyskietek. Jeśli nikt nie jest zalogowany wtedy CD-ROM może być dostępny przez sieć. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies = 1</p>	Włączone
<p><u>Urządzenie: Zachowanie podczas instalacji sterowników nie podpisanych</u> Ustawienie to określa zachowanie podczas próby instalacji sterowników, które nie zostały podpisane cyfrowo. Ustawienie to pozwala na: Brak zgłoszenia, Ostrzeżenie ale zezwolenie na instalację, Zabronienie instalacji HKLM\Software\Microsoft\Driver Signing\Policy = 1</p>	Wyłączone ale dozwolona instalacja
<p><u>Kontroler domeny: Zezwalaj operatorom serwera na harmonogramowanie zadań</u> Ustawienie określa czy operatorzy serwera mogą tworzyć harmonogramy zadań używając narzędzi. Nie wpływa to na Harmonogram Zadań.</p>	Nie zdefiniowane
<p><u>Kontroler domeny: Wymaganie sygnatury serwera</u> Wymaga podpisania danych zanim serwer (LDAP) zautentyfikuje klientów LDAP.</p>	Nie zdefiniowane

Atrybuty Bezpieczeństwa	Rekomendowane ustawienia
<p><u>Kontroler domeny: Odrzucenie zmiany hasła komputera</u> Określa czy kontroler domeny zaakceptuje żądanie zmiany hasła dla konta komputera. Ustawienie to jest nie zdefiniowane na stacjach roboczych.</p>	Nie zdefiniowane
<p><u>Członek domeny: Cyfrowe kodowanie lub podpis bezpiecznego kanału danych</u> Ustawienie kontroluje podpis i kodowanie transmitowanych danych poprzez bezpieczny kanał. Ustawienie powinno być włączone jedynie, jeśli w środowisku domeny, gdzie wszystkie kontrolery mają możliwość podpisu lub kodowania w bezpiecznych kanałach danych. Oznacza to, że kontroler domeny musi być uruchomiony albo na Windows 2000 albo na Windows NT 4.0 z Service Pack'iem 4 lub wyższym. W innym wypadku ustawienie powinny być wyłączone lub pozostać nie zdefiniowane. Kiedy jest to wyłączone można nadal zestawiać tego typu kanały, lecz bezpieczeństwo podpisywania i kodowania jest już dyskusyjne.</p>	Nie zdefiniowane
<p><u>Członkowie domeny: Cyfrowe kodowanie bezpiecznych kanałów danych</u> Jeśli włączone należy się upewnić, że wszystkie kolejki bezpiecznych kanałów są kodowane, a także sprawdzić czy kontrolery domeny mają możliwość obsługi takiej opcji. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ SealSecureChannel = 1</p>	Włączone
<p><u>Członkowie domeny: Cyfrowy podpis bezpiecznych kanałów danych, (jeśli jest to możliwe)</u> Jeśli włączone należy się upewnić, czy wszystkie kolejki bezpiecznych kanałów, za równo dla klientów, jak i serwerów są zgodne z protokołem podpisywania. Cyfrowy podpis pomaga zapewnić prawność i autentyczność wiadomości. Informacja: Jeśli członek domeny: Cyfrowy podpis lub kodowaie jest włączony, opcja ta jest automatycznie uaktywniana. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ SignSecureChannel=1</p>	Włączone
<p><u>Członek domeny Wyłączenie zmian haseł kont komputerów</u> Ustawienie to określa możliwość członków domeny do zmian haseł kont ich komputerów. Ustawienie to powinno być wyłączone, by członkowie domeny próbowali zmienić hasło konta komputera, szczególnie w sytuacji, gdy aktywne jest Członek domeny: Maksymalny czas na zmianę hasła konta komputera". HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ DisablePasswordChange=0</p>	Wyłączone
<p><u>Członkowie domeny: Maksymalny czas hasła konta komputera</u> Ustawienie to określa maksymalny okres na zmianę hasła, domyślnie ustawione jest na do 30 dni. Zaleca się zmianę na 7 dni. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ MaximumPasswordAge=7</p>	7 dni

Atrybut Bezpieczeństwa	Rekomendowane ustawienie
<p><u>Członkowie domeny: Wymaganie mocnego (Windows 2000 lub następne) klucza sesji</u> Kiedy jest włączone, bezpieczny kanał może być tylko zestawiony z kontrolerami domeny, które ustanawiają połączenie z kodowaniem z mocnym (128-bit) kluczem sesji. Ostrzeżenie: By włączyć to ustawienie, wszystkie kontrolery domeny w domenie muszą mieć możliwość kodowania z mocnym kluczem, co oznacza, że kontrolerami domeny mogą być tylko komputery z systemem Windows 2000 lub późniejszym. Jeśli istnieje konieczność komunikacji z innymi kontrolerami domeny, należy tą opcję wyłączyć. HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\ RequireStrongKey=1</p>	Włączone
<p><u>Interaktywne logowanie: Brak wyświetlania nazwy ostatnio logującej się osoby</u> Ustawienie określa czy będzie wyświetlana nazwa ostatnio zalogowanego użytkownika w oknie logowania do systemu Windows Informacja: W pewnych okolicznościach opcja ta może być wyłączona. Na przykład, jeśli administratorzy, koncentrują się na niezautoryzowanych fizycznych dostęпах do systemu, co może w przypadku wyłączenie tej opcji przydatne. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ DontDisplayLastUserName= 1</p>	Włączone
<p><u>Interaktywne logowanie: Pozwolenie na automatyczne logowania administratora</u> Zezwala by podczas startu systemu, możliwe było automatyczne zalogowanie się jako konto administratora. Domyślnie opcja ta jest wyłączona. Informacja: Jeśli opcja ta była włączona to może istnieć klucz w rejestrze DefaultPassword. Ciąg ten zawiera hasło administratora zapisane w postaci otwartego tekstu i może zostać odczytane poprzez zdalny dostęp przez sieć. Dlatego też powinien zostać usunięty. HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\AutoAdminLogon = 0</p>	Wyłączone
<p><u>Interaktywne logowanie: Nie wymagaj CTRL+ALT+DEL</u> Jeśli opcja ta jest włączona, użytkownik nie musi nacisnąć, by zalogować się. CTRL+ALT+DEL tworzy zaufaną ścieżkę do operacji systemowych, które zawierają użytkowników i hasła. Wyłączenie jednak powoduje pewne ryzyko bezpieczeństwa dla referencyjnych logowań użytkownika. Domyślnie opcja ta jest włączona na stacji roboczej w domenie, a włączona dla wolno stojących stacji roboczych. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ DisableCAD = 0</p>	Wyłączone
<p><u>Interaktywne logowanie: Wiadomość tekstowa dla użytkowników próbujących się zalogować.</u> System powinien wyświetlać wiadomość ostrzegawczą przed logowaniem, oznajmującym prywatny charakter systemu. Wiele organizacji rządowych używa wiadomości tekstowej by ostrzec potencjalnych użytkowników, że będą monitorowani i będą odpowiadać z tytułu przepisów prawa karnego, jeśli będą wykorzystywać to bez odpowiednich praw autoryzacji. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ LegalNoticeText="Message text of your choice"</p>	<Konfiguracja lokalna – zobacz załącznik jako przykład>

Atrybuty bezpieczeństwa	Rekomendowane ustawienia
<p>Interaktywne logowanie: Tytuł wiadomości dla użytkowników próbujących się zalogować</p> <p>Użytkownicy, którzy logują się do systemu i otrzymują odpowiednią wiadomość tekstową, powinni również zobaczyć komunikat ostrzeżenia na tabliczce tytułowej.. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption="Caption of your choice to be displayed on the title bar"</p>	<p><konfiguracja lokalna – zobacz załączniki dla przykładu></p>
<p>Interaktywne logowanie: Liczba wcześniejszych logowań przechowywane w pamięci podręcznej – cache (w przypadku, gdy kontroler domeny jest niedostępny)</p> <p>Liczba tego typu logowań określona jest przez to ustawienie. Pozwala to użytkownikom na zalogowanie się do systemu nawet, jeśli nie jest podpięty do sieci lub kontroler domeny jest niedostępny.</p> <p>Ostrzeżenie: Ustawienie 0 powoduje, iż użytkownicy nie będą mogli się zalogować do domeny dopóki nie będą oni podpięci do sieci. Jest to nie wygodne ustawienie dla użytkowników laptopów, którzy często pracują poza obszarem biura.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=0</p>	<p>0 logowań</p>
<p>Interaktywne logowanie: Przypominaj o zmianie hasła zanim ono wygaśnie</p> <p>Ustawienie to określa jak długo użytkownicy będą ostrzegani o wygasaniu hasła. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning=14</p>	<p>14 dni</p>
<p>Interaktywne logowanie: Wymaganie autoryzacji kontrolera domeny do odblokowania stacji roboczej</p> <p>Kiedy włączone kontroler domeny musi zautentykować konto podczas odblokowywania systemu.</p> <p>Ostrzeżenie: Jeśli kontroler domeny będzie niedostępny, systemy z zablokowanymi ekranami nie będą miały możliwości odblokowania na stacjach roboczych</p> <p>Informacja: Ta opcja może nie być właściwa dla posiadaczy laptopów. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=1</p>	<p>Włączone</p>

Atrybuty bezpieczeństwa	Rekomendowane ustawienia
<p><u>Interaktywne logowanie: Wyjęcia Smart Card</u> Ustawienie określa jakie będzie zachowanie systemu, na którym zalogowany jest użytkownik, po wyjęciu Smart Card. Możliwe opcje: Brak reakcji Blokowanie stacji Użytkownicy mogą wyjąć smart card, a potem ją przywrócić. Procedura wylogowywania Automatyczne wylogowane po wyjęciu Smart Card. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption= 1</p>	Blokowanie stacji roboczej
<p><u>Klient sieci Microsoft: Cyfrowa (podpis) komunikacja (zawsze)</u> Włączone prowadzi do wysyłania 8MB klienta z 8MB cyfrowym podpisem. Cyfrowy podpis zamyka próby włamań „coś w środku” i wspiera autentykację wiadomości, co chroni przed atakami na wiadomości. Informacja: Rekomenduje się tą opcję do włączenia w środowiskach tylko z Windows 2000/XP HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature</p>	Nie zdefiniowane
<p><u>Klient sieci Microsoft: Cyfrowa komunikacja (jeśli serwer dopuści taką sytuację)</u> Kiedy włączone klientowi SMB optymalizują podpisane pakiety podczas komunikacji z serwerem SMB, które wymaga lub ma taką opcję włączoną. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=1</p>	Włączone
<p><u>Klient sieci Microsoft: Wysyłania odkodowanego hasła do „trzecich” serwerów SMB</u> Wyłączenie tej opcji ochrania przed przekierowywaniem na serwerach SMB wiadomości zawierających hasło zapisane otwartym tekstem do innych nie Microsoft’u serwerów SMB, które nie wspierają kodowania hasła podczas autentykacji. Ostrzeżenie: Włączenie pozwoli na odkodowane (czysty tekst) wysyłanie hasła poprzez sieć w trakcie autoryzacji na serwerach SMB. To zredukuje poziom bezpieczeństwa środowiska i powinno być jedynie dozwolone po dokładnym rozważeniu konsekwencji wysyłania odkodowanego hasła. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=0</p>	Wyłączone
<p><u>Sewer sieci Microsoft: Wartość czasu bezczynności zanim zosanie wykonane żądanie uśpienia</u> Określa wartość czasu bezczynności, po którym sesja SMB zostanie przeniesiona w stan uśpienia. Jeśli klient wznowi po rozłączeniu działanie sesja zostanie automatycznie zestawiona ponownie.. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=1 5</p>	1 5 minut

Atrybuty bezpieczeństwa	Rekomendowane ustawienia
<p><u>Serwer sieci Microsoft: Cyfrowy podpis połączenia (zawsze)</u> Informacja: Włączenie tej opcji może być pożądaną by chronić przed zmniejszaniem poziomu klientów przy użyciu stacji roboczej jako serwera sieciowego. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature</p>	Nie zdefiniowane
<p><u>Serwer sieci Microsoft: Cyfrowy podpis komunikacji, (jeśli klient wyrazi zgodę)</u> Określa czy serwer SMB optymalizuje podpisywanie pakietów. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=1</p>	Włączone
<p><u>Serwer sieci Microsoft: Rozłączanie, gdy wygasną godziny używania</u> Określa czy użytkownicy zostaną rozłączeni, gdy ustalone godziny ich działalności zostaną przekroczone. HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogoff=1</p>	Włączone
<p><u>Dostęp sieciowy: pozwolenie na translacje SID'a użytkownikom anonymous</u> Określa czy użytkownik anonymous może zarządzać identyfikatorem bezpieczeństwa (SID) dla innego użytkownika lub użyć SID'a by otrzymać nazwę użytkownika.</p>	Wyłączone
<p><u>Dostęp sieciowy: Nie zezwalaj użytkownikom anonymous na wylistowanie konta z SAM</u> Ustawienie to kontroluje możliwość dostępu do SAM przez użytkowników anonymous. Ta opcja bezpieczeństwa pozwala dodatkowo na restrykcje na połączenie anonymous: Brak. Domyślne ustawienia. Nie pozwól na odczyt kont z SAM. Ta opcja zastępuje "wszyscy" z Autentykowane użytkownicy" w prawach dostępu do zasobów. Ta opcja jest ustawiona jako domyślna w Windows XP. Ostrzeżenie: Włączenie tej opcji ma wpływ na możliwości administracyjne dla użytkowników w zaufanych domenach, które nie obsługują zwrotnego zaufania. HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=1</p>	Włączone

Atrybuty bezpieczeństwa	Rekomendowane ustawienia
<p><u>Dostęp sieciowy: Nie zezwalaj użytkownikom anonymous na odczyt kont oraz zasobów z SAM</u></p> <p>Ustawienie to kontroluje możliwość dla użytkowników typu anonymous do odczytu kont oraz zasobów z SAM. Ta opcja domyślnie jest wyłączona w Windows XP</p> <p>Informacja: System musi zostać uruchomiony ponownie by ustawienia te przyniosły efekt.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=1</p>	Włączone
<p><u>Dostęp sieciowy: Nie zezwalaj na przechowywanie dokumentów, referencji lub paszportu.NET</u></p> <p>Ustawienie to kontroluje przechowywanie dokumentów lub haseł autentykacji w lokalnym systemie.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=1</p>	Włączone
<p><u>Dostęp sieciowy: Przenieść uprawnienia Wszyscy na użytkowników anonymous</u></p> <p>Określa dodatkowe zagwarantowane prawa dla połączeń typu anonymous do komputera. Kiedy jest wyłączone prawa gwarantowane dla Wszyscy nie są automatycznie przenoszone na anonymous. Użytkownicy Anonymous mogą jedynie posiadać dostęp do zasobów , które mają zdefiniowane takie prawa.</p> <p>Informacja: Wyłączenie tej opcji jest jednoznaczne z ustawieniem wartości 2 dla RestrictAnonymous w Windows 2000.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\ EveryoneIncludesAnonymous=0</p>	Wyłączone
<p><u>Dostęp sieciowy: Tylko nazwane komunikacje będą umożliwiające</u></p> <p>Pakiety są integralną częścią procesu komunikacji, który jest identyfikowany przez ID, które są różne w systemach. By ułatwić proces zachodzi proces nadawania nazw, które nie różnią się w systemach To określa, które połączenie anonymous będą dostępne.</p> <p>HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes</p>	Nie zdefiniowane
<p><u>Dostęp sieciowy: Zdalny dostęp do ścieżki rejestru systemu</u></p> <p>Określa czy dostęp do określonej ścieżki rejestru możliwy jest poprzez zdalne połączenie.</p> <p>HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\ AllowedPaths\Machine</p>	Nie zdefiniowane
<p><u>Dostęp sieciowy: Zasoby, które mogą być dostępne dla anonymous</u></p> <p>Określa, które zasoby będą dostępne dla użytkowników i połączeń anonymous.</p> <p>HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares</p>	Nie zdefiniowane

Atrybut Bezpieczeństwa	Zalecane Ustawienia
<p>Dostęp do sieci: Modele zabezpieczeń i udostępniania dla kont lokalnych Ustawienie to kontroluje, w jaki sposób identyfikatory sieciowe używane przez konta lokalne są uwierzytelniane. Model "Klasyczny wymusza używanie uwierzytelniania dla kont lokalnych do zalogowania się do sieci, podczas gdy model "Tylko Gość" pozwala na mapowanie identyfikatorów sieciowych do konta użytkownika, bez względu na przedstawiane przez niego uwierzytelnienie. Model "Klasyczny" zapewnia dobra kontrole dostępu do zasobów. Dla każdego zasobu można zapewnić różne rodzaje dostępu dla różnych użytkowników. Dla komputerów połączonych w domenę, opcja ta w Windows XP Professional ustawiona jest na model Klasyczny. Model "Tylko Gość" ustawiany jest jak domyślny przez Windows XP, dla komputerów pracujących osobno.</p> <p>Uwaga: Ustawienie to nie dotyczy identyfikatorów sieciowych używających kont w domenie oraz identyfikatorów interaktywnych używanych do korzystania z usług takich jak Telnet lub Usług Terminalowe.</p> <p>OSTRZEŻENIE: Model "Tylko Gość" pozwala każdemu użytkownikowi posiadającemu dostęp do komputera poprzez sieć (włączając w to anonimowych użytkowników Internetu) na dostęp do udostępnianych zasobów.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\ForceGuest=0</p>	<p>Klasyczne: lokalni użytkownicy uwierzytelniają się nazwami własnymi</p>
<p>Bezpieczeństwo sieci: Podczas kolejnej zmiany hasła nie zachowuj znaków w LAN Manager Uruchomienie tej opcji zapobiega zachowaniu znaków w LAN Manager i SAM podczas kolejnych zmian hasła.</p> <p>UWAGA: The LAN Manager hash jest wykorzystywany do uzyskania kompatybilności z komputerami pracującymi na systemach starszych niż WinNT oraz z niektórymi aplikacjami. Ponieważ jest są to hasła Windows konwertowane na wielkie litery oraz traktowany jak 2 hasła składające się z 7 znaków, jest bardziej narażony na ataki (ewentualne złamanie) jest także głównym celem dla wszelkich aplikacji łamiących hasła. Dlatego też rekomendowane jest wyłączenie zapisywania hasła LM w SAM.</p> <p>OSTRZEŻENIE: Wyłączenie tej opcji spowoduje problemy z połączeniem z systemami operacyjnymi lub aplikacjami, które wymagają uwierzytelniania LANManager.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash=1</p>	<p>Włączone</p>
<p>Bezpieczeństwo sieci: Wymuszaj wylogowanie, gdy upłynie czas zalogowania Gdy ta opcja jest włączona, sesje klienta z serwerem SMB są przymusowo rozłączane, gdy czas zalogowania klienta przekroczy odpowiednia ilość godzin zalogowania się danego klienta.</p>	<p>Włączone</p>

Atrybut Bezpieczeństwa	Zalecane Ustawienia
<p>Bezpieczeństwo sieci: Poziom uwierzytelniania LAN Manager</p> <p>Ten parametr określa rodzaje wywołań/odpowiedzi uwierzytelniających używanej do identyfikacji klientów Windows nie pracujących w Windows 2000/XP. Weryfikacja LanManager (LM) jest najmniej bezpieczna z metod, zezwalającą na łatwe przechwycenie zakodowanych haseł z sieci oraz ich złamanie. Weryfikacja NT LanManager (NTLM) jest nieco bezpieczniejsza. NTLMv2 jest bardziej solidna wersja NTLM, jest dostępna w Windows XP, Windows 2000, Windows NT wersja Service Pack 4 i wyższe oraz w Windows 95/98 z opcjonalnym Klientem Usług Katalogowych.</p> <p>Dostępne są następujące opcje: Send LM & NTLM responses - Registry value = 0. Send LM & NTLM – use NTLMv2 session security if negotiated - Registry value = 1. Send NTLM response only - Registry value = 2. Send NTLMv2 response only - Registry value = 3. Send NTLMv2 response only\refuse LM - Registry value = 4. Send NTLMv2 response only\refuse LM and NTLM - Registry value = 5.</p> <p>OSTZREZENIE: Niektóre procesy systemu Windows, jak na przykład Grupowe Usług, wykorzystują do weryfikacji NTLM. Wykorzystanie ustawień zalecanych może spowodować błędy podczas korzystania z danej usług. Więcej informacji na temat NTLM oraz Usług Grupowych można uzyskać pod adresem: http://support.microsoft.com/default.asp?scid=kb;EN=US;q272129 KB Article Q272129</p> <p>OSTRZEŻENIE: Ustawienie tej wartości na wyższą od 2 w systemie Windows XP może przeszkodzić w uzyskaniu połączenia z systemami wykorzystującymi weryfikację LM (Windows 95 ® /98 ® i Windows for Workgroups ®) lub tylko NTLM (Windows NT 4.0 wersje wcześniejsze niż Service Pack 4). W celu uzyskania zabezpieczenia NTLMv2 w komputerach pracujących pod Windows 9x Można zainstalować Klienta Aktywnych Usług Katalogowych.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 5</p>	<p>Send NTLMv2 response \ refuse LM and NTLM</p>
<p>Bezpieczeństwo sieci: Wymagania oznaczeń klienta LDAP.</p> <p>Ustawienie to kontroluje wymagania oznaczeń klienta LDAP. Konieczne jest, aby oznaczenia danych były negocjowane zanim klienci Lightweight Directory Access Protocol (LDAP) połączą się z serwerem Active Directory LDAP.</p> <p>HKLM\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=1</p>	<p>Negocjuj oznaczenia</p>
<p>Bezpieczeństwo sieci: Minimalne zabezpieczenia sesji opartych na klientach NTLM SSP (włączając w to zabezpieczenia RPC).</p> <p>To ustawienie określa minimalne standardy bezpieczeństwa dla klienta podczas sesji komunikacji aplikacja-aplikacja.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=537395200</p>	<p>Wymagaj zabezpieczeń sesji NTLMv2. Wymagaj szyfrowania 128-bitowego</p>

Atrybut Bezpieczeństwa	Zalecane Ustawienia
<p>Bezpieczeństwo sieci: Minimalne zabezpieczenia sesji opartych na serwerach NTLM SSP (włączając w to zabezpieczenia RPC). To ustawienie określa minimalne standardy bezpieczeństwa dla serwera podczas sesji komunikacji aplikacja-aplikacja.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=537395200</p>	<p>Wymagaj zabezpieczeń sesji NTLMv2, Wymagaj szyfrowania 128-bitowego</p>
<p>Konsola odzyskiwania: Zezwalaj na automatyczne logowanie administracyjne Konsola odzyskiwania pracuje w trybie linii poleceń i służy do przywracania sprawności po problemach z systemem. Jeśli ta opcja jest uruchomiona, konto administratora będzie automatycznie zalogowywane do konsoli odzyskiwania, gdy zostanie ona wywołana podczas startu. Ustawienie to powinno być wyłączone, w ten sposób do zalogowania się do konsoli wymagane będzie podanie hasła.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=0</p>	<p>Wyłączone</p>
<p>Konsola odzyskiwania: Zezwalaj na kopiowanie i dostęp z dyskiety do wszystkich dysków i katalogów. Gdy opcja ta jest włączona, użytkownik ma pełen dostęp do wszystkich dysków w systemie i może kopiować pliki z dysku twardego na dyskietkę. Polecenie Konsoli Odzyskiwania SET jest dostępne, pozwala ono użytkownikom na ustawienie następujących zmiennych w środowisku Konsoli Odzyskiwania: "AllowWildCards", "AllowAllPaths", "AllowRemovableMedia", oraz "NoCopyPrompt". Wyłączenie tej opcji uniemożliwia kopiowanie plików z dysku twardego na dyskietkę. Dodatkowo wprowadza ograniczenia dostępu do dysków i katalogów.</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=0</p>	<p>Wyłączone</p>
<p>Zamknięcie: Zezwalaj na zamknięcie systemu bez konieczności logowania Ustawienie to określa czy system może zostać zamknięty bez konieczności zalogowania się. Gdy ta opcja jest włączona, komenda zamknięcia systemu jest widoczna ekranie logowania Windows. Opcja ta powinna być wyłączona, aby ograniczyć uprawnienie do zamknięcia systemu do uwierzytelnionych użytkowników.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=0</p>	<p>Wyłączone</p>
<p>Zamknięcie: Wyczyść zawartość pliku stronicowania Pamięć wirtualna wykorzystuje systemowy plik do przemieszczania kart pamięci na dysk, gdy nie są wykorzystywane. Jeśli plik wymiany zostanie oczyszczony, żadna istotna informacja, która mogła być przechowywana w pamięci wirtualnej nie będzie dostępna dla niewierzytelnionego użytkownika, nawet, gdy uzyska on bezpośredni dostęp do pliku wymiany.</p> <p>UWAGA: Uruchomienie tej opcji znacznie wydłuży czas zamykania systemu.</p> <p>HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=1</p>	<p>Włączone</p>
<p>Szyfrowanie systemowe: Używaj algorytmów zgodnych z FIPS do szyfrowania, podpisywania, Ustawienie to gwarantuje, że Dostawca Zabezpieczenia TLS/SSL używa do szyfrowania, podpisywania, hasłowania algorytmów, które są zgodne z FIPS. Algorytmy zgodne z FIPS to te, które spełniają standardy wyznaczone przez Rząd Stanów Zjednoczonych.</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=1</p>	<p>Włączone</p>

Atrybut Bezpieczeństwa	Zalecane Ustawienia
<p>Obiekty systemowe: Domyślny właściciel obiektów stworzonych przez członków grupy Administratorów</p> <p>Ustawienie to określa czy grupa Administratorów czy też twórca obiektów są właścicielami wszelkich stworzonych obiektów systemowych. Ze względu na wymogi odpowiedzialności, twórca obiektów powinien być ich właścicielem</p> <p>HKLM\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=1</p>	Włączone
<p>Obiekty Systemowe: Wymagania niewrażliwości rejestrów klawiatury dla podsystemów nie pracujących w Windows.</p> <p>Ustawienie to określa czy niewrażliwości rejestrów klawiatury jest wymuszana dla wszystkich podsystemów. Gdy to ustawienia jest włączone, niewrażliwości rejestrów klawiatury jest wymuszana dla wszystkich obiektów katalogowych, łączy symbolicznych oraz obiektów IO.</p> <p>HKLM\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=1</p>	Włączone
<p>Obiekty systemowe: Ustaw bezpieczną ścieżkę poszukiwania dla DLL</p> <p>Ten klucz zmienia domyślny porządek poszukiwań, gdy DDL jest wywołany z:</p> <ul style="list-style-type: none"> Katalogu aplikacji Bieżącego katalogu Katalogów systemowych Ścieżki do Katalogu aplikacji Katalogów systemowych Bieżącego katalogu Ścieżki <p>W ten sposób DLL z katalogów systemowych są chronione przed zamiana na DLL z katalogów niesystemowych.</p> <p>UWAGA: W Windows XP Service Pack 1 (SP1) jest to zachowanie domyślne, nawet jeśli brak takiego ustawienia. Innymi słowy, jeśli brak takiego ustawienia w rejestrze system Windows XP RTM przeszukuje wpierw bieżący katalog zanim przeszuka katalogi systemowe, podczas gdy system Windows XP SP1 przeszukuje wpierw katalogi systemowe zanim przeszuka katalog bieżący.</p> <p>HKLM\System\CurrentControlSet\Control\Session Manager\ SafeDllSearchMode = 1</p>	Włączone
<p>Obiekty systemowe: Wzmocnienie domyślnych zezwoleń wewnętrznych obiektów systemowych (np. Symbolicznych Łączy)</p> <p>Wyłączenie tej opcji wzmacnia DACLS na ogólnej liście współdzielonych zasobów systemowych (jak np. nazwy urządzeń DOS, i sygnalizatory) tak, aby użytkownicy spoza grupy administratorów mogli czytać, ale nie modyfikować udostępnione obiekty, których nie stworzyli.</p> <p>HKLM\System\CurrentControlSet\Control\Session Manager\ProtectionMode = 1</p>	Włączone

Tabela 6 Opcje Bezpieczeństwa

Dodawanie pozycji do Opcji Bezpieczeństwa

W systemie Windows XP, możliwe jest dodanie do rejestru własnych ustawień Grupy

Narzędzi Konfiguracji Bezpieczeństwa. By tego dokonać, wykonaj następujące czynności:

- § Skopiuj plik `%SystemRoot%\inf\sceregl.inf` do innego pliku, pod inną nazwą.
- § W ten sposób zachowasz oryginalny plik w razie wystąpienia problemów.
- § Otwórz `%SystemRoot%\inf\sceregl.inf` w Notatniku, Wordpadzie, lub innym edytorze tekstu.
- § Dodaj linie w formie: *regpath, type, displayname, displaytype* gdzie
 - *regpath* – ścieżka wartości klucza rejestru, np.,
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects
 - *type* – typ danych we wpisie w rejestrze obrazowany cyfrą. Dostępne wartości to: REG_SZ (1), REG_EXPAND_SZ (2), REG_BINARY (3), REG_DWORD (4), REG_MULTISZ (7)
 - *displayname* – nazwa wyświetlana w szablonie bezpieczeństwa, np.,
“Kontrola dostępu do ogólnych obiektów systemu”
 - *displaytype* – W jaki sposób będzie wyświetlany typ wartości rejestru. Możliwe wartości: Boolean (0), number (1), string (2), choices (3), multivalued (4), bitmask (5). Wartości 4 i 5 są dostępne tylko w Windows XP.
 - Jeśli określono już możliwe wartości, wybór powinien zostać sprecyzowany w formie *value1/display1,value2/display2,...*
- § Ponownie zarejestruj `scecli.dll` uruchamiając `regsvr32 scecli.dll`, gdy system
- § zarządza komendy

Przykładowa linia w `sceregl.inf` wygląda następująco:

```
MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption,1,%ScRemove%,3,0|%ScRemove0%,1|%ScRemove1%,2|%ScRemove2%
```

Powyższe ciągi znaków są zdefiniowane w sekcji: [Strings] `sceregl.inf`:

```
%ScRemove% = Smart card removal behavior  
%ScRemove0% = No Action  
%ScRemove1% = Lock Workstation  
%ScRemove2% = Force Logoff
```



UWAGA: Zmodyfikowanie `sceregl.inf` konieczne jest tylko w systemie, w którym szablon bezpieczeństwa i/lub strategia grupowa są edytowane. W innych komputerach, otrzymujących ostatecznie nowe ustawienia dzięki algorytmowi podziału grupowego nie zachodzi konieczność edytowania `sceregl.inf`.

Więcej informacji na temat edytowania szablonów Menadżera Konfiguracji Bezpieczeństwa, można uzyskać pod adresem:

<http://support.microsoft.com/?scid=kb;en-us;Q214752> article Q214752.

Usuwanie zmodyfikowanych opcji

Usuwanie zmodyfikowanych opcji bezpieczeństwa nie polega na zwykłym usunięciu ich z pliku *sceregl.inf* i ponownym zarejestrowaniu DLL. Aby zagwarantować trwałe usunięcie opcji z szablonu, wykonaj następujące czynności:

- § Otwórz *sceregl.inf* w edytorze tekstu (np. Notatnik)
- § Usuń określoną opcje bezpieczeństwa z pliku *sceregl.inf* w sekcji *[Register Registry Values]*
- § W pliku *sceregl.inf* w sekcji oznaczonej "usuń te wartości z UI," dodaj klucz rejestru, który ma być usunięty z szablonu. Wzorując się na przykładzie wykorzystanym w poprzedniej sekcji, umieść w tej sekcji:
MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScRemoveOption .
- § Zapisz i zamknij *sceregl.inf*
- § Gdy system zażąda komendy, uruchom: *regsvr32 scecli.dll*
- § Aby potwierdzić, że opcja została usunięta, otwórz wtyczkę Szablonów Bezpieczeństwa w MMC i zauważysz, że opcja już nie widnieje w sekcji **Strategie Lokalne** →→→→**Opcje Bezpieczeństwa** plików szablonu.
- § Na zakończenie, ponownie edytuj *sceregl.inf*, usuń wpis poprzednio dodany pod "usuń te wartości z systemu," zapisz i zamknij ten plik, a następnie ponownie uruchom *regsvr32 scecli.dll*.

Modyfikowanie Ustawień Dziennika Wydarzeń Za Pomocą Szablonów Bezpieczeństwa

Dzienniki Wydarzeń Windows XP zapisują wydarzenia, w czasie ich zajścia. Dzienniki Wydarzeń Bezpieczeństwa, Aplikacji i Systemu zawierają informacje generowane przez specjalne ustawienia kontroli. Oprócz ustawień kontroli dopuszczonych przez szablony bezpieczeństwa, możliwa jest także kontrola innych obiektów systemowych, jak określone pliki, klucze rejestru, i drukarki.

W celu przejrzania ustawień monitora wydarzeń w szablonie bezpieczeństwa kliknij dwukrotnie:

- **Szablony Bezpieczeństwa**
- Domyślny katalog pliku konfiguracji (%SystemRoot%\Security\Templates)
- Określony plik konfiguracji
- **Monitor Wydarzeń**



UWAGA: Po dokonaniu jakichkolwiek modyfikacji plików konfiguracji upewnij się, że zmiany te zostały zapisane i przetestuj je zanim zainstalujesz je w pracującej sieci.

Ustawienia monitora wydarzeń

Ustawienia monitora wydarzeń, które mogą zostać zmienione przy pomocy szablonów bezpieczeństwa obejmują: rozmiar maksymalny, dostęp dla gości, jak długo monitory będą zachowywane oraz w jaki sposób system postępuje z monitorami, które osiągną maksymalny rozmiar

Aby zmodyfikować ustawienia Monitora za pomocą szablonów bezp., kliknij dwukrotnie ścieżkę:

Monitor → → → **Ustawienia Monitora** → → → → określoną opcję do wyświetlenia lub edycji

Tabela 7 lista zalecanych ustawień Monitora Wydarzeń dla Monitorów Aplikacji, Bezpieczeństwa i Systemu.

Ustawienia Dziennika Wydarzeń	Zalecane Ustawienia
Maksymalny rozmiar dziennika aplikacji Maksymalny rozmiar dziennika bezpieczeństwa Maksymalny rozmiar dziennika systemu Jeśli dzienniki są zbyt małe, zapełniają się częściej, i administratorzy muszą czyścić i zapisywać dzienniki częściej niż jest to wymagane. Dostępne rozmiary zawierają się między 64 KB a 4194240 KB. UWAGA: To ustawienie pozwoli plikowi dziennika na osiągnięcie rozmiarów równych przestrzeni dostępnej na dysku albo rozm. 4GB, zależnie od tego, która wartość jest mniejsza.	4194240 KB
Ograniczenie dostępu Gości do dziennika aplikacji Ograniczenie dostępu Gości do dziennika bezpieczeństwa Ograniczenie dostępu Gości do dziennika systemu Domyślna konfiguracja umożliwia Gościom oraz niezalogowanym przeglądanie monitorów zdarzeń (aplikacji i systemu). Podczas gdy dostęp do dziennika bezpieczeństwa jest domyślnie zamknięty dla Gości, mogą go oglądać użytkownicy, którzy posiadają uprawnienia Zarządzenie Dziennikami Kontroli. Opcja ta uniemożliwia gościom i niezalogowanym przeglądanie jakichkolwiek dzienników.	Włączone
Okres przechowywania dziennika aplikacji Okres przechowywania dziennika bezpieczeństwa Okres przechowywania dziennika systemu Opcje te kontrolują, jak długo plik dziennika jest przechowywany, zanim zostanie nadpisany. Dostępne wartości od 1 do 365 dni. UWAGA: Dla zapewnienia przechowywania istotnych informacji, w szczególności w przypadku wystąpienia wylomu w bezpieczeństwie systemu, dzienniki wydarzeń na stacjach roboczych powinny być okresowo gromadzone przez odpowiednie oprogramowanie zanim zostaną nadpisane.	14 dni
Metoda przechowywania dziennika aplikacji Metoda przechowywania dziennika bezpieczeństwa Metoda przechowywania dziennika systemu Opcja ta określa, w jaki sposób system postępuje z plikami dzienników, które osiągnęły już maksymalny rozmiar. Dzienniki mogą zostać nadpisane po określonej liczbie dni, gdy się zapełnia, lub będą musiały być czyszczone ręcznie. UWAGA: Zalecenie to dotyczy tylko stacji roboczych. Dzienniki serwerów powinny być czyszczone ręcznie.	Wg liczby dni

Tabela 7 Opcje Dziennika Wydarzeń

Zarządzanie dziennikami wydarzeń

Poniższa sekcja opisuje podstawy administrowania dziennikami wydarzeń Windows XP.

Zapisywanie i Czyszczenie Dzienników Kontroli

Aby zapisać i wyczyścić dzienniki:

- Wybierz **Start** → **Programy** → → → → **Narzędzia Administr.** → → → → **Przeglądarka Wydarzeń**

- q W prawej części okna Przeglądarki Wydarzeń kliknij dziennik, który ma być oczyszczony
- q Wybierz **Wyczyść Wszystkie Wydarzenia** zalecane menu **Akcja**
- q Kliknij **Tak, aby** zapisać ustawienia w pliku z osobną nazwą
- q Określ gdzie dziennik ma zostać zapisany i kliknij **Save**
- q Kliknij **Tak, aby** oczyścić dziennik
- q Powtórz powyższe kroki dla każdego dziennika

Resetowanie Ustawień Dziennika Kontroli po Zatrzymaniu Systemu

Jeśli w rezultacie przeprowadzonej kontroli system się zatrzyma, administrator musi go restartować oraz użyć edytora rejestru (regedit.exe) do zmodyfikowania następującej wartości klucza rejestru:

Hive: **HKEY_LOCAL_MACHINE**
Key: **\System\CurrentControlSet\Control\Lsa**
Name: **CrashOnAuditFail**
Type: **REG_DWORD**
Value: 1



UWAGA: Wartość ta jest ustawiana przez system operacyjny tuż przed zatrzymaniem w wyniku przeprowadzonej kontroli. Gdy wartość wynosi 2, tylko administrator może się zalogować do komputera. Wartość ta potwierdza przyczynę zatrzymania. Zresetuj wartość 1.

Ta strona celowo jest pusta

Zarządzanie Grupami Ograniczonymi za pomocą Szablonów Bezpieczeństwa

Opcja Grup Ograniczonych pozwala administratorowi na zarządzanie składem grup wrażliwych. Na przykład, jeśli grupa Administratorzy ma się składać tylko z wbudowanego konta Administratora, grupa Administratorzy może zostać dodana do Grup Ograniczonych a Administrator może zostać umieszczony w kolumnie **Administratorzy**. Ustawienie to uniemożliwi innym użytkownikom zmianę swego statusu na Administratorów, z wykorzystaniem różnorodnych narzędzi do hackowania.

Nie wszystkie grupy muszą zostać dodane do Grup Ograniczonych. Zalecane jest by tylko grupy "wrażliwe" były konfigurowane z wykorzystaniem szablonów bezpieczeństwa. Grupa nie dodana do tej opcji zachowa własną listę członków.

We wszystkich grupach objętych tą opcją, wszystkie skatalogowane grupy i/lub użytkownicy nie będący aktualnie członkami danej grupy są do niej dodawani, będący zaś członkami danej grupy a nie skatalogowani w pliku konfiguracyjnym są usuwani.

Modyfikacja Grup Ograniczonych przez przystawkę Szablonów Bezpieczeństwa

Ponieważ ustawienia w opcji Grup Ograniczonych powinny być odpowiednie dla otoczenia, ustawienia tylko jednej grupy są konfigurowane w towarzyszących plikach konfiguracji (inf). Jednakże witryna może domagać się ograniczenia członkostwa dodatkowych grup wrażliwych wewnątrz domeny.

Aby przejrzeć ustawienia grup ograniczonych w szablonie SCM kliknij dwukrotnie:

- q Szablony Bezpieczeństwa
- q Domyślny katalog pliku konfiguracji (%SystemRoot%\Security\Templates)
- q Określony plik konfiguracji
- q **Grupy ograniczone**



UWAGA: Po dokonaniu jakichkolwiek modyfikacji w pliku konfiguracyjnym upewnij się, że zmiany zostały zapisane a następnie przetestuj wprowadzone ustawienia przed zainstalowaniem ich w pracującej sieci.

by dodać Grupę Ograniczoną do listy wykonaj następujące czynności:

- q Kliknij prawym klawiszem myszy **Grupy Ograniczone**
- q Wybierz **Dodaj Grupę**
- q Kliknij przycisk **Przeglądaj**
- q Kliknij dwukrotnie każdą grupę, która ma być dodana i **OK** →→→→**OK**
- q Kliknij dwukrotnie nowo dodana grupę w prawym oknie

- q Kliknij **Dodaj**
- q Kliknij dwukrotnie każdą grupę i/lub użytkowników pragnących przynależeć do danej grupy
- q Kliknij **OK** →→→→→**OK**

Zalecane ustawienia w istniejącym szablonie stacji roboczej minimalizują liczbę członków grupy Użytkowników Pełnomocnych. Z punktu widzenia bezpieczeństwa to praktyka wskazana. Jednak środowiska używające starszych aplikacji lub pisanych na zamówienie aplikacji biznesowych mogą wymagać dodatkowych przywilejów dla użytkowników przy pracy z określonymi plikami, folderami, czy kluczami rejestru związanymi z tymi aplikacjami. Optymalnym rozwiązaniem jest identyfikowanie i implementowanie odpowiednich zezwoleń na prace z tymi plikami i kluczami zamiast dodawania użytkowników do grupy Użytkowników Pełnomocnych. Pod żadnym pozorem nie wolno dodawać użytkowników do grupy Administratorów jedynie w celu zapewnienia działania aplikacji.

Zarządzanie Usługami Systemowymi za pomocą Szablonów Bezpieczeństwa

Opcja Usług Systemowe pozwala zdefiniować tryby uruchamiania oraz listy uprawnień dostępu dla wszystkich usług systemowych. Opcje konfiguracji zawierają ustawienia rozruchu (Automatyczny, Ręczny, lub Wyłączone) dla takich usług jak usługi sieciowe, drukowania, pliku. Istnieje możliwość ustanowienia zabezpieczenia kontrolującego, którzy użytkownicy i/lub grupy są uprawnieni do uruchamiania, zapisywania, usuwania, wstrzymania, lub zatrzymania usług.

Modyfikacja usług systemowych przez przystawkę szablonów bezpieczeństwa

Ze względu na obszerność tej dziedziny, konfiguracja Usług Systemowych zależy od środowiska. Usługi nie wyświetlone w tej opcji mogą być dodane poprzez edytowanie sekcji "Ogólne Ustawienia Usług" w szablonie bezpieczeństwa. Sekcja ta wygląda następująco:

```
<service name>,stan,<sddl string specifying ACL>
```

"Stan" może przyjąć następujące wartości:

- 2 Automatycznie
- 3 Ręcznie
- 4 Wyłączone

Na przykład, aby wyłączyć usługę IISADMIN i wyłączyć dostęp do niej dla użytkowników (usuniecie wszelkich uprawnień dostępu), można użyć następującego ciągu:

```
IISADMIN,4,"D:ARS:AR"
```

Usług dodawane do tego obszaru można konfigurować tak jak usługi już domyślnie tu zamieszczone. Administrator może także użyć *załącznika konfiguracji zabezpieczeń*, aby skonfigurować specyficzne ustawienia usług. Załącznik taki składa się z biblioteki DLL, przystawki rozszerzenia oraz narzędzi instalacyjnych. Aby uzyskać więcej informacji nt. tworzenia załączników konfiguracji zabezpieczeń czytaj *Security Configuration Toolset*

<http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp>.

Aby przejrzeć ustawienia bezpieczeństwa usług w szablonie bezpieczeństwa kliknij dwukrotnie:

- q **Szablony Bezpieczeństwa**
- q Domyślny katalog pliku konfiguracji
- q (%SystemRoot%\Security\Templates)
- q Określony plik konfiguracji
- q **Usług Systemowe**

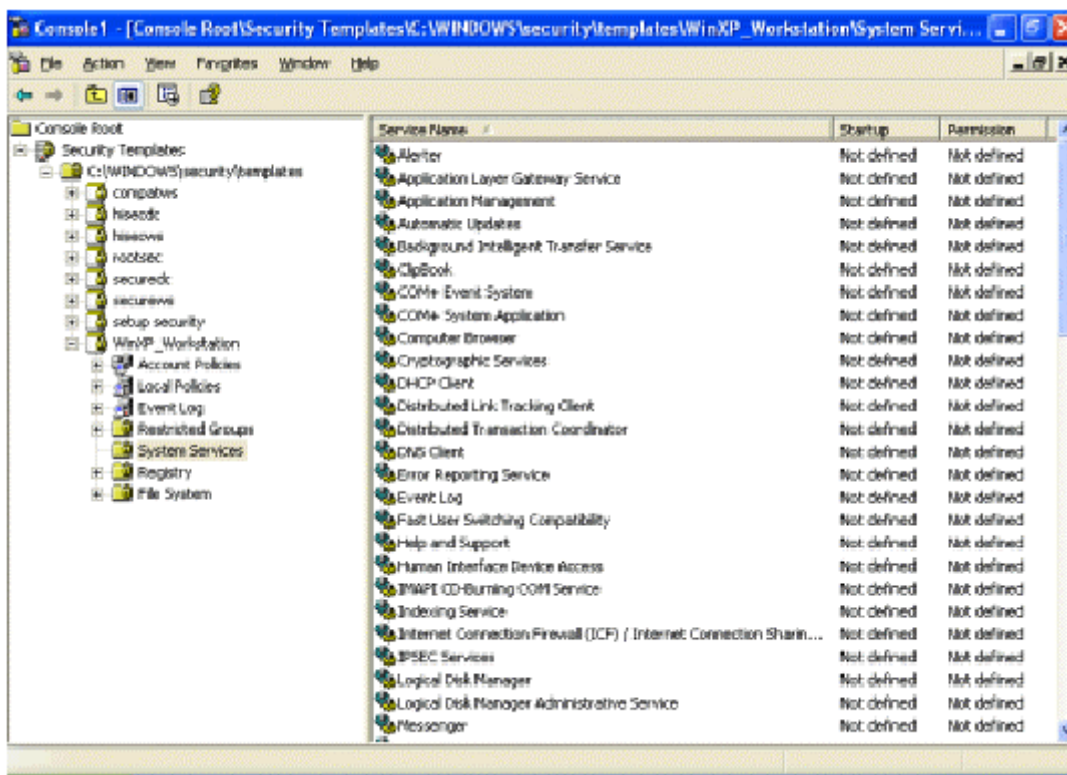


UWAGA: Po dokonaniu jakichkolwiek modyfikacji w pliku konfiguracyjnym upewnij się, że zmiany zostały zapisane a następnie przetestuj wprowadzone ustawienia przed zainstalowaniem ich w pracującej sieci.

Aby skonfigurować ustawienia usług systemowych wykonaj następujące czynności:

- q Kliknij dwukrotnie usługę, którą chcesz skonfigurować
- q Zaznacz okienko **Określ ustawienia tego algorytmu** w szablonie
- q Jeśli algorytm ten nie był wcześniej zdefiniowany, automatycznie pojawi się okno dialogowe Bezpieczeństwa. W przeciwnym razie kliknij **Edytuj Zabezpieczenia**
- q Kliknij **Dodaj** (aby dodać grupy i/lub użytkowników do listy dostępu)
- q Kliknij dwukrotnie każdą grupę i/lub użytkownika, których chcesz dodać i **OK**
- q Zaznacz zezwolenia dla tej usług dostępne dla każdego użytkownika / grupy
- q Kliknij **Usuń** (aby usunąć grupę i/lub użytkownika z listy dostępu)
- q Po zakończeniu wpisywania zezwoleń kliknij **OK**
- q W opcji **Wybierz tryb uruchamiania usług** wybierz **Automatycznie**, **Ręcznie**, lub **Wyłączona**

Ilustracja 4 pokazuje wpisy Usług Systemowych w przystawce Szablonów Bezpieczeństwa.



Ilustracja 4 Usługi systemowe

Zabezpieczenia usług systemowych

W przypadku włamania, poprzez usług można uzyskać dostęp do zasobów systemu, usług mogą paść ofiarą przepełnienia buforów oraz odmowy usług. Dlatego tak ważna jest właściwa konfiguracja usług. Ponieważ usługi są zależne od określonej aplikacji i środowiska, w tym dokumencie nie ma opisu konfiguracji żadnej z nich. Istnieją jednakże pewne wskazówki, które należy brać pod uwagę przy konfigurowaniu usług:

- q Uruchamiaj tylko potrzebne usług. Na przykład, jeśli uruchomiona jest usługa telnet albo FTP, a nie są one używane - wyłącz je.
- q Upewnij się, że tylko ograniczona ilość grup/użytkowników jest uprawniona do uruchamiania, zatrzymywania i modyfikowania usług
- q Jeśli usługa jest wyświetlona ale niepotrzebna, zmień tryb uruchamiania na Wyłączone zamiast Ręcznie. W ten sposób usługa nie zostanie ponownie uruchomiona przez nie- autoryzowanych lub złośliwych użytkowników. Jeśli usługa jest aktualnie wyłączona i ma tak pozostać zaleca się zaznaczenie opcji Wyłączona zamiast "Nie określono"
- q Jeśli edytujesz tryb uruchamiania usług, musisz również edytować listę uprawnień dostępu. Jeśli usługa jest zdecydowanie Wyłączona, jej lista uprawnień dostępu również powinna być zabezpieczona poprzez zmianę ustawień domyślnych z Pełna Kontrola dla Wszystkich na: przyznaj Administratorom oraz SYSTEMOWI pełna kontrola a Uwierzytelnionym Użytkownikom tylko uprawnienia do odczytu.

- Uruchamiaj usługę tylko z najbardziej niezbędnymi uprawnieniami. Na przykład, nie uruchamiaj usług jako administrator domeny, jeśli wystarczają uprawnienia użytkownika.

Modyfikacja Ustawień Zabezpieczeń Rejestru za pomocą Szablonów Bezpieczeństwa

Zestaw narzędzi konfiguracji zabezpieczeń może zostać użyty do konfiguracji ustawień dostępu (DACLs) dla kluczy rejestru. W celu zaimplementowania właściwego zabezpieczenia w środowisku Windows XP, uprawnienia niektórych kluczy rejestru powinny być zmienione. Zalecane zmiany mogą zostać dokonane ręcznie z wykorzystaniem regedit.exe; metoda ta jest jednak bardziej czasochłonna i wprowadza większe ryzyko błędu.



OSTRZEZENIE: Domyślne ustawienia zabezpieczeń na niektórych elementach rejestru pozwalają na prace z aplikacjami przy jednoczesnym zachowaniu standardowego poziomu zabezpieczeń. Ustawienie wysokiego poziomu zabezpieczeń wymusza modyfikację pewnych uprawnień dostępu. Należy zachować ostrożność, ponieważ wykorzystywane przez użytkowników aplikacje często wymagają dostępu do poszczególnych kluczy rejestru w imieniu użytkownika. Należy uważnie przeczytać poniższe wskazówki, ponieważ nadmierne, niepotrzebne zmiany w rejestrze mogą sprawić, że nie będzie można pracować z systemem a nawet, że nie będzie można systemu odzyskać.

Model dziedziczenia

Model "dziedziczenia" w Windows XP, automatycznie przenosi uprawnienia z obiektów pierwotnych na dziedziczone. W edytorze DACL widoczne jest zaznaczenie w okienku **Dziedziczenie uprawnień dla obiektów pochodnych z obiektów pierwotnych**. Obok uprawnień dziedziczonych, także inne uprawnienia mogą zostać wyraźnie zdefiniowane dla obiektów pochodnych.

Jeśli okienko nie jest zaznaczone, DACLs zdefiniowane dla danego obiektu dotyczą tylko tego obiektu i jego pochodnych. Żadne uprawnienia nie są dziedziczone z obiektu pierwotnego.

Uprawnienia rejestru

Aby ręcznie sprawdzić uprawnienia dla danego klucza rejestru:

- q Uruchom regedit.exe
- q Kliknij prawym przyciskiem na określony klucz
- q Wybierz **Uprawnienia...** z menu

W oknie dialogowym uprawnień widnieją tylko uprawnienia **Pełnej Kontroli**, **Odczytu** i **Specjalne**. Bardziej szczegółowe ustawienia uprawnień dostępne są po naciśnięciu prawym przyciskiem na **Zaawansowane**. **Tabela 8** pokazuje listę szczegółowych uprawnień rejestru. **Tabela 9**

pokazuje, które ze szczególnych uprawnień należy wybrać w celu osiągnięcia określonego, wysokiego poziomu zabezpieczeń.



UWAGA: Jeśli uprawnienie nie jest oznaczone Odczyt albo Pełna Kontrola, uprawnienie opatrzone jest adnotacją Specjalne w oknie Zaawansowane ustawienia zabezpieczeń

Upewnienia Specjalne	Opis
Zapytanie o Wartość	Zezwala na wysyłanie zapytań do rejestru o określoną wartość
Ustaw Wartość	Zezwala na tworzenie nowych wartości dla klucza oraz nadpisywanie starych
Utwórz Klucz Podrzędny	Zezwala na tworzenie kluczy podrzędnych
Sporządź Wykaz Wartości	Zezwala na oglądanie kluczy podrzędnych w danym kluczu rejestru
Powiadom	Pozwala na zarejestrowanie funkcji wywołania zwrotnego, która jest uruchamiana, gdy wartość się zmienia.
Utwórz Łącze	Pozwala tworzyć łącza do określonych kluczy
Usuń	Pozwala na usuwanie określonej wartości lub klucza
Zapisz DAC	Zezwala na modyfikacje kontroli dostępu do klucza
Zapisz Właściciela	Zezwala użytkownikowi na przejęcie klucza na własność
Odczytaj Kontrole	Zezwala na odczytanie listy kontroli dostępu do klucza.

Specjalne Upewnienia	Pełna Kontrola	Odczyt	Zapis	Usuwanie
Zapytanie o Wartość	x	x		
Ustaw Wartość	x		x	
Utwórz Klucz Podrzędny	x		x	
Sporządź Wykaz Wartości	x	x		
Powiadom	x	x		
Utwórz Łącze	x			
Usuń	x			x
Zapisz DAC	x			
Zapisz Właściciela	x			
Odczytaj Kontrole	x	x	x	

Czynne Uprawnienia

Określenie uprawnień udzielonych i odmawianych poszczególnym grupom, pokazujące, które uprawnienia rejestru dotyczą określonego użytkownika lub grupy mogą być mylące. Windows XP pozwala w łatwy sposób przejrzeć, które uprawnienia (dla danego obiektu) są faktycznie udzielane określonym użytkownikom lub grupom. Aby przejrzeć “czynne zezwolenia”, wykonaj następujące czynności:

- q W edytorze rejestru (np. regedit), kliknij prawym przyciskiem na klucz rejestru
- q Wybierz **Uprawnienia** z pokazującego się menu
- q Kliknij **Zaawansowane**
- q Kliknij na tabelkę **Rzeczywiste Zezwolenia**
- q W sekcji **Nazwa grupy lub użytkownika** kliknij **Wybierz**
- q W oknie **Wprowadź nazwę obiektu do wybrania**, wprowadź nazwę użytkownika lub grupy
- q Kliknij **OK**. Te uprawnienia, które dotyczą określonego użytkownika lub grupy zostaną zaznaczone.

Modyfikacja ustawień rejestru

W szablonie bezpieczeństwa, uprawnienia rejestru można dostosować poprzez modyfikacje istniejących kluczy rejestru w pliku inf, lub przez dodanie własnych kluczy rejestru oraz uprawnień.

Aby przejrzeć ustawienia rejestru w szablonie bezpieczeństwa wybierz:

- q **Szablony Bezpieczeństwa**
- q Domyślny katalog pliku (%SystemRoot%\Security\Templates)
- q Określony plik konfiguracji
- q **Rejestr**

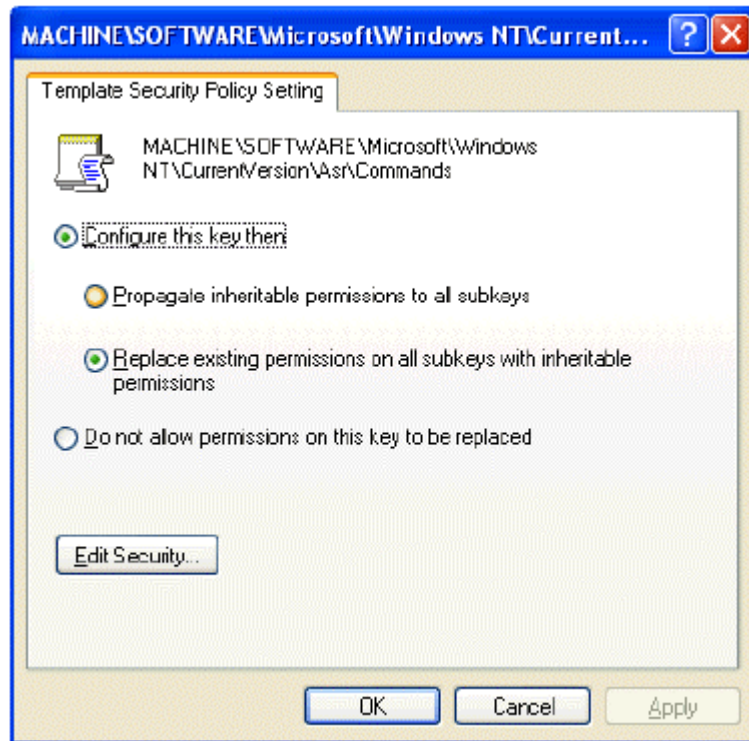
Modyfikacja uprawnień dla klucza rejestru

Aby zmodyfikować istniejące już w szablonie ustawienia zabezpieczeń dla określonego klucza rejestru:

- q W prawej ramce kliknij dwukrotnie klucz, który chcesz zmienić
- q Upewnij się, że zaznaczono przycisk **Konfiguruj ten klucz.....** . Opcja ta zawiera w sobie dwie opcje pokazane na **Rysunku 5**:

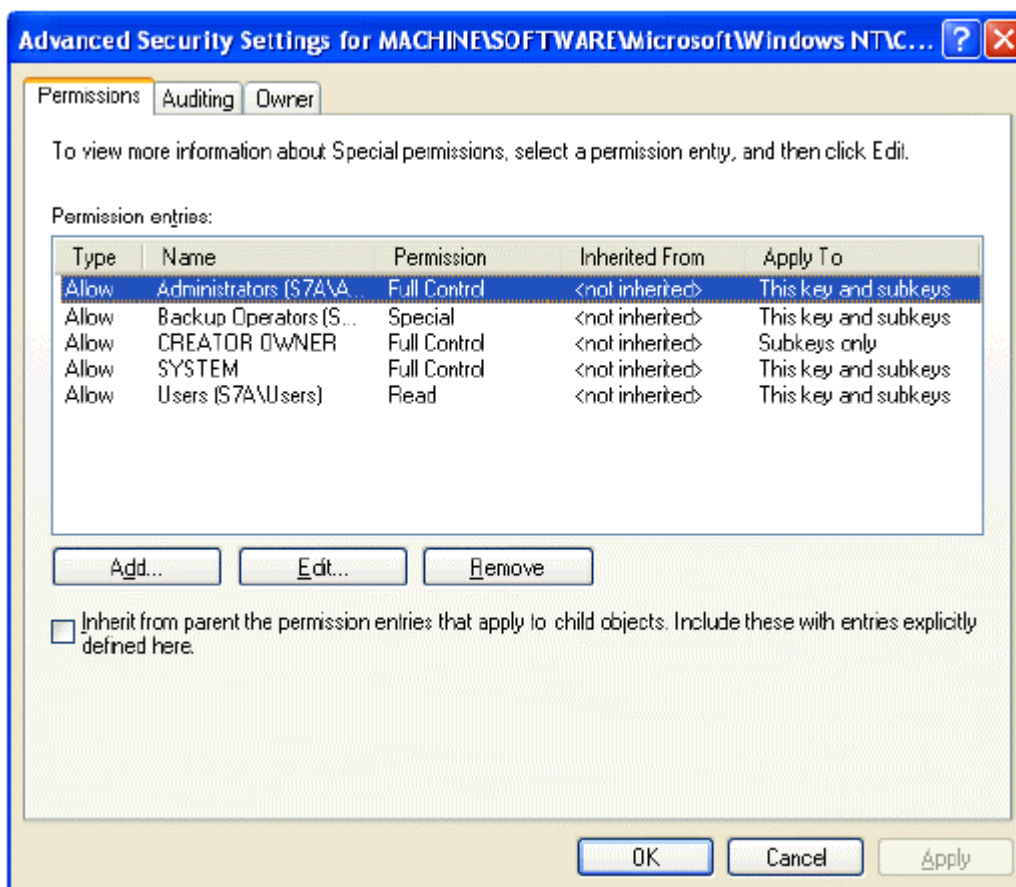
§ **Rozszerzaj dziedziczne uprawnienia na klucze podrzędne** – wszystkie klucze podrzędne już dziedziczące uprawnienia z modyfikowanego klucza automatycznie odziedziczą nowe uprawnienia. Opcja ta nie znajdzie zastosowania dla kluczy, które nie mają w DACL uaktywnionego dziedziczenia z obiektów pierwotnych.

§ **Zamień istniejące uprawnienia we wszystkich kluczach dziedziczących uprawnienia** – uprawnienia wszystkich kluczy podrzędnych będą zamienione na nowe klucze będą dziedziczyć z modyfikowanego klucza bez względu na wcześniejsze dziedziczenia ani na ograniczenia dziedziczenia kluczy podrzędnych.



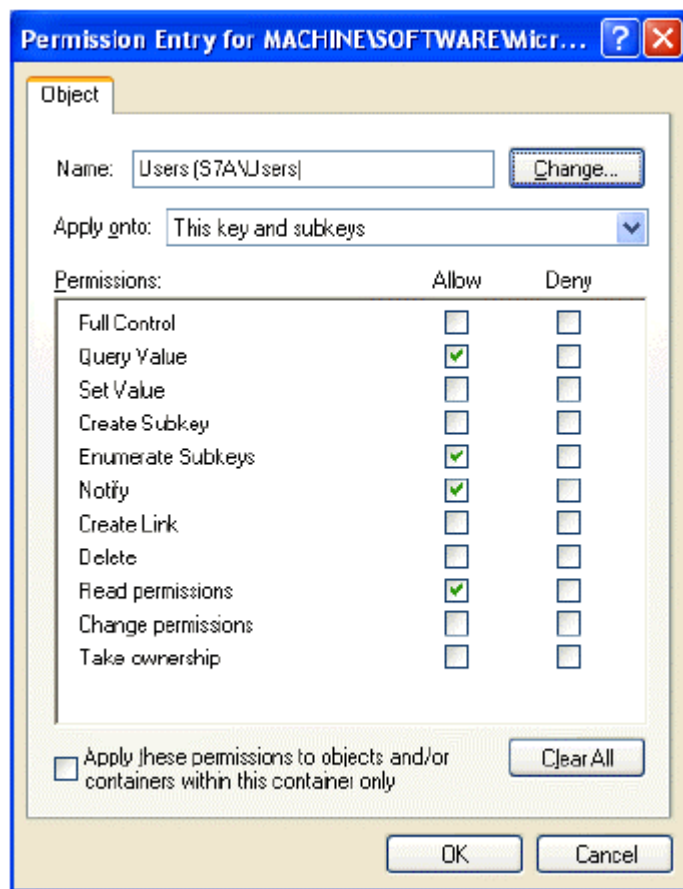
Rysunek 5 Opcje konfiguracji uprawnień rejestru

- q Kliknij **Edytuj zabezpieczenia**
- q Kliknij **Zaawansowane**. Rysunek 6 pokazuje okno **Zaawansowanych Ustawień Zabezpieczeń**



Rysunek 6 Zaawansowane ustawienia zabezpieczeń

- q Jeśli uprawnienia NIE MAJA być dziedziczone z klucza pierwotnego, upewnij się, że okno **Dziedziczenie uprawnień dotyczących obiektów pochodnych z obiektów pierwotnych** jest puste
- q Modyfikuj użytkowników i grupy w celu zastosowania zalecanych uprawnień, klikając przyciski **Dodaj** lub **Usuń**
- q Kliknij użytkownika i/lub grupę
- q Kliknij **Edytuj**. Wyświetli się okno dialogowe **Wpis Uprawnienia**, jak to pokazuje **Rysunek 7**
- q W menu **Zatwierdź** wybierz odpowiednią konfigurację. Dostępne wartości to: **Tylko dla tego klucza**, **Ten klucz i klucze podrzędne** oraz **Tylko klucze podrzędne**
- q Na karcie **Uprawnienia** wybierz zadane uprawnienia. O uprawnieniach rejestru czytaj w sekcji poprzedniej
- q Kliknij **OK** →→→→**OK** →→→→**OK** →→→→**OK**, aby wyjść



Rysunek 7 Okno Wpisów Uprawnień dla kluczy rejestru

Dodawanie kluczy rejestru do konfiguracji zabezpieczeń

Aby dodać klucz do konfiguracji zabezpieczeń:

- q Kliknij prawym przyciskiem **Rejestr**
- q Wybierz **Dodaj Klucz** z dostępnego menu
- q Wybierz klucz, który ma być dodany
- q Kliknij **OK**
- q Wyświetli się okno dialogowe **Baza Danych Zabezpieczeń**. Okno to pokazuje ustawienia, które mają zostać zapisane w bazie danych konfiguracji zabezpieczeń dla tego klucza.
- q Kliknij **Zaawansowane** i zmień uprawnienia stosując się do wskazówek zawartych w sekcji **Modyfikacja uprawnień dla klucza rejestru**
- q Po zamknięciu okien **Zaawansowane** i **Baza Danych Zabezpieczeń**, wybierz przycisk **Rozszerzaj dziedziczne uprawnienia na klucze podrzędne** Lub **Zamień istniejące uprawnienia we wszystkich kluczach dziedziczących**
- q Kliknij **OK**.

Usuwanie kluczy rejestru z konfiguracji zabezpieczeń

W niektórych przypadkach zalecane jest, aby określony klucze rejestru zachowały istniejące ustawienia zabezpieczeń. W celu wykluczenia rozszerzania uprawnień przez klucze pierwotne na te klucze, obiekt taki można usunąć z konfiguracji.

Aby usunąć obiekt:

- q W prawym oknie **Rejestru**, kliknij dwukrotnie na klucz do usunięcia
- q Kliknij przycisk **Nie zezwalaj na zastępowanie uprawnień tego klucza**.
- q Kliknij **OK**

Zalecane uprawnienia klucza rejestru

Zakłada się, że Klucze niewyszczególnione poniżej w **Tabeli 10** dziedziczą uprawnienia swoich kluczy pierwotnych, jeśli w swoich DACL mają zaznaczona opcje **Dziedziczenie uprawnień dotyczących obiektów pochodnych z obiektów pierwotnych**. Klucze z zaznaczona opcja **Nie zezwalaj na zastępowanie uprawnień tego klucza** są w sposób wyraźny wykluczone z konfiguracji zabezpieczeń i zachowują swoje oryginalne uprawnienia.

Użyte w tabeli określenie “Rozszerzaj” sygnalizuje, że należy zaznaczyć **Rozszerzaj dziedziczne uprawnienia na klucze podrzędne, podczas gdy** określenie “Zastąp” wskazuje, że należy zaznaczyć **Zamień istniejące uprawnienia we wszystkich kluczach dziedziczących**. “Ignoruj” oznacza, że klucz jest wyłączony z konfiguracji.



UWAGA: Wiele z wymienionych poniżej ustawień zabezpieczeń bazuje na domyślnych zabezpieczeniach Windows XP zawartych w szablonie “setup security.inf”. Z uprawnień domyślnych Usunęliśmy grupy Użytkownicy Pełnomocni oraz Wszyscy i zmodyfikowaliśmy niektóre dalsze uprawnienia rejestru

W tej sekcji szablonów bezpieczeństwa wykorzystano następujące oznaczenia umowne:

- q CLASSES_ROOT oznacza ośrodek HKEY_CLASSES_ROOT
- q MACHINE oznacza ośrodek HKEY_LOCAL_MACHINE
- q USERS oznacza ośrodek HKEY_USERS

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
CLASSES_ROOT\ Inaczej MACHINE\SOFTWARE\Classes. Zawiera skojarzenia plików i COM Common Object Model) i ich połączeń	Administratorzy Właściciel Twórcza SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Zastęp
\MACHINE\SOFTWARE Zawiera informacje o oprogramowaniu zainstalowanym na lokalnym systemie.	Administratorzy Właściciel Twórcza SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Zastęp
\MACHINE\SOFTWARE\Microsoft\Cryptography\Calais	Administratorzy Właściciel Twórcza USŁUGA LOKALNA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Zapytanie o Wartość Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu Pełna Kontrola Odczyt	Zastęp
MACHINE\SOFTWARE\Microsoft\MSDTC	Administratorzy USŁUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, uprawnienia Odczytu Pełna Kontrola Odczyt	Rozszerzaj
\MACHINE\SOFTWARE\Microsoft\MSDTC\Security\XAKey	Administratorzy USŁUGA SIECIOWA SYSTEM	Pełna Kontrola Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, uprawnienia Odczytu Pełna Kontrola	Zastęp
\MACHINE\SOFTWARE\Microsoft\NetDDE Ustawienia Sieciowej Dynamicznej Wymiany Danych, protokołu pozwalającego aplikacjom na wymianę danych	Administratorzy Właściciel Twórcza SYSTEM	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola	Zastęp
\MACHINE\SOFTWARE\Microsoft\UPnP Device Host	Administratorzy Właściciel Twórcza USŁUGA LOKALNA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Pełna Kontrola Odczyt	Zastęp
\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Asr\Commands Komendy Automatycznego Odzyskiwania Serwera. UWAGA: Jeśli używamy grupy Operatorzy zastępczy, grupie tej należy udzielić następujących uprawnień: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Sporządź Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu.	Administratorzy Właściciel Twórcza SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Zastęp

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
\\MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Perflib Parametry dla Biblioteki Wydajności, która zbiera informacje dla Monitora Wydajności. Zawiera klucz kodu języka dla każdego języka mówionego skonfigurowanego w systemie Windows XP. Na przykład, klucz podrzędny oznaczony 009 dane i opisy dla kodu języka Angielski (Stany Zjednoczone).	Administratorzy Twórca Właściciel INTERAKTYWNE USLUGA SIECIOWA	SYSTEM Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Odczyt Odczyt Pełna Kontrola	Zastęp
\\MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SeCedit Zawiera rozmieszczenie plików i wartości rejestru dostępne poprzez Edytor Konfiguracji Zabezpieczeń.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Group Policy Zawiera dane dla ustawień Strategii Grupowych które konfiguruja komponenty Strategii Grupowych Windows XP. Zawiera klucze podrzędne reprezentujące każde z rozszerzeń po stronie klienta wykorzystywane do tworzenia ustawień Strategii Grupowych.	Administratorzy Użytkownicy Uwierzytelnieni SYSTEM	Pełna Kontrola Odczyt Pełna Kontrola	Rozszerzaj
\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Installer Zawiera informacje o konfiguracji dla instalatora Windows	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies Gromadzi wpisy w rejestrze zarządzane przez Strategie Grupowa. Zarządza wpisami dla następujących kluczy podrzędnych: HKLM\\SOFTWARE\\Policies HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies HKCU\\SOFTWARE\\Policies HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies	Administratorzy Użytkownicy Uwierzytelnieni SYSTEM	Pełna Kontrola Odczyt Pełna Kontrola	Rozszerzaj
\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Ratings	Administratorzy Użytkownicy	Pełna Kontrola Odczyt	Zastęp
\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Telephony	Administratorzy Twórca Właściciel USLUGA LOKALNA USLUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Zastęp

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
\\MACHINE\SYSTEM Gromadzi wartości dla aktualnego zestawu startowego lub zestawów startowych poprzednio używanych do uruchomienia Windows XP.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Zastęp
\\MACHINE\SYSTEM\clone \\MACHINE\SYSTEM\controlsetXXX (XXX reprezentuje numer zestawu kontrolnego 001- 010) Zawiera zestaw kontrolny, który może być użyty do uruchomienia Windows XP.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\SYSTEM\CurrentControlSet\Control\Class UWAGA: Wpis ten jest wyraźnie wymieniony w pliku szablonu, ponieważ zawiera klucze podrzędne z wieloma różnymi uprawnieniami. Cecha "Rozszerzaj" wpłynie tylko na te klucze podrzędne, które dziedziczą uprawnienia z tego klucza podrzędnego pozostawiając te, które nie dziedziczą bez zmian.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\SYSTEM\CurrentControlSet\Control\Network UWAGA: Jeśli wykorzystujemy grupę Operatorów Konfiguracji Sieci przyznaj tej grupie następujące uprawnienia: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu.	Administratorzy USŁUGA LOKALNA USŁUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg Uprawnienia zabezpieczeń zamieszczone w tym kluczu określają, którzy użytkownicy lub grupy mogą połączyć się z systemem w celu zdalnego dostępu do rejestru. Jeśli klucz nie istnieje, każdy może się zdalnie połączyć z rejestrem. Zaleca się, aby tylko administratorzy mieli zdalny dostęp do rejestru. UWAGA: Jeśli używamy grupy Operatorów Zastępczych, przyznaj tej grupie następujące uprawnienia (tylko ten klucz).	Administratorzy USŁUGA LOKALNA	Pełna Kontrola Odczyt	Zastęp

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
\\MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Wmi\\Security Ustawienia zabezpieczeń dla Narzędzi Zarządzania Windows (WMI). WMI to implementacja Microsoftu Web-Based Enterprise Management (WBEM)	Administratorzy Administratorzy Twórca Właściciel SYSTEM	Odczyt Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Enum Zawiera dane konfiguracji dla urządzeń zainstalowanych w systemie. Zmiana uprawnień tego klucza może spowodować uszkodzenia funkcji Plug and Play w Windows XP.	Ignoruj		Ignoruj
\\MACHINE\\SYSTEM\\CurrentControlSet\\Hardware Profiles Zawiera systemowe profile urządzeń (zmiany wstępnej konfiguracji urządzeń gromadzonej w kluczach oprogramowania i systemu).	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\AppMgmt\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\ClipSrv\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\CryptSvc\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\DNSCache UWAGA: Jeśli używamy Grupy Operatorów Konfiguracji Sieci, przyznaj tej grupie następujące uprawnienia: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu.	Administratorzy USŁUGA LOKALNA USŁUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Ersvc\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Eventlog\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\IRENUM\\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
\\MACHINE\SYSTEM\CurrentControlSet\Services\Netbt UWAGA: Jeśli używamy Grupy Operatorów Konfiguracji Sieci, przyznaj tej grupie następujące uprawnienia: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu	Administratorzy USLUGA LOKALNA USLUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\SYSTEM\CurrentControlSet\Services\Netdde\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\Netddedsm\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess UWAGA: Jeśli używasz Grupy Operatorów Konfiguracji Sieci, przyznaj tej grupie następujące uprawnienia: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości Powiadom, Usuń, uprawnienia Odczytu	Administratorzy USLUGA LOKALNA USLUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Rozszerzaj
\\MACHINE\SYSTEM\CurrentControlSet\Services\Rpsss\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\Sams\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\Scarddrv\Security			
\\MACHINE\SYSTEM\CurrentControlSet\Services\Scardsvr\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers Istnieje tylko, gdy usługa SNMP została uruchomiona w systemie. Określa, którzy użytkownicy mogą gromadzić informacje SNMP.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\Stisvc\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities Istnieje tylko, gdy usługa SNMP została uruchomiona w systemie. Ogranicza możliwość gromadzenia informacji SNMP dla zwykłych użytkowników.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp

Klucz Rejestru	Grupy Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
\MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog\Log Queries	Administratorzy Twórca Właściciel USLUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Pełna Kontrola Odczyt	Zastęp
\MACHINE\SYSTEM\CurrentControlSet\Services\Tapisrv\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip UWAGA: Jeśli używamy Grupy Operatorów Konfiguracji Sieci, przyznaj tej grupie następujące uprawnienia: Zapytanie o Wartość, Ustaw Wartość, Utwórz Klucz Podrzędny, Wykaz Wartości, Powiadom, Usuń, uprawnienia Odczytu	Administratorzy USLUGA LOKALNA USLUGA SIECIOWA SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola Pełna Kontrola Odczyt	Rozszerzaj
\MACHINE\SYSTEM\CurrentControlSet\Services\W32time\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
\MACHINE\SYSTEM\CurrentControlSet\Services\Wmi\Security	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastęp
USERS\DEFAULT Profil wykorzystywany do generowania nowych profili, gdy użytkownicy po raz pierwszy się logują. Jest również wykorzystywane, gdy wyświetlana jest informacja Windows XP CTRL+ALT+DEL.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola Odczyt	Zastęp
USERS\DEFAULT\Software\Microsoft\NetDDE Ustawienia Sieciowej Dynamicznej Wymiany Danych, protokołu pozwalającego aplikacjom na wymianę danych.	Administratorzy Twórca Właściciel SYSTEM	Pełna Kontrola Pełna Kontrola (Tylko klucze podrzędne) Pełna Kontrola	Zastęp
USERS\DEFAULT\Software\Microsoft\SystemCertificates\Root\ProtectedRoots	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt	Zastęp

Tabela 10 Rekomendowane prawa dostępu do rejestru

Ta strona celowo jest pusta

Modyfikacja Zabezpieczeń Systemu Plików za pomocą Szablonów Bezpieczeństwa

System Plików NT (NTFS) zapewnia należyłą ochronę istotnych informacji. NTFS razem z systemem kont użytkowników Windows przyznają dostęp do plików tylko uwierzytelnionym użytkownikom. **Aby wdrożyć wysoki poziom bezpieczeństwa, zawsze formatuj partycje plików Windows XP w systemie NTFS.**

Zabezpieczenia oferowane przez NTFS opiera się na kontroli systemu, która jest sprawowana przez system Windows XP. Tak długo, jak działa Windows XP, uprawnienia NTFS oraz kontrola dostępu użytkowników uniemożliwiają nieautoryzowanym użytkownikom dostęp do plików, zarówno lokalnie jak i poprzez sieć.

NTFS pozwala różnicować poziom uprawnień dostępu w zależności od użytkownika, lub ich grupy. Występują powiązania między uprawnieniami dostępu do plików a pojęciem “dziedziczenia.” Nowo utworzone foldery lub pliki domyślnie dziedziczą uprawnienia dostępu z folderowi pierwotnych. W poprzednim rozdziale dotyczącym rejestru znajdziesz więcej informacji o dziedziczeniu w Windows XP.

Konwersja na NTFS

Wolumen można w każdej chwili przekonwertować na NTFS używając programu Convert.exe (%SystemRoot%\system32\convert.exe). Komenda convert musi być egzekwowana z okna dialogowego komend, przy wykorzystaniu konta administratora.

Nowością w Windows XP jest to, że komenda convert.exe automatycznie stosuje domyślne uprawnienia NTFS dla danego wolumenu. W wcześniejszych wersjach Windows NT 3.x, 4.0 oraz 2000, konwersja wolumenu na NTFS przyznawała pełny dostęp do całego wolumenu grupie Wszyscy.

Aby konwertować napęd na NTFS wykonaj następujące czynności:

- q Wybierz **Start** →→→→**Uruchom** →→→→**cmd.exe**, aby otworzyć okno dialogowe komend
- q W oknie komend wpisz:
`convert wolumen /FS:NTFS [/V]`



Informacja: Wpisz literę dysku partycji, która ma być konwertowana w miejsce słowa *wolumen* (np. C:)



UWAGA: Parametr /v jest opcja i uruchamia program w trybie werbose

- q Restartuj system

Uprawnienia plików i folderów

Aby ręcznie wyświetlić parametry danego pliku lub folderu:

- q W Eksploratorze Windows kliknij prawym przyciskiem plik lub folder
- q Wybierz **Właściwości** z pojawiającego się menu
- q Wybierz zakładkę **Zabezpieczenia**

q Kliknij **Zaawansowane** aby zobaczyć szczegółowe informacje o uprawnieniach

Szczegółowość uprawnień plików

Uprawnienia plików można ustawić z większą szczegółowością niż pokazana w oknie **Uprawnienia** po naciśnięciu przycisku **Zaawansowane**. **Tabela 11** pokazuje listę szczegółowych uprawnień plików. **Tabela 12** oraz **Tabela 13** - Opcje Uprawnień Plików pokazuje, które ze szczegółowych uprawnień wybrać aby osiągnąć wymagany wysoki poziom uprawnień plików i folderów

Specjalne Uprawnienia	Opis
Przechodzenie przez folder/Wykonywanie Pliku	Przechodzenie przez folder pozwala użytkownikom na przechodzenie przez foldery lub pliki, nawet, gdy użytkownik nie ma uprawnień do danego folderu (dotyczy tylko folderów). Uprawnienie to działa tylko wtedy, gdy grupie lub użytkownikowi nie udzielono uprawnienia Pomiń Sprawdzenie Przechodzenia .
Wyświetlanie zawartości folderu/Odczyt danych	Wyświetl Zawartość zezwala na wyświetlanie nazw plików i podfolderów w obrębie danego folderu (dotyczy tylko folderów). Odczyt Danych zezwala na wyświetlanie danych w plikach (dotyczy tylko plików)
Odczyt atrybutów	Zezwala na wyświetlanie atrybutów pliku lub folderu, takich jak tylko do odczytu lub ukryty(definiowanych przez system)
Odczyt atrybutów rozszerzonych	Zezwala na odczyt rozszerzonych atrybutów pliku. Atrybuty rozszerzone są definiowane przez programy i mogą się różnić w zależności od programu.
Tworzenie plików/Zapis danych	Tworzenie plików/Zapis danych Tworzenie plików pozwala tworzyć pliki w obrębie folderu (dotyczy tylko folderów). Zapis Danych pozwala wprowadzać zmiany w pliku i nadpisywać pliki (dotyczy tylko plików).
Tworzenie folderów/Dołączanie danych	Tworzenie folderów pozwala tworzyć foldery w obrębie folderu (dotyczy tylko folderów). Dołączanie danych zezwala na tworzenie zmian na końcu pliku (dotyczy tylko plików).
Zapis atrybutów	Zapis atrybutów Zezwala na zmianę atrybutów definiowanych przez NTFS (np., "Tylko do odczytu" lub "Ukryty").
Zapis atrybutów rozszerzonych	Zezwala na zmianę atrybutów rozszerzonych definiowanych przez programy.
Usuwanie podfolderów i plików	Zezwala na usuwanie podfolderów i plików niezależnie od tego czy uprawnienie Usuwanie zostało udzielone na dany podfolder lub plik.
Usuwanie	Zezwala na usuwanie plików lub folderów.
Odczyt uprawnień	Zezwala na przeglądanie uprawnień do pliku lub folderu.
Zmiana uprawnień	Pozwala na zmianę uprawnień do pliku lub folderu.
Przejęcie na własność	Pozwala przejść na własność plik lub folder.

Uprawnienia Folderów:

Specjale Uprawnienia	Pełna Kontrola	Zmiana	Odczyt & Wykonywanie	Wyświetl Zawartość Foldera	Odczyt	Zapis
Przechodzenie przez folder/Wykonywanie Pliku	X	X	X			
Wyświetlanie zawartości folderu/Odczyt danych	X	X	X	X		
Odczyt atrybutów	X	X	X	X		
Odczyt atrybutów rozszerzonych	X	X	X	X		
Tworzenie plików/Zapis danych	X	X				X
Tworzenie folderów/Dołączanie danych	X	X				X
Zapis atrybutów	X	X				X
Zapis atrybutów rozszerzonych	X	X				X
Usuwanie podfolderów i plików						
Usuwanie	X	X				
Odczyt uprawnień	X	X	X	X	X	X
Zmiana uprawnień	x					
Przejęcie na własność	x					



UWAGA: Uprawnienie Wyświetl Zawartość Folderu jest dziedziczone przez foldery, ale nie przez pliki, podczas gdy Odczyt i Wykonywanie są dziedziczone zarówno przez pliki jak i foldery.

Uprawnienia Plików:

Specjale Uprawnienia	Pełna Kontrola	Zmiana	Odczyt & Wykonywanie	Wyświetl Zawartość Foldera	Odczyt	Zapis
Przechodzenie przez folder/Wykonywanie Pliku	X	X	X			
Wyświetlanie zawartości folderu/Odczyt danych	X	X	X	X		
Odczyt atrybutów	X	X	X	X		
Odczyt atrybutów rozszerzonych	X	X	X	X		
Tworzenie plików/Zapis danych	X	X				X
Tworzenie folderów/Dołączanie danych	X	X				X
Zapis atrybutów	X	X				X
Zapis atrybutów rozszerzonych	X	X				X
Usuwanie podfolderów i plików						
Usuwanie	X	X				
Odczyt uprawnień	X	X	X	X	X	X
Zmiana uprawnień	x					
Przejęcie na własność	x					

Tabela 13 Opcje Uprawnień Plików

Rzeczywiste uprawnienia

Występowanie wielu grup użytkowników utrudnia zdeterminowanie, której grupie lub użytkownikowi przyznać lub odmówić dane uprawnienia. Windows XP pozwala w łatwy sposób zobaczyć, które uprawnienia do danego obiektu rzeczywiście są przydzielane danym użytkownikom lub grupie. Aby obejrzeć te “rzeczywiste uprawnienia” wykonaj następujące czynności:

- q W eksploratorze windows prawym przyciskiem kliknij plik lub folder
- q Wybierz **Właściwości** z pojawiającego się menu
- q Kliknij zakładkę **Zabezpieczenia**
- q Kliknij **Zaawansowane**
- q Kliknij zakładkę **Rzeczywiste uprawnienia**
- q W sekcji **Nazwa użytkownika lub grupy** kliknij przycisk **Wybierz**
- q Wpisz nazwę użytkownika lub grupy w oknie **Nazwa wybranego obiektu**
- q Kliknij **OK**. Uprawnienia odnoszące się do danego użytkownika lub grupy zostaną zaznaczone.

Modyfikacja ustawień systemu plików przez przystawkę Szablonów Bezpieczeństwa

Zalecane zmiany systemu plików i folderów wymienione są w **Tabeli 14**.

Niezbędnych zmian można dokonać na jeden z dwóch sposobów. Pierwsza metoda polega na wykorzystaniu Menadżera Konfiguracji Zabezpieczeń do wprowadzania uprawnień dla plików i folderów. Metoda alternatywna i bardziej czasochłonna polega na ręcznym zmienianiu uprawnień dla każdego pliku i folderu osobno.

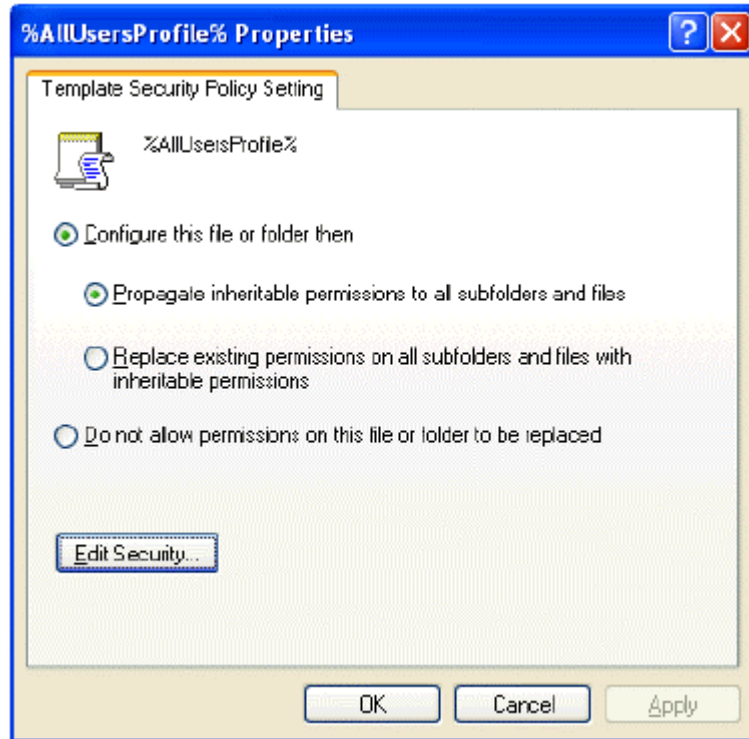
Aby obejrzeć ustawienia systemu plików w szablonie bezpieczeństwa wybierz w MMC:

- Szablony bezpieczeństwa
- Domyślny katalog pliku (%SystemRoot%\Security\Templates)
- Określony plik konfiguracji
- System Plików

Modyfikacja uprawnień do pliku lub folderu

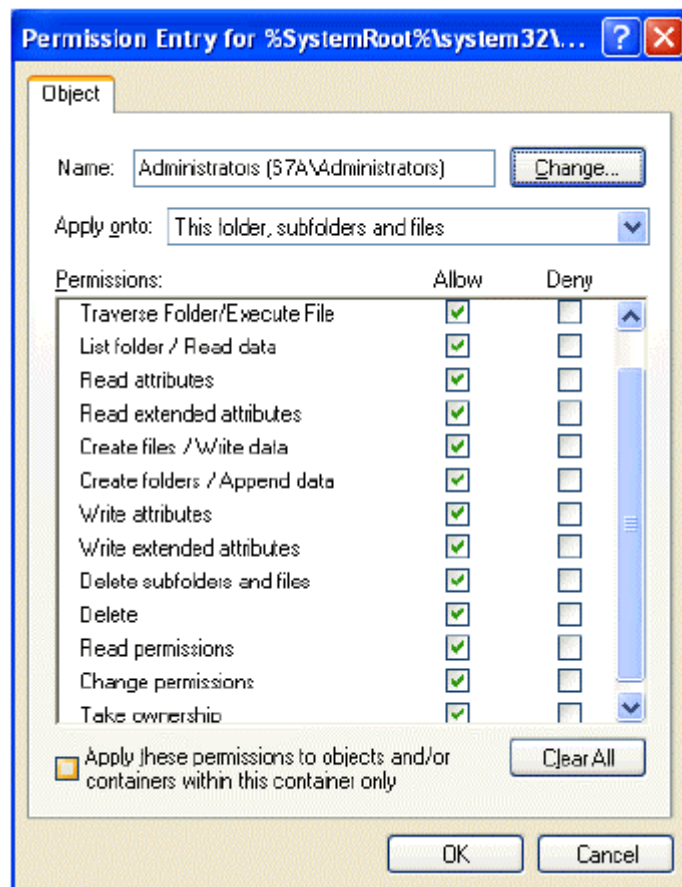
Aby zmodyfikować ustawienia zabezpieczeń danego pliku lub foldera uprzednio określone w szablonie bezpieczeństwa:

- W prawym oknie dwukrotnie kliknij dany plik lub folder
- Upewnij się, że przycisk **Konfiguruj ten plik lub folder** następnie jest wybrany. Ta opcja zawiera w sobie dwie inne, jak pokazuje **Rysunek 8**:
 - **Rozszerzaj uprawnienia dziedziczne na wszystkie podfoldery i pliki** – wszystkie podfoldery i pliki, które domyślnie dziedziczą uprawnienia z folderów, które są konfigurowane, odziedzicza nowe uprawnienia. Opcja ta nie wpłynie na podfoldery i pliki z wyłączoną opcją **Dziedziczenia z obiektów pierwotnych uprawnień dotyczących obiektów pochodnych** (w DACL).
 - **Zastąp we wszystkich plikach i folderach istniejące uprawnienia na uprawnienia dziedziczne – Uprawnienia wszystkich podfolderów i plików zostaną ustawione na nowe uprawnienia**, subfoldery i pliki będą dziedziczyć z konfigurowanego klucza niezależnie od tego, czy dziedziczenie przez te pliki zostało uaktywnione, czy też nie. Nie będzie to miało wpływu na foldery z zaznaczoną w szablonie opcją "Nie zezwalaj na zmianę uprawnień do tego pliku lub foldera"



Rysunek 8 Opcje konfiguracji uprawnień pliku

- q Kliknij **Edytuj zabezpieczenia**
- q Kliknij **Zaawansowane**
- q Jeśli zezwolenia z klucza pierwotnego NIE MAJA być dziedziczone, upewnij się, że okienko **Dziedziczenie z obiektów pierwotnych uprawnień dotyczących obiektów pochodnych** pozostanie niezaznaczone
- q Aby zastosować zalecane uprawnienia zmodyfikuj grupy i użytkowników klikając przyciski **Dodaj** lub **Usuń**
- q Kliknij użytkownika lub grupę, która chcesz edytować.
- q Kliknij **Edytuj**. Pojawi się okno dialogowe **Wpis Uprawnienia**, jak to pokazuje **Rysunek 9**.
- q W pojawiającym się menu, w **Zastosuj**, wybierz poprawną konfigurację (np., **Ten folder, podfoldery, pliki**).
- q Kliknij **OK** →→→→**OK** →→→→**OK** →→→→**OK**, aby wyjść



Rysunek 9 Okno Wpisu Uprawnień dla folderów

Dodawanie plików lub folderów do konfiguracji zabezpieczeń

Aby dodać plik lub folder do konfiguracji zabezpieczeń:

- q Kliknij prawym przyciskiem na **System Plików**
- q Z pojawiającego się menu wybierz **Dodaj plik**
- q Wybierz plik lub folder, który ma być dodany
- q Kliknij **OK**
- q Pojawi się okno dialogowe **Zabezpieczenia Bazy Danych**
- q Konfiguruj uprawnienia kierując się wskazówkami zawartymi w sekcji: **Modyfikacja uprawnień do pliku lub folderu**

Wyłączanie plików lub folderów z konfiguracji zabezpieczeń

Występują przypadki, gdy określony plik lub folder powinien zachować dotychczasowe ustawienia zabezpieczeń. Aby uniemożliwić folderom pierwotnym rozszerzanie nowych uprawnień na takie pliki lub foldery, obiekty takie mogą zostać wyłączone z konfiguracji zabezpieczeń.

Aby wyłączyć obiekt:

- W prawym oknie **Systemu Plików**, kliknij dwukrotnie na plik lub folder, który ma być zmieniony
- Kliknij przycisk **Nie zezwalaj na zmianę uprawnień do tego pliku lub foldera**
- Kliknij **OK**

Zalecane uprawnienie do plików i folderów

Foldery i pliki nie wymienione poniżej w **Tabeli 14** domyślnie dziedziczą uprawnienia folderów pierwotnych. Foldery z opcją **Nie zezwalaj na zmianę uprawnień do tego pliku lub foldera** są wyraźnie wyłączone z konfiguracji zabezpieczeń i zachowują swoje pierwotne uprawnienia. Zwrot “Zastąp” wskazuje, że przycisk **Zastąp istniejące uprawnienia dla wszystkich podfolderów i plików uprawnieniami dziedzicznymi** powinien być zaznaczony, podczas gdy zwrot “Rozszerzaj” wskazuje, że przycisk **Rozszerzaj dziedziczne uprawnienia na wszystkie podfoldery i pliki** powinien być zaznaczony. “Ignoruj” oznacza, że folder jest wyłączony z konfiguracji.

Jeśli nie zaznaczono inaczej, domyślnie uprawnienia znajdują zastosowanie do wszystkich podfolderów i plików poniżej skonfigurowanego foldera.



UWAGA: Kilka z przedstawionych poniżej ustawień zabezpieczeń bazuje na domyślnych zabezpieczeniach Windows XP zawartych w szablonie “setup security.inf”. Usunęliśmy grupy Użytkownicy Pełnomocni i Wszyscy Użytkownicy z uprawnień domyślnych i zmodyfikowaliśmy pewne dodatkowe uprawnienia do plików i folderów

Foldery i pliki w **Tabeli 14** ułożone są w porządku alfabetycznym tak, jak występują w szablonach bezpieczeństwa GUI.

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
<p>%AllUsersProfil% Folder zawierający atrybuty pulpitu i profili dla wszystkich użytkowników, zwykle C:\Documents and Settings\All Users.</p> <p>UWAGA: Jeśli Windows XP został zainstalowany na innej kopii systemu operacyjnego, zostaną utworzone dodatkowe foldery dla profili wszystkich użytkowników w folderach Dokumentów i Ustawień. Zazwyczaj ten ten nowy profil nazywany jest All Users.WINDOWS lub All sers.COMPUTERNAME. Wcześniejsze kopie folderu All Users, mimo iż nadal istnieją, nie będą wykorzystywane. Zmienna środowiska %ProfiluAllUsers% automatycznie wskaże profil, który jest aktualnie wykorzystywany. Aby ustalić, który z profili jest aktualnie wykorzystywany, sprawdź następujący wpis w rejestrze HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList\AllUsersProfile.</p>	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Rozszerzaj
<p>%AllUsersProfile%\Application Data Zawiera dane aplikacji.</p>	Administratorzy Twórca Właściciel SYSTEM Użytkownicy Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie Zapis (Tylko ten folder i podfoldery)	Zastąp
<p>%AllUsersProfile%\Application Data\Microsoft Zawiera dane stanu aplikacji Microsoft.</p>	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Zastąp
<p>%AllUsersProfile%\Application Data\Microsoft\Crypto\DSS\MachineKeys</p>	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Wyświetlenie zawartości foldera, Odczyt atrybutów, Odczyt atrybutów rozszerzonych, Tworzenie plików, Tworzenie folderów, Zapis atrybutów, Zapis atrybutów rozszerzonych, Odczyt uprawnień (Tylko w tym folderze)	Zastąp

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
%AllUsersProfile%\Application Data\Microsoft\Crypto\RSA\MachineKeys	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Wyświetlanie zawartości foldera, Odczyt atrybutów, Odczyt atrybutów rozszerzonych, Tworzenie plików, Tworzenie folderów, Zapis atrybutów, Zapis atrybutów rozszerzonych, Odczyt Uprawnień (Tylko w tym folderze)	Zastęp
%AllUsersProfile%\Application Data\Microsoft\Dr Watson Folder zawiera dziennik błędów aplikacji Dr. Watson.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie Przechodzenie przez folder, Tworzenie plików, Tworzenia Folderów (Tylko podfoldery i pliki)	Zastęp
%AllUsersProfile%\Application Data\Microsoft\Dr Watson\drwtsn32.log Plik dziennika błędów aplikacji Dr. Watson. UWAGA: Ustawienia to ma znaczenie tylko, gdy plik drwtsn32.log już został utworzony. Alternatywnie, zamiast zapisywać plik dziennika we wspólnej lokacji i ryzykować tym samym, że wszyscy użytkownicy będą mieli do niego dostęp, aplikacji drwtsn32.exe może zostać uruchomiona i można wygenerować nową lokację dla pliku dziennika oraz pliku rzutu podczas błędów systemu.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Modyfikacja	Zastęp
%AllUsersProfile%\Application Data\Microsoft\HTML Help	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Pełna Kontrola	Zastęp
%AllUsersProfile%\Application Data\Microsoft\Media Index	Administratorzy SYSTEM Użytkownicy Użytkownicy Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie Tworzenie plików, Tworzenie folderów, Zapis atrybutów, Zapis atrybutów rozszerzonych, Odczyt uprawnień (Tylko ten folder) Zapis (Tylko podfoldery i pliki)	Zastęp

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
%AllUsers%\Documents UWAGA: Podczas przeglądania folderu %AllUsersProfile% w Eksploratorze Windows, podfolder Dokumenty występuje pod nazwą "Dokumenty Udostępnione."	Administratorzy Twórca Właściciel SYSTEM Użytkownicy Użytkownicy s	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie Zapis (Ten folder i podfoldery)	Zastąp
%AllUsers%\Documents\desktop.ini	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Zastąp
%AllUsers%\DRM	Ignoruj		Ignoruj
%ProgramFiles% Folder, w którym instalowane są aplikacje. Domyślnie umieszczony w %Dysk Systemowy%\Program Files.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie	Zastąp
%Dysk Systemowy% Dysk, na którym zainstalowany jest Windows XP. Zawiera pliki konfiguracji i rozruchu systemu.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie	Rozszerzaj
%Dysk Systemowy%\autoexec.bat c:\autoexec.bat Wymagane przez niektóre aplikacje DOS do parsowania ścieżek. Właściwym plikiem do inicjowania aplikacji DOS jest KatalogSystemowy%\system32\autoexec.nt	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Zastąp
%Dysk Systemowy%\boot.ini c:\boot.ini Boot menu.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
%Dysk Systemowy%\config.sys c:\config.sys Wymagane przez niektóre aplikacje DOS do parsowania ścieżek. Właściwym plikiem do aplikacji DOS jest KatalogSystemowy%\system32\config.nt.	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Zastąp
%Dysk Systemowy%\Documents and Settings Folder zawierający profile użytkownika i domyślny.	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Rozszerzaj
%Dysk Systemowy%\Documents and Settings\Administrator Folder zawierający wbudowany profil Administratora.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
<p>%Dysk Systemowy%\Documents and Settings\Default User Folder zawierający domyślne atrybuty profilu i pulpitu dla użytkowników logujących się po raz pierwszy.</p> <p>Uwaga: Jeśli Windows XP został zainstalowany na innej kopii systemu operacyjnego, dodatkowe foldery Użytkowników Domyślnych zostaną utworzone w folderze Documents and Settings. Zazwyczaj nowy profil jest nazywany Default User.WINDOWS lub Default User.COMPUTERNAME. Wcześniejsze kopie foldera Default User, mimo iż wciąż istniejące, nie będą używane. W przeciwieństwie do profilu All Users, profil Default User nie posiada skojarzonej zmiennej środowiskowej, dlatego też aktualnie wykorzystywany profil powinien być sprecyzowany w tym wpisie w szablonie, jeśli jest różny od profilu Default User. Aby ustalić, który profil jest aktualnie wykorzystywany sprawdź następujący wpis w rejestrze HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\DefaultUserProfile</p>	<p>Administratorzy SYSTEM Użytkownicy</p>	<p>Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie</p>	<p>Zastęp</p>
<p>%Dysk Systemowy%\io.sys Pusty plik, który jest wykorzystywany przez aplikacje DOS w celu określenia położenia partycji systemowej.</p>	<p>Administratorzy SYSTEM Użytkownicy</p>	<p>Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie</p>	<p>Zastęp</p>
<p>%Dysk Systemowy%\msdos.sys Pusty plik, który jest wykorzystywany przez aplikacje DOS w celu określenia położenia partycji systemowej.</p>	<p>Administratorzy SYSTEM Użytkownicy</p>	<p>Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie</p>	<p>Zastęp</p>

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
%Dysk Systemowy%\ntbootdd.sys Kopia sterownika urządzeń SCSI. Używany, gdy w pliku boot.ini wykorzystywana jest wpis o urządzeniach SCSI lub sygnatury.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
%Dysk Systemowy%\ntdetect.com c:\ntdetect.com Wykrywacz sprzętu podczas inicjalizacji Windows.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
%Dysk Systemowy%\ntldr c:\ntldr Program ładujący systemu operacyjnego Windows XP.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
%Dysk Systemowy%\System Volume Information Dostępny tylko dla SYSTEMU.	Ignoruj		Ignoruj
%KatalogSystemowy% Folder, w którym system operacyjny Windows XP jest zainstalowany. W czasie nowej instalacji Windows XP, folder ten jest domyślnie nazywany WINDOWS. Podczas aktualizacji na Windows XP zostaje zachowana stara nazwa folderu systemowego, zwykle winnt, jeśli zostały aktualizowane Windows NT 4.0 lub 2000 oraz WINDOWS, jeśli były aktualizowane z Windows 9x.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie	Zastąp
%KatalogSystemowy%\\$NtServicePackUninstall\$ Zawiera starsze wersje plików systemowych wymagane do wycofania dodatku service pack.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zastąp
%KatalogSystemowy%\CSC Zawiera wszystkie pliki offline wymagane przez wszystkich użytkowników komputera. CSC oznacza "client side caching".	Administratorzy	Pełna Kontrola	Zastąp
%KatalogSystemowy%\Debug Zawiera różnorodne pliki dzienników.	Administratorzy Twórca Właściciel SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Odczyt, Wykonywanie	Rozszerzaj
%KatalogSystemowy%\Debug\UserMode Zawiera dzienniki aplikacji grup użytkowników	Administratorzy SYSTEM Użytkownicy Użytkownicy	Pełna Kontrola Pełna Kontrola Przechodzenie przez folder, Wyświetlanie zawartości, tworzenie plików (Tylko w tym folderze) Zapis danych, Dołączanie danych (Tylko pliki)	Rozszerzaj
%KatalogSystemowy%\Debug\UserMode\userenv.log Plik dziennika aplikacji.	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Zapis danych, Dołączanie danych	Zastąp
%KatalogSystemowy%\Installer Administratorzy	SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt, Wykonywanie	Zastąp

FOLDER LUB PLIK	Grupa Użytkowników	Zalecane Uprawnienia	Metoda Dziedziczenia
%KatalogSystemowy%\Offline Web Pages Folder zawierający strony sieci web, które zostały ściągnięte do przeglądania off-line .	Ignoruj		Ignoruj
%KatalogSystemowy%\Prefetch Zawiera dane związane z szybkością uruchamiania aplikacji.	Administratorzy Administratorzy SYSTEM	Pelna Kontrola (Tylko w tym folderze) aplikacji. Odczyt, Wykonywanie (Tylko pliki) Pelna Kontrola (Tylko pliki)	Zastap
%KatalogSystemowy%\regedit.exe Narzędzie edycji rejestru.	Administratorzy SYSTEM	Pelna Kontrola Pelna Kontrola	Zastap
%KatalogSystemowy%\Registration Folder zawierający pliki rejestrujące Component Load Balancing (CLB) odczytywane przez aplikacje COM+ .	Administratorzy SYSTEM Użytkownicy	Pelna Kontrola (W tym folderze lub plikach) Pelna Kontrola (W ym folderze lub plikach) Odczyt (W tym folderze lub plikach)	Zastap
%KatalogSystemowy%\Registration\CRMLog	Administratorzy Tworca Właściciel SYSTEM Użytkownicy	Pelna Kontrola Pelna Kontrola (Tylko podfoldery i pliki) Pelna Kontrola Przechodzenie przez folder, Wyświetlanie zawartosci, Odczyt atrybutow, Odczyt atrybutow rozszerzonych, Tworzenie plikow, Odczyt uprawnień (Tylko w tym folderze) Odczyt danych, Odczyt atrybutow, Odczyt atrybutow rozszerzonych, Zapis danych, Dolaczanie danych, Zapis atrybutow, Zapis atrybutow rozszerzonych, Usuwanie, Odczyt uprawnień (Tylko dla plikow)	Zastap
%KatalogSystemowy%\repair Pliki zastępcze bazy danych SAM oraz innych ważnych plików systemowych i rejestru, używanych podczas naprawy systemu. Aktualizowane jeśli używany jest NTBACKUP, gdy opcja przywracania systemu jest włączona.	Administratorzy SYSTEM	Pelna Kontrola Pelna Kontrola	Zastap
%KatalogSystemowy%\security Zawiera szablony bezpieczeństwa bazy danych analiz	Administratorzy Tworca Właściciel SYSTEM	Pelna Kontrola Pelna Kontrola (Tylko podfoldery i Pliki) Pelna Kontrola	Zastap

FOLDER LUB PLIK	GRUPY UŻYTKOWNIKÓW	ZALECANE UPRAWNIENIA	METODA DZIEDZICZ ENIA
<u>%System%\system2</u> Zawiera pliki systemowe	Administratorzy TWÓRCA WŁAŚCICIEL SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Tylko podfoldery i pliki) Pełna Kontrola Odczyt Uruchom	Zamiana
<u>%System%\system2\arpsvc.exe</u> Wyświetla i modyfikuje IP do Tabel translacji adresów Protokołu Rozdzielczości Adresu (ARP)dla MA':	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\at.exe</u> Ustawia programy do uruchomienia określonego dnia i o określone] godzinie	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\cmdv.msc</u> Konsola do Indeksowania	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\ComComExD.msc</u> Konsola dla Usług Komponentowych	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\comom.msc</u> Konsola obsługi komputera	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\confi</u> Zawieia pliki rejestru i logi	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\devmamt.msc</u> Konsola obsługi urządzeń	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\dfia.msc</u> Konsola Defragmentatora Dysków	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\dishmamt.msc</u> Konsola do obsługi dysków	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\dlcach</u> Zawiera kopie chronionych plików systemowych te kopie są używane przez System File Checker do reperacji uszkodzonych lub zmodyfikowanych plików systemowych	Administratorzy TWÓRCA WŁAŚCICIEL SYSTEM	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola	Zamiana
<u>%System%\system2\eventvwr.msc</u> Konsola Monitora Wydarzeń	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\fsma.msc</u> Konsola Folderów Współdzielonych	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%System%\system2\groupedit.msc</u> Konsola Polis Grupowych	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana

%System%\system2\Group Policy Folder zawierający obiekty Polis Grupowych	Administratorzy Zalogowani użytkownicy SYSTEM	Pełna Kontrola Odczyt, Uruchamianie Pełna Kontrola	Rozszerzanie
%system%\system2\ias Zawiera bazy danych dla Usługi Uwierzytelniania Internetowego.	Administratorzy TWÓRCA WŁAŚCICIEL SYSTEM	Pełna Kontrola Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\lusrmar.msc Konsola dla lokalnych użytkowników i grup	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\MSDTC Zawiera pliki dla Koordynatora Transakcji MS, który jest potrzebny dla Serwera Transakcji Microsoft.	Administratorzy SERWIS SIECIOWY SYSTEM	Pełna Kontrola Odczyt. Zapis. Uruchamianie Pełna Kontrola	Rozszerzanie
%system%\system2\nbtstat.exe Pokazuje statystyki protokołów i aktualne połączenia TCP/IP używając NetBIOS na TCP/IP	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\netsh.exe Narzędzie do konfiguracji sieci (Linia Komend).	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\netstat.exe Pokazuje statystyki protokołu i aktualne połączenia TCP/IP.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\dnsllookup.exe Pokazuje informacje DNS	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\Ntbackup.exe Program tworzący kopie zapasowe.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\NTMSData Standardowa lokalizacja dla bazy danych Wymiennych Dysków.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Rozszerzanie
%system%\system2\ntmsmgr.msc Konsola dla Dysków Wymiennych	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\ntmsoprq.msc Konsola dla Poleceń Operatora Dysków Wymiennych.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\perfmon.msc Konsola Monitora Wydajności Systemu	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\rpc.exe Program używany do wywoływania zdalnych procedur.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\reg.exe Narzędzie do edycji i sprawdzenia rejestru	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
%system%\system2\regedit2.exe To samo co regedit.exe. W poprzednich wersjach Windows NT (również 2000) było to dodatkowe narzędzie do edycji rejestru.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana

FOLDER LUB PLIK	GRUPY UŻYTKOWNIKÓW	ZALECANE UPRAWNIENIA	METODA DZIEDZICZENIA
<u>%system%\system2\regini.exe</u> Narzędzie do edycji i sprawdzenia rejestru.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\rexec.exe</u> Program do uruchamiania zdalnych wywołań.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\route.exe</u> Program do manipulacji tabel routingu sieciowego.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\rsh.exe</u> Program do uruchamiania zdalnego shella.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\RSOP.msc</u> Konsola do Resultant Set of Policy.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\secdit.exe</u> Narzędzie do konfiguracji i analizy zabezpieczeń	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\secpol.msc</u> Konsola do Polisy Lokalnych Zabezpieczeń	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\services.msc</u> Konsola usług.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\Setup</u> Zawiera pliki menagera elementów opcjonalnych	Administratorzy SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola Odczyt. Uruchamianie	Rozszerzanie
<u>%system%\system2\Spool\Printers</u> Drukarki.	Administratorzy TWÓRCA WŁAŚCICIEL SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Folder przechodni. Atrybuty odczytu. Rozszerzony odczyt Tworzenie plików Tworzenie folderów (Ten folder i podfoldery)	Zamiana
<u>%system%\system2\systeminfo.exe</u> Program sprawdzający podstawowe informacje o systemie.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\tftp.exe</u> Używa usługi Trivial File Transfer Protocol do transferu plików do i z komputera zdalnego bez autoryzacji.	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana
<u>%system%\system2\wmimamt.msc</u> Konsola do Zarządzania Windows	Administratorzy SYSTEM	Pełna Kontrola Pełna Kontrola	Zamiana

FOLDER LUB PLIK	GRUPY UŻYTKOWNIKÓW	ZALECANE UPRAWNIENIA	METODA DZIEDZICZENIA
%system%\Tasks Folder zawierający zadania zaplanowane w Harmonogramie Zadań	Ignoruj		Ignoruj
%system%\Temp Folder zawierający pliki tymczasowe.	Administrator TWÓRCA WŁAŚCICIEL SYSTEM Użytkownicy	Pełna Kontrola Pełna Kontrola (Tylko podfoldery i pliki) Pełna Kontrola Folder przechodni. Tworzenie plików. Tworzenie folderów (Ten folder i podfoldery)	Zamiana

Tabela 14 Zalecane Uprawnienia dla folderów i plików

Modyfikacja usług systemowych przez przystawkę szablonów bezpieczeństwa



UWAGA: Po dokonaniu jakichkolwiek modyfikacji w pliku konfiguracyjnym upewnij się, że zmiany zostały zapisane a następnie przetestuj wprowadzone ustawienia przed zainstalowaniem ich w pracującej sieci.

Analiza i konfiguracja Zabezpieczeń

Po modyfikacji odpowiednich matryc zabezpieczeń, analiza i konfiguracja zabezpieczeń może być dokonana przez zatrask Security Configuration and Analysis lub linię komend. Najlepiej wykonać tę procedurę gdy wprowadzamy zabezpieczenia do lokalnego systemu. Po instrukcje jak importować ustawienia zabezpieczeń do grup, patrz Rozdział 42



UWAGA: Wprowadzenie konfiguracji zabezpieczeń do systemu Windows XP może być przyczyną utraty wydajności i funkcjonalności

Uruchomienie Konfiguracji Bezpieczeństwa i Analiz w MMC

Aby załadować Security Configuration and Analysis do MMC:

- § Uruchom Konsolę Zarządzania (mmc.exe)
- § Wybierz Console-» Dodaj/Usuń zatrask
- § Kliknij Dodaj
- § Wybierz Analiza i Konfiguracja
- § Kliknij Dodaj
- § Kliknij Zamknij
- § Kliknij OK

Aby uniknąć konieczności przeładowania zatrasku za każdym razem gdy MMC jest zamykane i otwierane, zapisz aktualne ustawienia konsoli przez:

W menu Konsola, wybierz Zapisz. Domyślnie plik będzie zapisany w menu Narzędzi Administracyjnych aktualnie załadowanego użytkownika.

Wpisz nazwę pliku, pod którą będą zapisane ustawienia

Od teraz do konsoli można wejść z Start —»• Programy Narzędzia Administracyjne



Uwaga: Więcej niż, jeden zatrask może być jednorazowo załadowany do MMC. Na przykład Matryce Zabezpieczeń i matryce Konfiguracji i Analizy Zabezpieczeń **mogą być załadowane do konsoli do przyszłego użycia.**

Bazy danych konfiguracji zabezpieczeń


Zatrask Analizy i Konfiguracji Zabezpieczeń używa bazy danych do przetrzymywania ustawień dla analizy lub konfiguracji. Aby otworzyć istniejącą lub nową bazę danych używając GUI:

W MMC, kliknij prawym klawiszem myszy na Analiza i Konfiguracja Zabezpieczeń

Wybierz Otwórz Bazę Danych


§ Wpisz nazwę istniejącej lub nowej bazy danych


§ Kliknij Otwórz

 **Uwaga: Zaleca się tworzenie nowej bazy danych dla każdej pary analizy i konfiguracji**

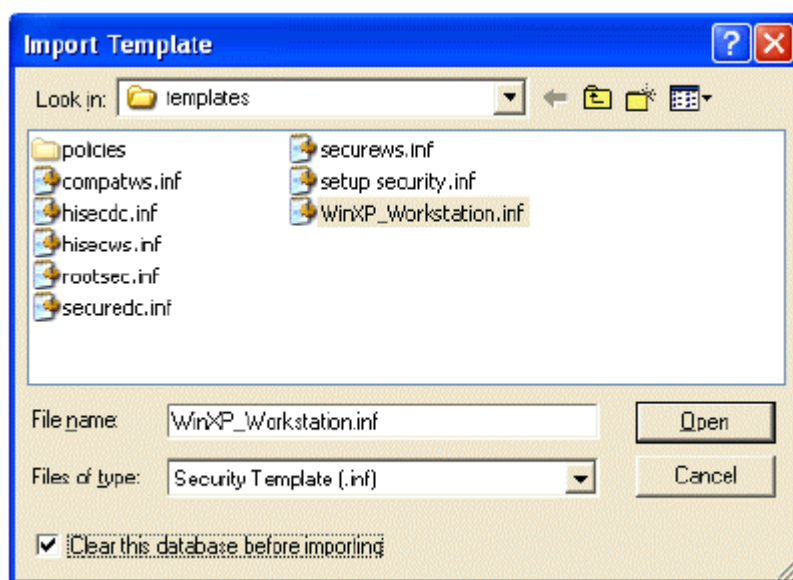
Pliki konfiguracyjne mogą być importowane do bazy przez wykonanie poniższej procedury:

- § Jeżeli wpisano przy otwieraniu nową nazwę bazy danych, użytkownik będzie automatycznie poproszony o wpisanie nazwy pliku konfiguracyjnego do importu.
- § Kliknij prawym klawiszem myszy na Analiza i Konfiguracja Zabezpieczeń z lewej strony MMC
- § Wybierz Importuj szablon
- § W oknie Importuj szablon, wybierz właściwy plik konfiguracyjny p-nf
- § Zaznacz Wyczyść bazę danych przed importem aby usunąć poprzednie dane z bazy tak jak na Rys. 40

 **UWAGA:** Importowanie może być przez wznowienie lub nadpisanie informacji wcześniej importowanej. Wznawianie jest domyślne. Jeżeli użytkownik nie chce mieszać szablonów konfiguracji, zaznacz "Wyczyść bazę danych przed importem, aby nadpisać aktualną bazę danych"

 **UWAGA:** Aby uniknąć zagubienia i przypadkowego połączenia konfiguracji zaleca się zaznaczenia tej opcji przy tworzeniu nowych analiz

§ Kliknij Otwórz



Rys. 10 Wybór pliku konfiguracji

Opcje programu Secedit, używanego w linii poleceń

secedit. exe , przedstawiony w Rozdziale 2, jest pomocny przy wykonywaniu analiz i konfiguracji zabezpieczeń przez linie komend i wsadowe i/lub zaplanowane programy. Składnia linii komend dla secedit do użytku do analizy i konfiguracji systemu:

```
secedit {/analyze /configure} [/cfg filename] [/db filename]
[/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

Tabela 15 wyjaśnia składnie parametrów dla secedit. Exe

Parametr	Opis
/analyze	Wykonuje analizę
/configure	Wykonuje konfigurację
/cfg filename	Ścieżka do pliku konfiguracyjnego, który będzie wznowiony przy dokonywaniu analizy
/db filename	Ścieżka do bazy danych, którą secedit będzie analizował. Jeżeli brak parametru to użyta będzie ostatnia baza konfiguracji/analizy. %SystemRoot%\Security\Database\secedit.sdb jest używany D Uwaga: Zaleca się tworzenie nowej bazy danych dla każdej pary analizy i konfiguracji
/log LogPath	Ścieżka do pliku logów dla procesu. Jeżeli brak, informacje o postępie będą wyświetlane w konsoli Uwaga: Informacje w pliku logu będą dopisywane. Użytkownik musi wpisać inną nazwę, jeżeli ma być utworzony nowy plik
/verbose	Dokładne informacje o postępie
/quiet	Ukrywa okno i raportowanie logów
/overwrite	Nadpisuje nazwaną bazę danych, dodaną informacją konfiguracji UWAGA: Pliki konfiguracyjne mogą być dopisane lub nadpisać bazę danych, która była utworzona wcześniej. Dopisywanie jest domyślne. Wpisz /overwrite aby nadpisać Aktualną bazę danych UWAGA: Aby uniknąć zagubienia i przypadkowego połączenia konfiguracji zaleca się zaznaczenia tej opcji przy tworzeniu nowych analiz

Parametr	Opis
/areas Areas	<p>Stosowany jedynie z /configure. Precyzuje obszary zabezpieczone.</p> <p>Dostępne są:</p> <p>SECURITYPOLICY - polisa lokalna i na domenę dla systemu, wliczając polisy na konta, polisy kontrolne, itd.</p> <p>GROUP_MGMT - Ustawienia Ograniczonych Grup</p> <p>USER_RIGHTS - Prawa Użytkowników</p> <p>DSOBJECTS - Zabezpieczenia na foldery</p> <p>REGKEYS - Zezwolenia dostępu do lokalnych kluczy rejestru</p> <p>FILESTORE - Zezwolenia dostępu do systemu plików</p> <p>SERYICES - Konfiguracja zabezpieczeń dla wszystkich zdefiniowanych usług</p> <p>UWAGA: Jeżeli /areas nie jest użyty, domyślny jest cały obszar. Jeżeli użyty każda nazwa obszaru powinna być oddzielona spacją.</p>

Tabela 45 Parametry linii komend Secedit



UWAGA: Opcja `secedit /refreshpolicy` (wymuszone uaktualnienie polisy grupy), która była dostępna w Windows NT i Windows 2000 nie istnieje w Windows XP. Ta komenda została zastąpiona przez `gpupdate.exe`. Patrz Rozdział 12 po więcej szczegółów dotyczących `gpupdate`.

Tworzenie analizy zabezpieczeń

Analiza zabezpieczeń jest wykonywana na podstawie bazy danych. Pliki konfiguracyjne, które były importowane do bazy danych tworzą podstawę analizy. Ustawienia zabezpieczeń z plików konfiguracyjnych są porównywane z aktualnymi zabezpieczeniami systemu i rezultat jest przechowywany w tej bazie danych. Podstawowe ustawienia są ukazywane obok aktualnych. Konfiguracja może być modyfikowana jako wynik analizy. Zmodyfikowana informacja konfiguracyjna może być eksportowana do pliku konfiguracji do powtórnego użycia.

Dokonywanie Analizy Zabezpieczeń przez linie komend

Aby dokonać analizy z poziomu linii komend, wpisz w oknie dialogowym:

```
a secedit /analize [/cfg filename] [/db
filename] [/log LogPath] [/verbose] [/quiet]
[/overwrite] [> results_file]
```

`results_file` jest to nazwa pliku zawierającego wynik analizy. Przydatne jest sprawdzenie rezultatów później. W przypadku wybrania odpowiedniej opcji `results_file`, wynik będzie wyświetlony na ekranie.

Dokonywanie analizy zabezpieczeń przez GUI

Rys.11 pokazuje przykładowy wynik analizy przeprowadzonej przy pomocy Analizy i Konfiguracji Zabezpieczeń. Poniższe kroki powinny być wykonane aby dokonać analizy w GUI:

- § Kliknij prawym klawiszem myszy na Bazy Danych i Wybierz Analizuj Teraz ...
- § W oknie dialogowym wpisz ścieżkę dostępu do loga zawierającego informacje o błędach



Uwaga: Informacje w pliku logu będą dopisywane. Użytkownik musi wpisać inną nazwę jeżeli ma być utworzony nowy plik

- § Kliknij OK.

Policy	Database Setting	Computer Setting
Accounts: Administrator account status	Enabled	Enabled
Accounts: Guest account status	Disabled	Disabled
Accounts: Limit local account use of elevated functions to	Enabled	Enabled
Accounts: Rename administrator account	Not Analyzed	Administrator
Accounts: Rename guest account	Not Analyzed	Guest
Audit: Audit the access of global objects	Not Analyzed	Disabled
Audit: Audit the use of Backup on Remote Storage	Not Analyzed	Disabled
Audit: Shut down system immediately after specified period of inactivity	Enabled	Disabled
Devices: Allow undock without having to save	Disabled	Enabled
Devices: Allowed to format and eject hard disk	Administrators	Administrators
Devices: Prevent users from installing removable devices	Enabled	Disabled
Devices: Restrict CD-ROM access to removable media	Enabled	Disabled
Devices: Restrict floppy access to removable media	Enabled	Disabled
Devices: Unsigned driver installation restrictions	Warn but allow installation	Warn but allow installation
Domain controller: Allow server operating system to be remotely administered	Not Analyzed	Not Analyzed
Domain controller: LDAP server signing requirements	Not Analyzed	Not Analyzed
Domain controller: Refuse machine accounts	Not Analyzed	Not Analyzed
Domain member: Digitally encrypt communications with untrusted domain members	Not Analyzed	Enabled
Domain member: Digitally encrypt outgoing secure channel communications	Enabled	Enabled
Domain member: Digitally sign secure channel communications	Enabled	Enabled
Domain member: Disable machine authentication	Disabled	Disabled
Domain member: Maximum machine age	7 days	30 days
Domain member: Require strong authentication for secure channel with untrusted domain members	Enabled	Disabled
Interactive logon: Do not display last names	Enabled	Disabled
Interactive logon: Do not require authentication on the local computer	Disabled	Not Analyzed
Interactive logon: Message text for the prompt	Not Analyzed	
Interactive logon: Message title for the prompt	Not Analyzed	

Rys. 11 Wyniki Analizy zabezpieczeń

Konfigurowanie systemu

Podczas konfiguracji, błędy mogą wystąpić jeżeli odpowiednie pliki lub klucze rejestru nie istnieją w systemie tylko w pliku konfiguracyjnym inf. Nie przejmuj się. Pliki inf starają się spełnić różne scenariusze i konfiguracje, do których system może pasować lub nie

Konfigurowanie Systemu przez Linie Komend

Aby skonfigurować wszystkie dostępne opcje poprzez linie komend za jednym razem:

secedit /configure [/cfg filename] [/db filename] [/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]



UWAGA: Nie wpisanie nazwy nowej bazy danych za każdym razem tworzenia konfiguracji lub użycie /overwrite może spowodować nieprzewidziane zachowanie secedit. Np. importowane pliki konfiguracyjne mogą być połączone z innymi plikami, co może prowadzić do błędnych interpretacji zdarzeń

Poniżej przykład użycia linii komend do skonfigurowania tylko wybranych obszarów:

```
§ Q secedit /configure /cfg "WinXP_workstation.inf" /db newdb.sdb /log logfile.txt /overwrite /areas REGKEYS FILESTORE
```

Ten przykład importuje plik WinXP_workstation.inf system plików i zezwolenia rejestru i konfiguruje system lokalny

Poniższe kroki powinny być podjęte, aby skonfigurować system przez "Analiza i Konfiguracja Systemu":

- § Kliknij prawym klawiszem myszy na Bazy Danych
- § Wybierz Konfiguruj Komputer...
- § W oknie dialogowym wpisz ścieżkę dostępu do loga zawierającego informacje o błędach.



Uwaga: Informacje w pliku logu będą dopisywane. Użytkownik musi wpisać inną nazwę, jeżeli ma być utworzony nowy plik

- § Kliknij OK.



UWAGA: Podczas konfiguracji systemu przez GUI, wszystkie ustawienia w szablonie są wprowadzane. Nie ma opcji takiej jak w secedit.exe, aby precyzyjnie określić tylko część szablonu, np. Pozwolenia plików, polisy na kontakach, do wprowadzenia.

Wprowadzanie Grupowej Polisy Windows XP do Domeny Windows

Polisa Grupowa do kontroli użytkowników i komputera w środowisku Windows 2000/XP jest oparta na mechanizmie Aktywnych Katalogów. Ustawienia dotyczące zabezpieczeń, instalacji oprogramowania i skrypty mogą być ustalane przez Polisę Grupową. Polisa Grupowa jest stosowana do grup użytkowników i komputerów na podstawie ich lokalizacji w Aktywnym Katalogu.

Ustawienia Polis Grupowych są przechowywane w obiektach Polis Grupowych (GPOs) na kontrolerach domen. GPO są łączone z odbiorcami (strony, domeny i organizacje - OU) w strukturze Aktywnych Katalogów. Ponieważ Polisy Grupowe są wysoko zintegrowane z Aktywnymi Katalogami, ważna jest podstawowa wiedza nt. struktury Aktywnych Katalogów do implementacji Polis Grupowych. Patrz Instrukcja Zabezpieczania Microsoft Windows 2000 - Aktywne Katalogi po więcej informacji.

Polisa Grupowa jest narzędziem do zabezpieczania Window XP. Może być użyta do wprowadzenia i podtrzymania stałych zabezpieczeń na całej sieci z konkretnej lokalizacji.

Podsumowanie

Polisa Grupowa w Windows XP ma wiele nowych opcji nie dostępnych w Windows 2000. Mimo to kontrolery Windows 2000 mogą przesłać polisy do klientów Windows XP poprzez Aktywne Katalogi.

Aby skorzystać w pełni z nowych ustawień i funkcji Windows XP GPO musi być edytowane na komputerze z Windows XP. Administrator może dokonać kolejnej edycji GPO (np. łącząc domeny GPO i OU) z kontrolera Windows 2000. Jeżeli GPO jest załadowany do komputera zawierającego systemy Windows 2000 i XP, Windows 2000 będzie ignorował ustawienia dostępne tylko w XP konfigurując tylko te opcje, które Windows 2000 rozumie. Komputery z Windows XP w pełni wprowadzą wszystkie ustawienia. Patrz do instrukcji Zabezpieczania Microsoft Windows 2000 - Aktywne Katalogi po informacje o wprowadzaniu GPO na domeny z Windows 2000. Również artykuł Microsoftu "Aktualizacja Polis Grupowych Windows 2000 dla Windowsa XP" dostępny tutaj:

<http://support.microsoft.com/support/kb/articles/Q107/9/00.asp>.

Rozszerzenie ustawienia zabezpieczeń

Z perspektywy zabezpieczeń, jedną z najważniejszych części Polis Grupowych jest rozszerzenie Ustawienia Zabezpieczeń. Wiele nowych ustawień jest w nich zawartych. Pozwalają one administratorowi na połączenie wielu opcji zabezpieczeń i wprowadzenie ich do dowolnej liczby komputerów z Windows XP poprzez Polisy Grupowe i Aktywne Katalogi

Ustawienia Zabezpieczeń są ulokowane w Computer Configuration\Windows Settings\ Security Settings wraz z GPO i dostęp jest możliwy przez Polisy Grupowe MMC. Ustawienia Zabezpieczeń odnoszą się do komputera nie użytkowników i zawierają obszary wyszczególnione w szablonach zabezpieczeń (np Polisy Kontowe, Lokalne, itd) razem z Public Key Policies i IP Security Policies w Aktywnym Katalogu

Tworzenie GPO w Windows XP

GPO z Windowsa XP musi być edytowane na komputerze z Windows XP. Aby otworzyć i/lub stworzyć GPO wykonaj poniższe kroki z systemu Windows XP przyłączonego do domeny:

- § Uruchom mmc. exe
- § Wybierz Konsola —»-Dodaj/Usuń przystawkę
- § Kliknij Dodaj
- § Wybierz Polisa Grupowa
- § Kliknij Dodaj
- § Pojawi się okno Wybierz Obiekt Polisy Grupowej. Poniżej będzie wypisany domyślnie Komputer Lokalny. Aby zmienić GPO do edycji kliknij Przegadaj.
- § W domenie, przejdź do folderu docelowego dla GPO. Wybierz istniejący GPO lub kliknij na drugiej ikonie na górze okna aby utworzyć nowe GPO, potem je wybierz
- § Kliknij OK.
- § Kliknij Zamknij
- § Kliknij OK.

Importowanie szablonu zabezpieczeń do GPO

Aby importować istniejący szablon zabezpieczeń do GPO Windows XP, wykonaj następujące kroki:

- § W przystawce Polisy Grupowe, przejdź do Computer Configuration\Windows Settings\Security Settings.
- § Otwórz Ustawienia Zabezpieczeń przed importowaniem szablonu. Rys. 12 ukazuje otwarte rozszerzenie Ustawienia Zabezpieczeń



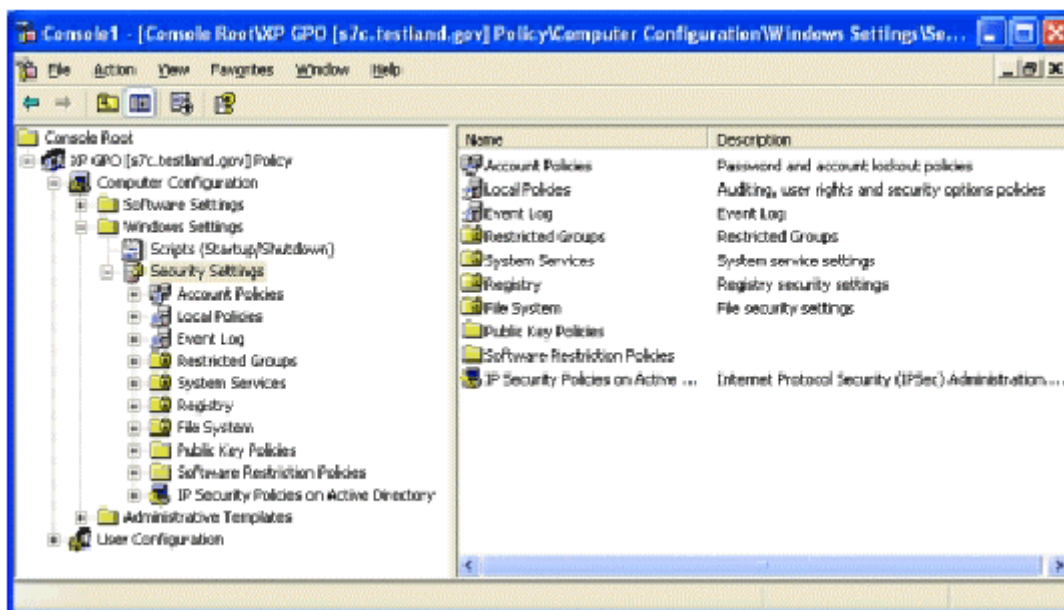
UWAGA: Z powodu błędu w MMC, nie otwarcie Ustawienia Zabezpieczeń przed importowaniem szablonu zaowocuje błędem przy ładowaniu szablonu

- § Kliknij prawym klawiszem myszy na Ustawienia Zabezpieczeń i Wybierz Importuj Polisę z rozszerzalnego menu

- § Okno Importuj Polisę z ... pokazuje wszystkie pliki w folderze % katalog_systemowy%\security\templates. Wybierz szablon z tego folderu lub przeglądaj inne aby znaleźć odpowiedni.
- § Kliknij Otwórz
- § Ustawienia w wybranym szablonie będą importowane do zakładki Ustawienia Zabezpieczeń. Możesz obejrzeć i edytować te ustawienia przez przejście w dół po drzewie Ustawień Zabezpieczeń



UWAGA: Aby poprawnie wprowadzić nowe GPO musisz zarejestrować wprowadzone zmiany. Proste importowanie szablonu do nowego GPO nie jest traktowane jak zmiana pomimo, że zamknięcie GPO w przystawce Polisy Grupowe i otwarcie ponownie pokaże, że importowane dane zostały zachowane. GPO będzie uważane za puste i nie będzie wprowadzone gdy polisy grupowe będą odświeżane. Aby zarejestrować zmianę edytuj cokolwiek w GPO po importowaniu szablonu zabezpieczeń, nawet jeżeli zmienisz ustawienie, a potem przywrócisz poprzednie



Rys. 12 Rozszerzenie Ustawień Zabezpieczeń w GPO

Zarządzanie GPO Windows XP z Kontrolera Domeny Windows 2000

Jak wspomniano wcześniej, gdy GPO Windows XP było edytowane na komputerze z Windows XP, kolejne GPO (np. łączenie GPO z domenami lub OU) może być wykonane z kontrolera domen Windows 2000.

Podczas przegadania GPO Windows XP przez kontroler domen Windows 2000, przejście w dół do sekcji Computer Configuration\Windows Settings\Security Settings może spowodować się pojawienie informacji: Nie można otworzyć pliku szablonu w prawym panelu. Tak się stanie jeżeli jakiegokolwiek grupy i/lub użytkownicy tylko Windows XP (np.: LOCAL SERVICE, NETWORK SERVICE) są wymienieni w jakimkolwiek pliku lub rejestrze skonfigurowanym w Ustawieniach Zabezpieczeń. Pomimo błędów przy otwieraniu ustawień w Windows 2000 GPO będzie wprowadzony poprawnie.

Obiekt Polisy Grup Lokalnych

Każdy komputer posiada Polisy Grupowe nie ważne czy jest częścią domeny. Polisa Grupy Lokalnej jest pierwszą stosowaną. Jednak inne polisy mogą obejść ustawienia polisy lokalnej, inne ustawienia Lokalnej Polisy Grupowej, nie ustawione w innej polisie pozostaną. Ważne jest skonfigurowanie trwałej polisy lokalnej w pouczeniu z Polisy Grupową Aktywnych Katalogów.

Obiekt Lokalnej Polisy Grupowej(LGPO) jest zapisany w %katalog_systemowy*\ System32\Group Policy. Może być oglądany wybierając obiekt Komputer Lokalny w przystawce Polisa Grupowa lub przez wybór opcji Lokalna Polisa Zabezpieczeń w menu Narzędzi Administracyjnych

LPGO nie ma wszystkich ustawień dostępnych w Polisie Grupowej Aktywnych Katalogów. Na przykład, w zakładce Ustawienia Zabezpieczeń, tylko Polisy Kont i Lokalne Polisy są dostępne. Tak więc podczas gdy szablon zabezpieczeń może być importowany do polisy lokalnej, tylko ustawienia dostępne dla polisy lokalnej będą importowane. Dodatkowe ustawienia, jak pozwolenia rejestru i plików, mogą być wprowadzone przez Analiza i Konfiguracja Zabezpieczeń.

Wymuszenie uaktualnienia polisy grupowej

Polisa Grupowa jest od czasu do czasu uaktualniana przez Aktywny Katalog. Domyślne ustawienie uaktualnia polisy stacji roboczej co 90 min.

Aby wymusić uaktualnienie Polisy Grupowej użyj narzędzia linii komend gpupdate.exe. Wpisanie gpupdate /? wypisze wszystkie dostępne komendy. Na przykład, aby wymusić uaktualnienie konfiguracji Polisy Grupowych komputera wpisz:

```
Gpupdate /target:computer /force
```

Oglądanie rezultatów ustawień Polisy Grupowej

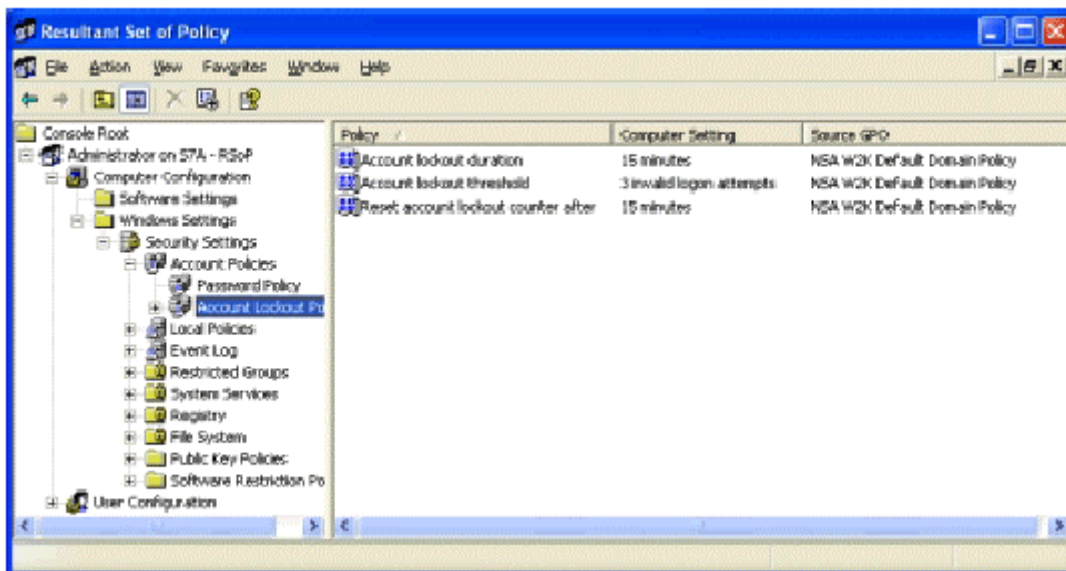
Różne GPO mogą być stosowane do obiektów domen zaleganie od komputera, na którym są dane obiekty. Na przykład ustawienie GPO na poziomie domeny będzie stosowane do wszystkich komputerów domeny, a GPO dla innych Jednostek Organizacyjnych (OU) będą stosowane do obiektów w danym OU. Ustawienie ręczne, który GPO gdzie i w jakiej kolejności stosować może być przerażające, szczególnie w kompleksowej strukturze domen. Przez to stworzenie poradnika do Polisy Grupowych jest trudne. Jednakże, Windows XP oferuje dwa narzędzia, Resultant Set of Policy(RSoP) i gpresult.exe, aby pokazać jak GPO jest wprowadzane do obiektu.

Przystawka RSoP

RSoP.msc jest przystawką MMC pokazującą ustawienia zbiorcze wszystkich polis wprowadzonych do komputera lokalnego. Aby utworzyć przystawkę, wpisz RSoP.msc w linii komend lub dodaj przystawkę Resultant Set of Policy gdy jesteś w MMC. Rys. 13 pokazuje przystawkę Rop.

Dla każdego ustawienia polis grupowych, RSoP pokazuje Ustawienia Komputera (jak komputer jest obecnie skonfigurowany) i źródłowe GPO (które GPO ustawiło aktualną konfigurację). Po więcej informacji na temat RSoP, patrz

<http://www.microsoft.com/technet/prodtechnet/winxpro/proddocs/RSPintro.asp>.



Rys. 13 przystawka RSoP

Gpresult.exe

Gpresult.exe jest narzędziem linii komend dającym statystyki ostatniego wprowadzenia Polisy Grupowej do komputera, jakie GPO i gdzie zostało wprowadzone i w jakiej kolejności i GPP które nie zostały wprowadzone z powodu filtrowania. Gpresult może również zbierać informacje o systemie zdalnym.

Aby zobaczyć wszystkie opcje linii komend gpresult, wpisz w linii komend:

```
gpresult /?
```

Znane rezultaty

Ta sekcja wskazuje kilka rezultatów włączając wymiennosc domen Windows XP Profesional i Windows 2000

Ustawienie RestrictAnonymous i "Użytkownik musi zmienić hasło przy następnym logowaniu"

Windows XP domyślnie nie nadaje użytkownikowi anonimowemu tych samych przywilejów co grupie Wszyscy tak jak to jest w Windows NT i Windows 2000. To może prowadzić do potencjalnych problemów gdy konto użytkownika w Windows 2000 ma ustawioną opcje "Użytkownik musi zmienić hasło po zalogowaniu i Klucz Rejestru RestrictAnonymous w kontrolerze domen Windows 2000 jest ustawiony tak, że użytkownik anonimowy nie ma żadnych praw chyba, że są wyjątki (wartość w rejestrze=2) tak jak jest podane w przewodniku po zabezpieczeniach NSA Windows 2000.

Podczas gdy użytkownik Windows 2000 Profesional nie ma problemów z logowaniem i zmianą hasła, z Windows XP użytkownik widzi błąd "Nie masz prawa zmieniać hasła" po wpisaniu nowego hasła. Jedynym rozważaniem jest zmiana ustawienia RestrictAnonymous w Windows 2000 na 0 lub 1. Zauważ, że ta zmiana otwiera kontroler

domen Windows 2000 na różne taktyki zbierania informacji możliwych do wykorzystania przez osoby niepowołane. Nawet gdy klucz rejestru jest ustawiony na 1, są narzędzia które mogą obejść to zabezpieczenie i wyliczyć informacje o kontach użytkowników. Ryzyko musi być odpowiednio wyważone do potencjalnych zysków ze zmuszania użytkownika do zmiany hasła przy następnym logowaniu z klienta Windows XP.

Pomoc Zdalna/Konfiguracja Pulpitu

Tak jak wszystkie technologie zdalne, Pomoc Zdalna i Zdalne Pulpity osłabiają zabezpieczenia i musi być to brane pod uwagę przy używaniu ich. Dla najwyższego stopnia zabezpieczeń zaleca się nie używać technologii zdalnej. Jednakże zrozumiałe jest, że ta technologia może przynieść zyski dla klientów. Ta sekcja zawiera zalecenia zabezpieczeń mogące podnieść ich skuteczność nie rezygnując ze zdalnych pulpitów i/lub pomocy, jeżeli zamierzasz używać tej technologii

Pomoc zdalna

Pomoc Zdalna (RA) jest zdolnością, która pozwala początkującemu użytkownikowi prosić o pomoc innych, ekspertów. Używając tej technologii ekspert może obejrzeć pulpit początkującego i wysłać mu wiadomość lub, gdy ustawienia na to pozwalają przejąć kontrolę nad systemem jednocześnie obsługując pulpit. Początkujący jest proszony o potwierdzenie lub zabronienie dostępu ekspertowi w przypadku połączenia tylko-podgląd, i ponownie gdy ekspert chce przejąć kontrolę nad systemem. Aby używać RA obaj użytkownicy muszą używać Windows XP.

RA może być zapoczątkowana przez prośbę użytkownika, zwaną Zapowiedzianą Pomocą Zdalną lub przez eksperta proponującego pomoc początkującemu, zwaną Oferty Pomocy Zdalnej. Konto AsystentaPomocy jest używane do połączeń RA. To konto jest tworzone jako część domyślnej instalacji, przyznawane jest losowo generowane hasło i konto jest wyłączone. Podczas otwierania zaproszenia RA bilecik "początkującego" jest tworzony na lokalnym komputerze użytkownika, port 3389 jest otwierany aby umożliwić dostęp do usług zdalnych i konto Asystenta jest aktywowane. Ekspert łączy się z komputerem początkującego używając list uwierzytelniających AsystentaPomocy. Po zamknięciu lub wygaśnięciu bilecików konto AsystentaPomocy jest wyłączone i port zamknięty



UWAGA: Usługi Zdalne są również używane do Połączeń Zdalnego Pulpitu więc port 3389 może zostać otwarty jeżeli Pulpity Zdalne są uruchomione

Użytkownik może wysłać zaproszenie do pomocy zdalnej przez e-mail, Windows Messenger, lub zapisać jako plik. Aktualnie nie ma limitu kogo początkujący może prosić o pomoc zdalną; zaproszenie może być wysłane do wszystkich, którzy mają fizyczne połączenie z siecią użytkownika. W momencie odpowiedzi na zaproszenie do Zapowiedzianego RA, początkujący widzi nazwę użytkownika eksperta.

Jedynym sposobem na upewnienie się, czy ekspert jest tym, za kogo się podaje jest użycie hasła. Początkujący jest proszony o wpisanie hasła przy tworzeniu zaproszenia, chociaż nie jest wymagane przez system. To hasło nie jest przesyłane razem z zaproszeniem i musi być wysłane do eksperta oddzielnie inną drogą. Kompleksowość hasła, polisy haseł i polisy zabezpieczającej konta nie są stosowane do haseł Zapowiedzianych RA.

Zaproszenia wysłane przez MSN Messangera są wysyłane jako czysty tekst XML. Wysyłane przez e-mail lub zapisane jako pliki MsRcIncident również są czystym tekstem XML. Możliwe jest odczytanie informacji kto potrzebuje pomocy, jego IP, portu używanego przez Usługi Zdalne i hasła jeżeli początkujący je załączył.

Z tych powodów nie zaleca się stosowania Zapowiedzianych RA w sieciach, w których bezpieczeństwo jest ważne.

Oferty Pomocy Zdalnej

Oferty RA są odczytywane jako bardziej zabezpieczony sposób udzielania pomocy początkującym. Oferty RA są dostępne tylko pomiędzy dwoma komputerami w tej samej domenie lub w zaufanych domenach i lista użytkowników mogących dać taką ofertę jest konfigurowalna. Przy ubyciu tej metody ekspert nie może połączyć się do użytkownika bez jego wyraźnej zgody. Użytkownik ma w dalszym ciągu możliwość akceptacji lub zabronienia pouczenia.

W celu ubycia zdolności Pomocy Zdalnej, muszą być dokonane następujące zmiany w Prawach Użytkowników we wprowadzonym szablonie konfiguracji zabezpieczeń.

Prawa Użytkowników	Zalecane Ustawienia
<p>Allow logon through Terminal Services</p> <p>Ustala, którzy użytkownicy lub Grupy mają prawo logowania się jako klienci Usług Zdalnych. To prawo jest wymagane dla użytkowników Zdalnych Pulpitów. Jeżeli Pomoc Zdalna jest umywana tylko administratorzy powinni mieć to prawo.</p> <p>UWAGA: Nie jest konieczne dodawanie jakichkolwiek użytkowników lub grup aby umożliwiać oferty RA.</p>	<nikt>
<p>Deny logon through Terminal Services</p> <p>Ustala, którzy użytkownicy lub Grupy mają zakaz logowania się jako klienci Usług Zdalnych. To prawo jest używane dla użytkowników Pulpitów Zdalnych</p>	<nikt>

Dodatkowo, aby zezwolić na Oferty Pomocy Zdalnej, poniższe opcje polisy grupowej muszą również być ustawione:

- § Otwórz GPO w przystawce Polisy Grupowe przez MMC lub wejdź w połączony GPO przez zakładkę Właściwości —> Polisy Grupowe
- § Jeżeli dostęp uzyskano przez zakładkę Polisy Grupowe podświetl żądany GPO i kliknij przycisk Edytuj aby przejść do przystawki Polisy Grupowe

- § Przejdź do zakładki Computer Configuration\Administrative Templates\System\ Remote Assistance
- § Kliknij dwukrotnie na ustawieniu Zapowiedziana Pomoc Zdalna w prawym panelu i Kliknij przycisk radiowy Włączone aby umożliwić użytkownikom prośby o pomoc zdalną a Wybierz "Zezwalaj pomocnikom tylko na podgląd komputera" z rozszerzanego menu.
- § Ustaw maksymalny czas (wartość) na 0 i maksymalny czas (jednostki) na minuty.
- § Zastosuj ustawienia i zamknij okno



UWAGA: Konieczne jest włączenie Zapowiedzianej Pomocy Zdalnej aby Oferty Pomocy Zdalnej mogły funkcjonować. Jednakże, ustawienie maksymalnego czasu biliciku na 0 zapobiegnie używaniu Zapowiedzianej Pomocy Zdalnej

- § Kliknij dwukrotnie na Oferty Pomocy Zdalnej po prawej stronie.
- § Kliknij przycisk radiowy "Włączone" jeżeli planujesz udostępnić ekspertom oferty pomocy z tego komputera.
- § Wybierz "Zezwalaj pomocnikom tylko na podgląd komputera" rozszerzanego menu.
- §



Uwaga: Zaleca się brak możliwości zarządzania systemem przez inne osoby wykonujące to zdalnie. Jednakże istnieje możliwość by użytkownicy mieli podgląd swojego komputera I wykonywali wszelkie operacje zdalnie.

- § Kliknij przycisk Pomocnicy Pokaż. i wprowadź listę użytkowników mogących udzielić pomocy tej maszynie, np. administratorzy, personel pomocniczy. Zaleca się zminimalizowanie listy osób tylko do tych, którzy są niezbędni. Użytkownicy powinni być wypisani w następującym formacie:

<Domain Name>\<User Name> or <Domain Name>\<Group Name>

Połączenie zdalne pulpitów

Pulpit Zdalny (RD) jest limitowaną wstawką Usług Zdalnych dostępnych na Windows XP Professional. Pozwala ona na połączenie do klienta ze zdalnej lokalizacji i używanie zasobów tak jakby były fizycznie podłączone do komputera klienta. RD jest domyślnie wyłączone w systemach Windows XP Professional.

Pouczenia RD są realizowane poprzez oprogramowanie klienckie. Jest ono domyślnie instalowane przy instalacji XP a klienci dla Windows 2000, NT, 98, 95 są dołączone do Windows XP. Istnieje również klient bazujący na ActiveX znany jako Pouczenie Sieciowe do Zdalnego Pulpitu (RDWC) który może być zainstalowany tylko na serwerach z IIS. Używając RDWC, komputer mający przeglądarkę obsługującą ActiveX może połączyć się ze stroną www, pobrać klienta ActiveX i wtedy zestawiać pouczenie RD nawet jeżeli nie ma zainstalowanego klienta

Usług Zdalnych na komputerze. RDWC jest domyślnie instalowany przy instalacji IIS na Windows XP Professional.

Gdy RD jest włączone port 3389 jest otwarty aby umożliwić dostęp do usług zdalnych. Wszyscy administratorzy (lokalni i domen) i użytkownicy/grupy wpisani do grupy "Użytkownicy Zdalnego Pulpitu" mogą połączyć się zdalnie z tym komputerem. Gdy Pouczenie jest zrealizowane komputer klienta jest rozpoznawany na podst. listy uwierzytelniającej użytej przy zestawianiu pouczenia. Gdy użytkownik jest połączony, gdy kolejny stara się połączyć, ten drugi ma możliwość rozłączenia pierwszego z jego sesji i wylogowania, ale tylko PO udanej autoryzacji i tylko gdy jest to Administrator.

RD używa standardowych mechanizmów autoryzacji Windows, jednakże polisy haseł i kont są stosowane do RD. Wszystkie konta użyte do połączeń RD muszą mieć ustawione hasła.



UWAGA: Możliwe jest zablokowanie konta administratora przez pouczenie zdalne i uniemożliwienie logowania się na to konto zdalnie. To konto może być używane jedynie do logowania lokalnego

Aby używać Zdalnego Pulpitu, następujące zmiany muszą być wprowadzone do Praw Użytkowników we wprowadzonym szablonie zabezpieczeń

Prawa Użytkowników	Zalecane Ustawienia
Zezwalaj na logowanie poprzez Usługi Terminalowe Określa którzy użytkownicy lub grupy mają prawo logowania poprzez usługi terminalowe. Jest to konieczne dla użytkowników zdalnego pulpitu. Jeśli korzysta się z Asystenta Zdalnego jedynie Administratorzy powinni mieć takie prawa	Administratorzy, Użytkownicy zdalnego pulpitu
Zabraniaj logowanie poprzez Usługi terminalowe Określa, którzy użytkownicy nie mają prawa (jest im to zabronione) na korzystanie z Usług Terminalowych.	<Nikt>

Aby włączyć komputer do akceptacji połączeń Zdalnego Pulpitu, wykonaj poniższe czynności:

- § Kliknij prawym klawiszem myszy na Mój Komputer i wybierz Właściwości aby otworzyć okno Właściwości Systemu.
- § Wybierz zakładkę Zdalne w oknie dialogowym.
- § Zaznacz "Zezwalaj użytkownikom na połączenia zdalne do tego komputera"
- § Kliknij Wybierz Zdalnych Użytkowników... aby otworzyć okno Użytkownicy Zdalnego Pulpitu.
- § Dodaj użytkowników lub grupy



UWAGA: Ten proces doda zaznaczonych użytkowników i grupy do lokalnej grupy "Użytkowników Pulpitów Zdalnych". Użytkownicy i grupy mogą być dodawani bezpośrednio używając lokalnego Menadżera Systemu

Usługi Terminalowe

Dodatkowo do powyższych opcji zaleca się zastosowanie poniższego przewodnika do Usług Zdalnych jako część Obiektów Polis Grupowych (GPO) lub poprzez konfiguracje komputera lokalnego.

Te zalecenia zastosowane do rozszerzenia Usług Zdalnych zlokalizowanych w Computer Configuration\Administrative Templates\Windows Components\Terminal Services poprzez GPO i dostęp do nich jest możliwy przez przystawkę MMC Polis Grupowych. Ustawienia Usług Zdalnych widocznych pod Konfiguracją użytkownika są nadpisywane przez te ustawienia Konfiguracji Komputera.

Opcje Terminala Polis Serwisowych	Zalecane Ustawienia
Ograniczaj użytkowników do jednej sesji zdalnej Ogranicza użytkownika do jednej sesji zdalnej. Domyślnie Serwer Terminala zezwala na nieograniczoną liczbę aktywnych lub wyłączonych sesji jednego klienta	Włączone
Ograniczaj ilość połączeń To ustawienie ogranicza liczbę jednoczesnych połączeń do Serwera Terminala.	Maksymalna liczba
Nie pozwalaj na nowe pouczenia klientów Gdy jest włączone, serwer będzie akceptował nowe połączenia aż osiągnie limit ustawiony wyżej. Jeżeli jest włączone usługa Zdalnego Pulpitu jest praktycznie wyłączona, z wyjątkiem możliwości użytkowników do ponownego połączenia do rozłączonej sesji.	Nie konfigurowane
Nie zezwalaj lokalnym administratorom na zmiany zezwoleń Wyłącza prawa administratora do zmian zezwoleń zabezpieczeń w narzędziu Konfiguracja Serwera Terminala. Ustawienia zabezpieczeń powinny być ustawione na poziomie domeny a nie przez lokalnego administratora	Włączone
Ustawienia Kontroli Zdalnej Aby używać zdolności Zdalnego Pulpitu to ustawienie musi być włączone. Zaleca się wybranie tylko "Podgląd sesji z zezwoleniem użytkownika", chyba że istotna jest kontrola użytkownika nad sesją innego użytkownika	Włączone = "Podgląd sesji z zezwoleniem użytkownika"
Start programu po pouczeniu Ustawia program, który będzie uruchamiany przy zalogowaniu się użytkownika, obchodząc ustawienia Start Programu przez administratora serwera lub użytkownika	Wyłączone
Nie zezwalaj na przekierowanie schowka Zapobiega przez kopiowaniem i wklejaniem zawartości schowka pomiędzy programami uruchomionymi na komputerze klienta a uruchomionymi na serwerze	Włączone
Nie zezwalaj na przekierowania smart card Zapobiega mapowaniu urządzeń smart card w sesji Usług Zdalnych. Jeżeli jest włączone użytkownik nie może używać urządzeń smart card do zalogowania się do sesji Usług Zdalnych	Wyłączone
Zezwalaj na przekierowanie audio Zezwala użytkownikom na odgrywanie audio z serwera na lokalnym komputerze lub odwrotnie podczas sesji.	Wyłączone
Nie zezwalaj na przekierowania portu COM Zapobiega przed dostępem użytkowników do urządzeń wymagających mapowania portu szeregowego (COM) z sesji Usług Zdalnych.	Włączone
Nie zezwalaj na przekierowania drukarek Zapobiega przed przekazywaniem zadań drukarki serwerowej do drukarki lokalnej.	Włączone
Nie zezwalaj na przekierowanie portu LPT Zapobiega przed dostępem użytkownika do urządzeń wymagających mapowania portu równoległego(LPT) z sesji Usług Zdalnych.	Włączone
Nie zezwalaj na przekierowania dysków Wyłącza mapowanie dysków klienta w sesji Usług Zdalnych	Włączone
Nie ustawiaj domyślnej drukarki klienta jako domyślnej danej sesji Gdy Włączone, domyślna drukarka ustawiona przez klienta nie będzie domyślną drukarką sesji Usług Zdalnych. Domyślną drukarką będzie ustawiona na serwerze	Włączone

Opcje Terminala Polis Serwisowych	Zalecane Ustawienia
Zawsze pytaj o hasło przy połączeniu Wymaga od użytkownika podania hasła przed rozpoczęciem sesji ze zdalnym serwerem. Zapobiega przed ubyciem zapisanych list uwierzytelniających.	Włączone
Ustaw poziom szyfrowania połączenia Ustawia parametry szyfrowania połączeń serwera z klientem. Są dwie opcje: "Kompatybilna z Klientem" i "Poziom Wysoki". Kompatybilna z klientem szyfruje dane z maksymalną długością klucza obsługiwaną przez klienta. Poziom wysoki używa 128-bitowego klucza UWAGA: Komputer użytkownika musi pracować na 128-bitowym oprogramowaniu TS aby nawiązać połączenie z serwerem, który używa wysokiego poziomu. Klienci, którzy nie obsługują takiego poziomu szyfrowania nie mogą się połączyć.	Włączone = "Poziom Wysoki"
Nie używaj folderów tymczasowych w sesji Zezwolenie na tworzenie tymczasowych folderów dla każdej sesji, która wspiera serwer. Taki zabieg redukuje ryzyko do dostępu do danych wspólnie składowanych.	Wyłączone
Nie kasuj folderów tymczasowych po wyjściu Zezwala na tworzenie folderów tymczasowych dla każdej obsługiwanej sesji. Tworzenie oddzielnych folderów redukuje ryzyko nieprawidłowego dostępu do danych. UWAGA: Foldery nie są usuwane po rozłączeniu sesji, lecz po jej zamknięciu przez wylogowaniu z niej.	Wyłączone
Ustaw limit czasu na rozłączenie sesji Ogranicza limit czasu rozłączonej sesji zanim zostanie ona zamknięta. W tym stanie programy/procesy, które klient uruchomił przed rozłączeniem będą działały nawet po zerwaniu połączenia z klientem.	Włączone = a0 min.
Ustaw limit czasu aktywnej sesji Ogranicza czas w jakim może istnieć aktywna sesja. Jeżeli ustawiono na "Nigdy" nie ma ograniczenia długości sesji.	Włączone = "nigdy"
ustaw limit czasu bezczynności sesji Ogranicza czas, jak długo może istnieć bezczynna, nierozłączona sesja. Taka sesja wskazuje na możliwość odejścia użytkownika od komputera dając możliwość innym do wykorzystania ich sesji jeżeli komputer nie jest zablokowany.	Włączone = a5 min.
Zezwalaj na ponowne połączenie tylko od oryginalnego To ustawienie obowiązuje tylko klientów Citrix ICA i jest ignorowane przez klientów Windows	Nie dostępne
Zakończ sesje gdy upłynął limit czasu Determinuje rozłączenie lub zamknięcie sesji po upływie limitu czasu. Gdy włączone wszystkie sesje są zamykane po upływie limitu.	Włączone

Tabela 16 Opcje Terminala Polis Serwisowych

Zalecenia konfiguracji sieci

Pomoc Zdalna i Zdalny Pulpit używają usług zdalnych do udostępnienia pomocy klientowi. Te usługi używają portu 3389 w systemie Windows XP. Wyjątkowo zaleca się używanie tych połączeń tylko w lokalnym intranecie i blokowanie tego portu przez firewall lub router filtrujący. Połączenia przychodzące i wychodzące muszą być zablokowane aby uniemożliwić dostęp z zewnątrz. W przypadku zablokowania tylko połączeń przychodzących wciąż możliwe jest nawiązanie pomocy zdalnej poprzez Windows Messenger. Te połączenia są realizowane poprzez obu klientów inicjujących połączenia wychodzące do serwera messenger dlatego pomoc w obu kierunkach musi być zablokowana.

Jeżeli wymagane są połączenia RA lub RD z zewnętrzną siecią LAN zaleca się filtrowanie połączeń przez firewall lub router aby umożliwić dostęp tylko wybranym adresom IP. Wszystkie inne adresy powinny mieć zakaz dostępu przez port 3389. Dla wyższych poziomów zabezpieczeń ustaw serwer VPN i wymagaj bardzo długiego wieloznakowego hasła dla bardzo ograniczonej liczby osób które mają dostęp do tego VPN. Generalnie dobrym pomysłem jest zezwalanie tylko podanym adresom IP na pomoc do tego serwera VPN.

Konfiguracja Firewall

Firewall (IGF) zapewnia podstawową ochronę komputera przed atakami z zewnątrz. Używa statycznej inspekcji pakietów do zatrzymywania zewnętrznych pakietów zanim dotrą do klienta, chyba, że są odpowiedzią na żądanie klienta. Wszystkie inne są zostawiane w domyślnym ustawieniu konfiguracyjnym.

Ten rozdział daje podstawowy pogląd na ustawienia zabezpieczeń dostępnych z IGF.

Zalecane stosowanie

Firewall nie jest z zamierzenia na tyle elastyczny aby używać go w ustawieniu sieci. IGF nie będzie normalnie pracował w sieci, gdzie klient jest jej częścią, lub komputer klienta udziela usług. Kilka przykładów usług: współdzielenie plików i drukarek, serwery www i ftp. W tych przypadkach powinien być użyty dedykowany firewall aby wprowadzić ustawialny poziom zabezpieczeń.

Są sytuacje, w których IGF daje dodatkową ochronę komputera klienta. Tak się dzieje, gdy komputer jest bezpośrednio podłączony do internetu lub innej sieci. Laptopy podłączone do DSL, modemu lub do innej sieci podczas podróży zyskają na IGF.

Cechy

IGF chroni komputer klienta na trzy różne sposoby: statyczna inspekcja pakietów, zabezpieczenie przed skanowaniem portów i logowanie. Ta część ogólnie wyjaśnia każdy sposób.

Styczna inspekcja pakietów

IGF używa statycznej inspekcji pakietów, która zawiera tabele wszystkich aktywnych połączeń inicjowanych przez klienta i porównuje przychodzące pakiety. Jeżeli są one odpowiedzią na żądanie klienta to są dozwolone. Jeżeli nie zainstalowano dodatkowego filtra połączeń niezapowiedzianych reszta jest zakazana.

Zabezpieczenie przed skanowaniem portów

W przypadku używania domyślnej konfiguracji, komputer nie będzie widoczny dla większości skanerów portów. Jeżeli zmieniono konfigurację aby umożliwić pouczenia zewnętrzne widziane będą tylko te porty, które zostały otwarte w tabeli zaawansowanych ustawień.

Wiele skanerów dokonuje ICMP ping aby sprawdzić istnienie hosta zanim dokona skanowania portu. Domyślnie pingi również są opuszczane i chroniony komputer może być pominięty nawet gdy ma otwarte porty.

Logowanie

IGF może być skonfigurowany do logowania prób połączeń. Możesz wybrać pomiędzy logowaniem udanych połączeń, opuszczonych pakietów lub obu. Nie ma więcej opcji co do informacji logowanych w pliku.

Czego nie oferuje ICF

IGF może jedynie zapewnić filtrowanie pakietów przychodzących. Nie można ograniczyć typu danych wychodzących z komputera klienta. To oznacza, że ICF nie może ograniczyć celów, z którymi komputer lokalny może się połączyć.

Ustawienia ICF, które pozwalają na zewnętrzne połączenia nie nakładają restrykcji na to, kto może się połączyć. Nie pozwoli ci uzyskać dostępu lub zabronić dostępu z określonych lokalizacji, użytkowników lub sieci. Jeżeli usługa jest włączona daje dostęp każdemu. Jeżeli jest wyłączona zabrania dostępu każdemu. Można jednak użyć filtru IP do ograniczania połączeń przychodzących lub wychodzących.

Włączenie ICF

Poniższe warunki muszą być spełnione przed włączeniem ICF:

- § Musisz mieć prawa administratora
- § ICF nie może być zabroniony w polisie grupowej.



UWAGA: Włączenie Zapory Ogniowej dla połączenia internetowego z domyślnymi ustawieniami może doprowadzić do wyłączenia udostępniania folderów i drukarek, jak również do przeglądania Moje Otoczenie Sieciowe. Zobacz <http://support.microsoft.com/support/kb/articles/Q298/8/04.a> by uzyskać więcej informacji

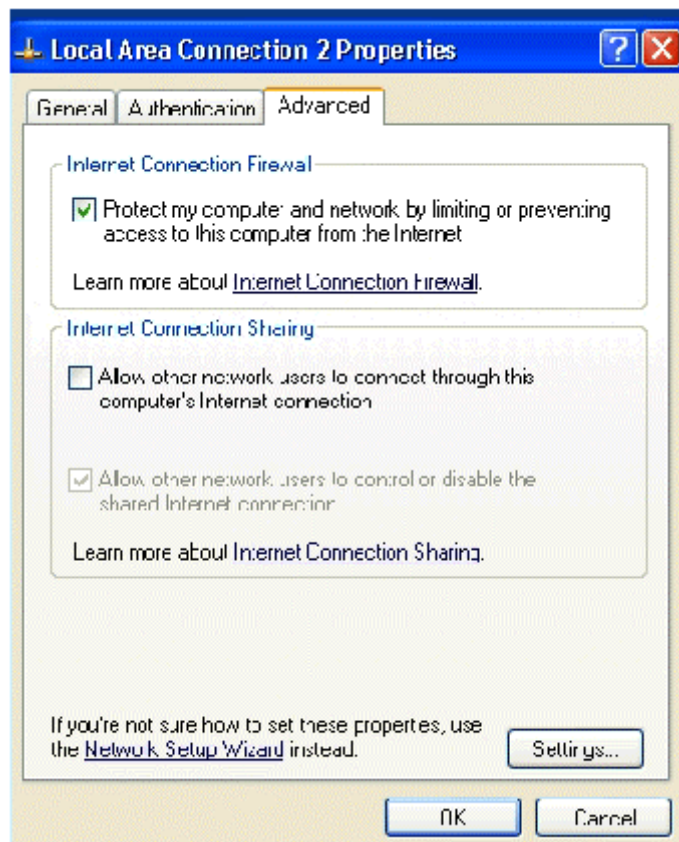
ICF musi być skonfigurowany i włączony na każdym interfejsie, na którym będzie pracował. Jeżeli użyłeś kreatora Ustaw Sieć Domową lub Małe Biuro z panelu Zadań Sieciowych lub z kreatora Nowych Połączeń Sieciowych, Firewall może być włączony domyślnie. Ten kreator włączy ICF w przypadku dwóch opcji:

- Ten komputer łączy się bezpośrednio lub przez huba. Inne komputery mojej sieci również łączą się do internetu bezpośrednio lub przez huba.
- Ten komputer łączy się bezpośrednio. Nie mam jeszcze sieci.

Jeżeli interfejs sieciowy był ustawiony w inny sposób lub ICF nie był włączony może zostać uruchomiony przez wykonanie poniższych czynności:

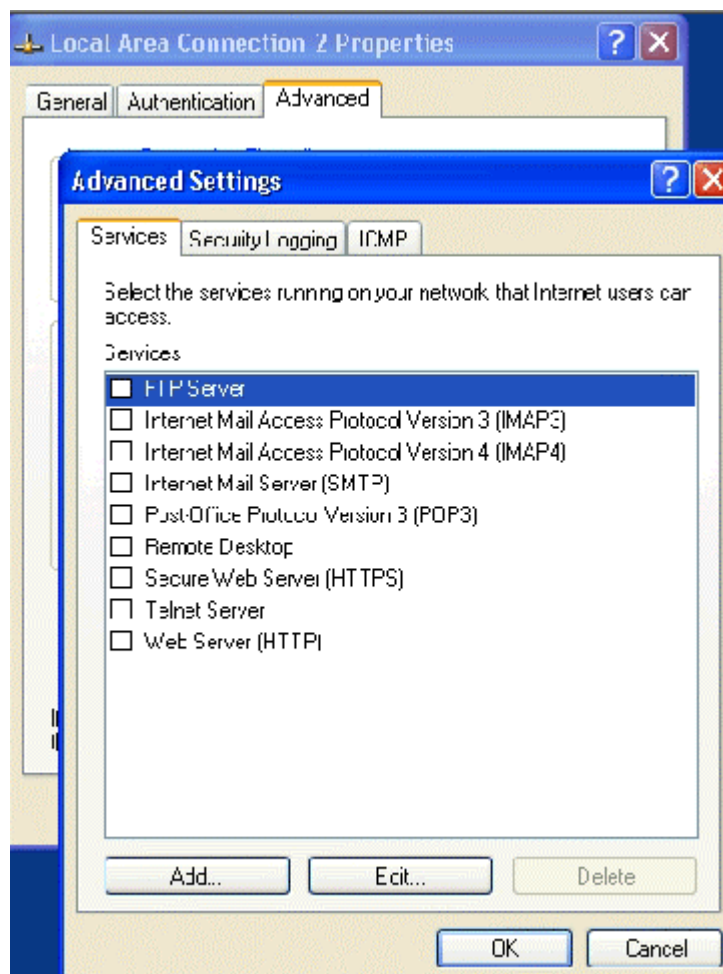
- § Panel Sterowania —Sieci
- § Kliknij prawym przyciskiem myszy na interfejsie pouczenia i wybierz właściwości z rozszerzanego menu
- § Kliknij zakładkę Zaawansowane

Kliknij na Chroń mój komputer i sieć przez limitowanie lub zakaz dostępu do tego komputera z internetu. Patrz Rys. 14. To uaktywni ICF w domyślnej konfiguracji.



Rys. 14 Włączanie ICF

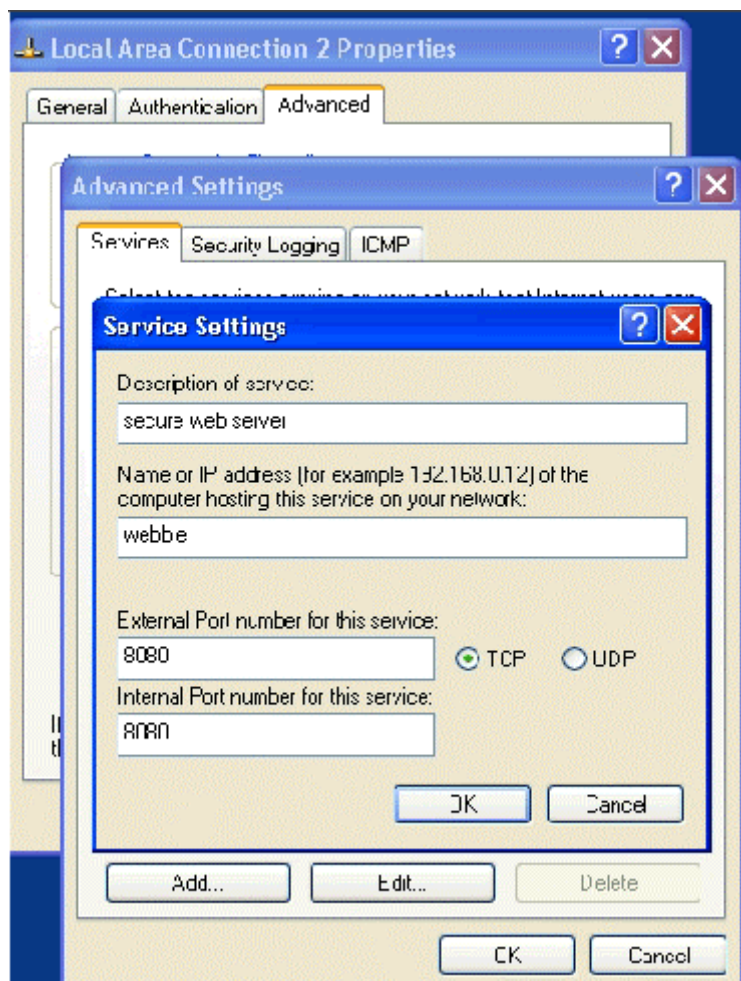
- § Jeżeli chcesz zmienić ustawienia firewall kliknij Ustawienia. To uruchomi interfejs z trzema zakładkami: Usługi, Logowanie i ICMP.



Rys 15. Zakładka Usługi

Zakładka Usługi na Rys 15 ukazuje domyślne opcje dostępne dla najczęstszych usług. Wybierz dowolną a ukaze się okno do wpisania nazwy lub adresu komputera, na którym ta usługa pracuje. O ile nie ubywasz komputera jako bramy dla innych komputerów, wpis powinien opisywać nazwę komputera na którym pracuje ICF.

Możesz dodać następane usługi klikając na Dodaj... i wpisując informacje dla tej usługi. Na przykład, aby dodać serwer www na port 8080, wpis może wyglądać jak Rys. 16

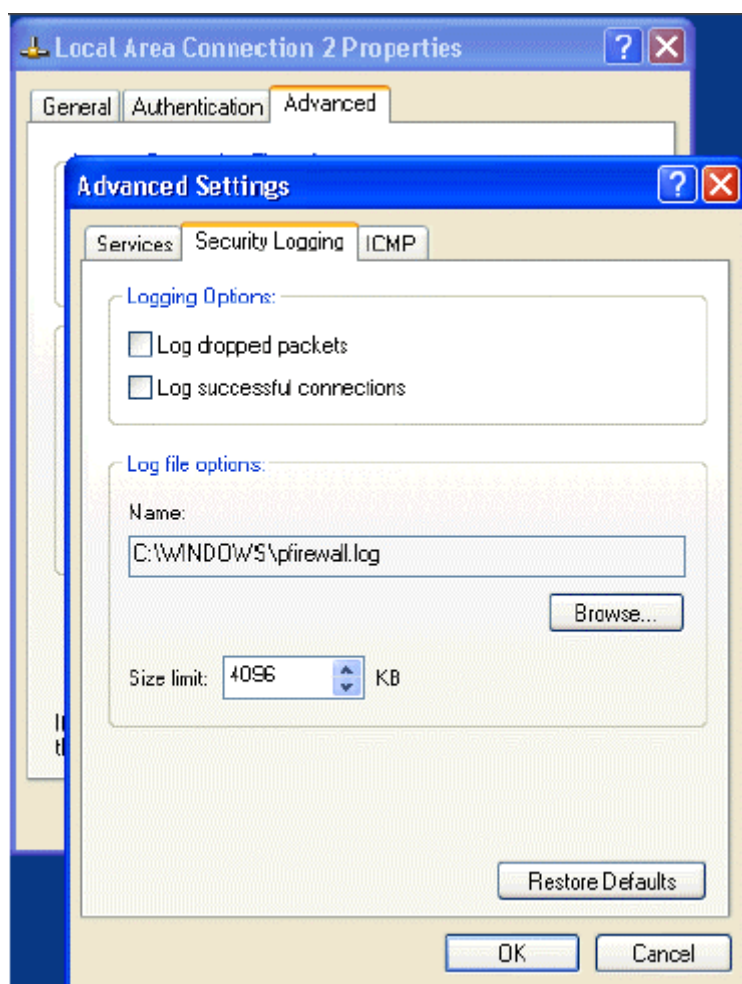


Rys. ą6 Przykładowe ustawienie usługi



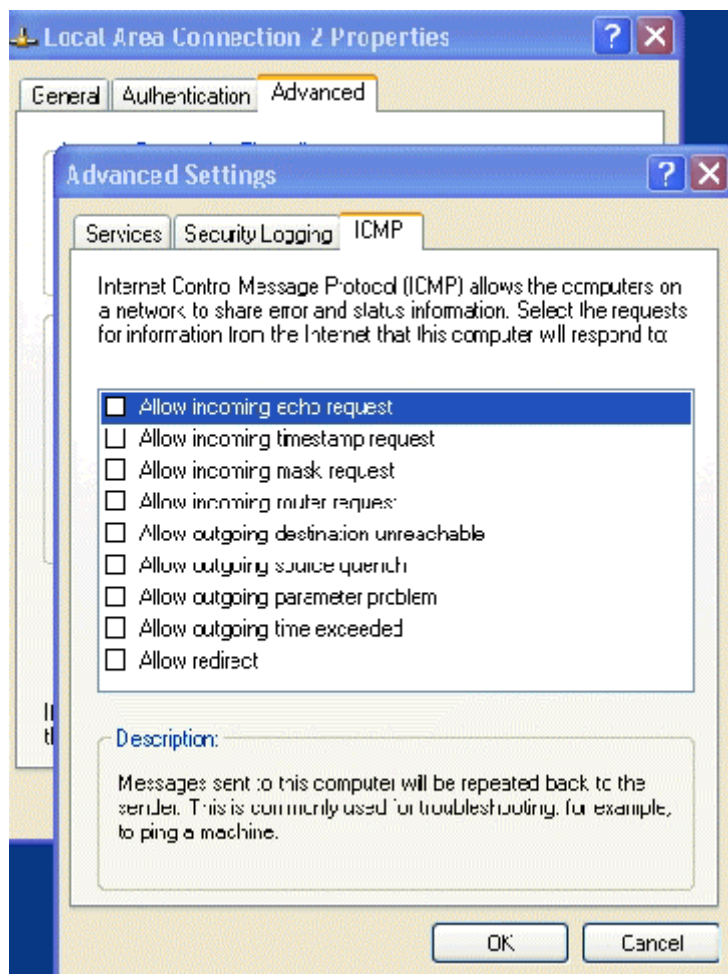
UWAGA: Jeżeli używasz DHCP aby dostać adres sieciowy, powinieneś użyć w tych formularzach nazwy komputera a nie adresu IP, ponieważ nie ma gwarancji, że te adresy będą stałe.

Zakładka Logowanie pozwala ustawić logowanie aktywności ICF. Możesz wybrać logowanie opuszczonych pakietów, udanych połączeń lub obu. Masz także wybór dotyczący lokalizacji pliku log i jego maksymalnej wielkości. Po osiągnięciu maksymalnej wielkości najstarsze wpisy są zastępowane nowymi. Nie ma możliwości automatycznej archiwizacji plików. Rys. 17 ukazuje opcje logowania.



Rys. 17 Zakładka Logowanie

Zakładka ICMP pozwala wybrać różne typy dozwolonych wiadomości ICMP. Inaczej niż usługi TCP/UDP, sekcja ICMP jest podzielona na pakiety przychodzące i wychodzące. Pakiety ICMP mogą być użyte do zbierania informacji o twojej sieci. Zaleca się nie włączanie żadnej z tych wiadomości, chyba że jest to konieczne. Rys. 18 ukazuje opcje ICMP.



Rys. 18 Zakładka ICMP

Podsumowanie

Firewall wprowadza podstawową ochronę komputera. Ta ochrona jest ograniczona do nowych połączeń przychodzących, ponieważ nie ma restrykcji na połączenia zainicjowane przez lokalną maszynę lub odpowiedzi na lokalne żądania. Domyślna konfiguracja blokuje wszystkie pouczenia przychodzące i dostarcza niewielką ochronę przed skanerami portów. Indywidualne usługi mogą być udostępnione przez ICF otwierając przypisany port ale nie ma możliwości wyboru. Ruch jest dozwolony lub zabroniony; nie można filtrować na podstawie zawartości lub adresu IP. Jeżeli komputer obsługuje te usługi, powinien stać za mocniejszym firewallem niż ICF.

ICF jest użyteczny w kilku sytuacjach, np gdy komputer nie jest częścią sieci i jest połączony bezpośrednio do internetu, gdy łączymy się z firmowym Serwerem Dostępu Zdalnego. Zauważ, że w środowiskach gdzie używany jest IPSec, ICF musi być wyłączony. W przeciwnym razie klient nie będzie w stanie wynegocjować polityki IPSec i nie będzie mógł nawiązać żadnego pouczenia sieciowego.

Ta strona zostawiona celowo pusta

Dodatkowe ustawienia Zabezpieczeń

Obok opcji zabezpieczeń konfigurowanych przez szablony zabezpieczeń, kilka innych pokrewnych ustawień powinno być skonfigurowanych. Ten rozdział ukazuje te ustawienia.

Zalecenia kont administratorów

W związku z ich siłą, konta administratorów powinny być szczególnie strzeżone w środowisku Windows. Ta część omawia kilka dodatkowych zaleceń związanych z kontami z przywilejami administratora.

Dodatkowe Konta Administratorów

Podczas instalacji Windows XP, jeżeli użytkownik wybrał instalację XP jako pojedynczego systemu w przeciwieństwie do członka domeny, będzie pytany "Kto będzie używał tego komputera?" i o wpisanie przynajmniej jednego konta użytkownika. Nie będzie możliwa dalsza instalacja bez podania co najmniej jednego konta. Jakikolwiek konta dodane tutaj automatycznie będą miały przypisane puste hasło i będą członkami grupy administratorów. Jednakże, pomimo wpisania tylko jednej nazwy użytkownika będą dwa konta administracyjne: wbudowany Administrator i ten wpisany przez użytkownika. Windows XP potrzebuje dodatkowego administratora, ponieważ nie jest zalecane logowanie lokalne przy ubyciu wbudowanego konta. Z drugiej strony, w środowisku domeny dodatkowe konto administracyjne sprawia potencjalne ryzyko. W Windows XP, lokalni użytkownicy z pustymi hasłami nie mogą logować się przez sieć, tylko lokalnie. Dlatego, w środowisku domeny zaleca się usunięcie dodatkowego konta stworzonego podczas instalacji i upewnienie się, że wbudowany administrator ma dobre hasło. Jeżeli potrzebne jest dodatkowe konto administracyjne upewnij się, że ma odpowiednio silne hasło.

Aby usunąć konto użytkownika:

- § Wybierz Panel Sterowania—> Konta Użytkowników
- § Kliknij na koncie(-ach) do usunięcia
- § Kliknij Usuń konto

Konta użytkowników mogą być również usunięte przez poniższe kroki:

- § Wybierz Start ->•Programy - Narzędzia administracyjne—Manager Komputera
- § Rozszerz Użytkownicy i Grupy Lokalne
- § Kliknij podwójnie na Użytkownicy
- § W prawym panelu kliknij prawym klawiszem myszy na użytkowniku do usunięcia
- § Wybierz Usuń z rozwiniętego menu

Używanie konta administratora I komendy Uruchom Jako

Administratorzy powinni mieć dwa konta: jedno administracyjne i jedno zwykłego użytkownika. Konto administracyjne i listy uwierzytelniające powinny być używane tylko w razie potrzeby, a do codziennych zadań powinno być używane normalne konto użytkownika. Administratorzy nie powinni przeglądać internetu na koncie administracyjnym, gdyż różne części kodu działają w kontekście z zalogowanym użytkownikiem.

Do wykonania zadań wymagających praw administratora może być użyta komenda Uruchom Jako.... Ta komenda pozwala uruchamiać programy zwykłemu użytkownikowi jako inny użytkownik. Wpisanie runas /? w linii komend wypisze listę opcji komendy. Użyj poniższej składni:

```
runas /user: nazwa_domeny\konto_administratora nazwa_programu
```

Komenda Uruchom Jako może również być uruchomiona przez skrót w menu, wykonując poniższe kroki:

- § z menu Start przejdź do odpowiedniej aplikacji
- § Trzymając SHIFT kliknij prawym przyciskiem myszy na aplikacji
- § Wybierz Uruchom Jako z rozwiniętego menu
- § Kliknij opcje Następujący użytkownik:
- § Wpisz lub wybierz Nazwę użytkownika
- § Wpisz hasło
- § Kliknij OK.



UWAGA: Właściwość UruchomJako wymaga uruchomienia usługi Secondary Logon na Windows XP lub Uruchom Jako na Windows 2000. Usługi te są uruchamiane domyślnie

Patrz the Microsoft Knowledge Base article G294676 at <http://support.microsoft.com/support/kb/articles/Q294/6/76.asp> po więcej informacji na temat używania komendy Uruchom Jako.

Zezwolenia współdzielonych źródeł

Współdzielony Windows oznaczają, które pliki, foldery, drukarki i inne zasoby mogą być dostępne do zdalnego dostępu dla użytkowników sieci. Zwykli użytkownicy nie mogą tworzyć współdzielonych na ich komputerach; tylko administratorzy i Użytkownicy Zaawansowani mogą to zrobić pod warunkiem, że mają co najmniej prawa do odczytu danego katalogu.. Każdy użytkownik mający prawo Create Permanent Shared Objects również może tworzyć współdzielony. Ponieważ mogą one zawierać ważne dane i mogą stanowić okno do wnętrza sieci, powinny być tworzone z dbałością o zabezpieczenia.

Poniższe prawa mogą być dostępne lub zabronione dla użytkowników lub grup:

- § Pełna Kontrola
- § Zmiana
- § Odczyt

Prawa współudziałów są nadawane niezależnie od praw NTFS. Jednakże działają wspólnie z prawami NTFS. Podczas uzyskiwania dostępu do udziału zastosowane będzie bardziej restrykcyjne prawo. Na przykład, jeżeli użytkownik uzyskuje dostęp do udziału, do którego ma Pełną Kontrolę, ale jednocześnie tylko odczyt na NTFS, dostanie tylko odczyt do danego udziału.

Domyślnie wszyscy mają prawo Pełnej kontroli jednakże musisz wybiórczo edytować prawa dostępu aby limitować ten udział. To oznacza, że prawa NTFS będą najczęściej używane do ustawienia praw dostępu do poszczególnych zasobów. Jeżeli z jakiegoś powodu użytkownicy uzyskujący dostęp do udziału lokalnie powinni mieć większe prawa niż użytkownicy zdalni możesz użyć praw dostępu aby bardziej ograniczyć ich dostęp. Miej na względzie, że restrykcje nałożone przez prawa dostępu do udziałów nie działają na użytkowników zalogowanych lokalnie lub przez Dostęp Zdalny. Z tego powodu dobrze jest ustawić dobre prawa dostępu przez NTFS.



UWAGA: Gdy proste Współdzielenie Plików jest wyłączone (tak jak w przypadku dołączenia Windows XP do domeny), Windows XP nie pozwala dzielić folderów Documents and Settings, Program Files i katalogu systemowego, tak jak folderów wewnątrz folderu systemowego.

Ustawianie Praw Dostępu

Aby stworzyć udział i ustawić prawa dostępu:

- § W eksploratorze, kliknij prawym przyciskiem myszy na folderze, który ma być współdzielony
- § Wybierz opcje menu Udostępnianie i Zabezpieczenia..
- § Kliknij przycisk radiowy Udostępnij ten folder
- § Ustaw nazwę udziału
- § Kliknij przycisk Prawa Dostępu
- § Dodaj, usuń lub edytuj listę użytkowników i/lub grup dla danego udziału



UWAGA: Jeżeli włączone jest Proste Współdzielenie Plików ten dialog będzie zupełnie inny. W tym przypadku wszyscy użytkownicy logują się jako Goście nie zaleganie od listy uwierzytelniających.

Zalecenia Zabezpieczeń Udziałów

Podczas tworzenia udziałów i praw dostępu, stosuj się do poniższych kryteriów gdy możliwe:

- § Upewnij się, że grupa Wszyscy nie ma praw do żadnego udziału
- § Użyj Uwierzygodnieni Użytkownicy lub grupy użytkowników zamiast grupy Wszyscy
- § Daj Użytkownikom i/lub grupom minimalne prawa wymagane dla udziału
- § Do ochrony walnych, nie do powszechnego użytku udziałów, ukryj je dodając \$ po nazwie udziału przy jego tworzeniu. Użytkownicy nadal mogą połączyć się do ukrytych udziałów lecz musi podać pełną ścieżkę dostępu do niego (np. udział nie będzie widoczny w Otoczeniu Sieciowym)

Usuwanie kluczy rejestru POSIX

Jak było stwierdzone wcześniej, podsystem POSIX nie wchodzi w skład systemu Windows XP. Pomimo to nadal istnieją dwa klucze rejestru POSIX. A w zasadzie jeden HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems\Posix jest przypisany do %katalog systemowy%\systemł2\psxs.exe, pliku który nie istnieje w Windows XP. Jednakże zaleca się usunięcie wartości tego klucza poprzez wykonanie poniższych kroków:

- § W edytorze rejestru, regedit, przejdź do klucza HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystems
- § W prawym panelu wybierz wartość Opcjonalne
- § Z menu Edycja wybierz Usuń
- § W oknie pytającym o potwierdzenie kliknij przycisk "Tak"
- § Powtórz ten proces dla wartości klucza posix, również w kluczu Subsystems

Dodatkowe ustawienie polis grupowych

Ta część zaleca kilka ustawień zabezpieczeń możliwych do wprowadzenia przez Polisy Grupowe. Polisa Grupowa może być zastosowana do Windows XP niezależnie od tego, czy komputer jest częścią domeny Aktywnych Katalogów. Oczywiście Polisa Grupowa może być dodana do Windows XP przez kontroler domen Windows 2000. Aby uzyskać dostęp do GPO:

- § Otwórz GPO w przystawce Polisy Grupowe poprzez MMC lub dostań się do połączonego GPO przez zakładkę Właściwości — Polisy Grupowe.
- § wszedłś przez zakładkę Polisy Grupowe, podświetl wymagany GPO i kliknij przycisk Edytuj aby dostać się do przystawki Polisy Grupowe

Wyłączanie Zdalnej Pomocy/Pulpitu

Jak wszystkie technologie zdalnej kontroli, Pomoc Zdalna i Zdalny Pulpit mają wpływ na zabezpieczenia połączone z ich użyciem. Zaleca się nie używanie technologii zdalnej na sieci operacyjnej, gdzie wymagany jest najwyższy poziom zabezpieczeń.

Aby wyłączyć używanie Pomocy Zdalnej, poniższe ustawienia Polisy Grupowej muszą być ustawione:

- § Przejdź do gałęzi Computer Configuration\Administrative Templates\System\ Remote Assistance\
- § Kliknij dwukrotnie na ustawieniu Zapowiedziana Pomoc Zdalna w prawym panelu.
- § Kliknij przycisk radiowy Wyłączone aby nie pozwolić użytkownikom na prośby o pomoc zdalną.
- § Zastosuj ustawienia i zamknij okno.
- § Kliknij dwukrotnie na ustawieniu Oferty Pomocy Zdalnej w prawym panelu.

Kliknij przycisk radiowy Wyłączone aby uniemożliwić ekspertom oferty pomocy zdalnej dla tego komputera.

Zastosuj ustawienia i zamknij okno.



UWAGA: Ustawienia polityki grupowej obchodzą wszystkie inne ustawienia w zakładce Właściwości Systemu/Zdalne i zapobiegną używaniu tych zdolności przez użytkowników nawet jeżeli zostały wybrane we Właściwościach Systemu.

Aby wyłączyć akceptacje Połączeń Zdalnego Pulpitu, wykonaj następujące kroki:

- § Kliknij prawym klawiszem myszy na Mój komputer i wybierz Właściwości aby otworzyć okno Właściwości Systemu.
- § Wybierz zakładkę Zdalne w oknie dialogowym
- § Upewnij się, że nie jest zaznaczone Zezwalaj na połączenia zdalne do tego komputera.
- § Kliknij Wybierz Zdalnych Użytkowników... aby otworzyć okno Użytkownicy Zdalnego Pulpitu.
- § Usuń wszystkich użytkowników i grupy z grupy Użytkowników Pulpitu Zdalnego.

Inicjalizacja Sieci

Domyślnie, Windows XP nie czeka na inicjalizację całej sieci aby rozpocząć logowanie użytkownika. Zamiast tego zakodowane listy uwierzytelniające są użyte do załogowania obecnych użytkowników, w rezultacie czego jest krótszy czas logowania. Polisy Grupowe są dodawane w tle.

Takie zachowanie owocuje kilkoma wyjątkami polityk, takimi jak Instalacja Software i Przekierowanie Folderów, zajmujących dwa załogowania do poprawnego wprowadzenia. Te wyjątki wymagają przerwania załogowywania jakiegokolwiek użytkownika i muszą być przeprowadzone przed rozpoczęciem pracy użytkownika. Również zmiany polityki użytkownika takie jak dodanie ścieżki profilu lub skryptu logowania mogą zająć dwa logowania zanim zostaną wykryte.

Problem pojawia się z respektu do notatki wygaśnięcia hasła, która nie pojawia się użytkownikowi logującemu się do klientów Windows XP w Windows 2000 lub NT 4.0. Jeżeli użytkownik jest załogowany przez zawartość informacji istniejących w pamięci podręcznej listy uwierzytelniające zanim wprowadzone zostaną polityki Grupowe, wyświetlenie polityki w momencie ostrzeżenia o wygaśnięciu hasła nie nastąpi do następnego załogowania się. Pomimo tego hasło może wygasnąć bez ostrzeżenia użytkownika i tym fakcie.

Ten przewodnik nie zaleca pozwolenia na cacheowanie list uwierzytelniających (Interaktywne logowanie: Liczba poprzednich załogowań wpisanych do cache wynosi 0). Cachowane listy uwierzytelniające nigdy nie powinny być użyte do logowania użytkowników do domeny, zmuszając sieć do pełnej inicjalizacji. W przypadku ustawienia liczby cachowanych loginów na coś innego niż 0, O może spowodować wystąpienie błędów. Patrz Microsoft Knowledge Base article Ołął94 na <http://support.microsoft.com/support/kb/articles/Qłłł/a9/4.asp> po więcej informacji o wygasaniu haseł w Windows XP.

W zasadzie, dobrą praktyką jest upewnianie się, że wszystkie zmiany polityk grupowych dotyczących komputerów są wprowadzone przed logowaniem się użytkowników, aby użytkownik mógł pracować na aktualnym ustawieniu zabezpieczeń. Zaleca się jednak poniższe ustawienia dla polityk grupowych:

Przejdź do opcji Computer Configuration\Administrative Templates\System\Logon

- § W prawym panelu, kliknij dwukrotnie na Zawsze czekaj na sieć podczas uruchamiania komputera i logowania
 - § Kliknij przycisk radiowy Włączone
- Kliknij OK

Wyłączenie Autoodtworzenia Mediów

Autoodtworzenie czyta z napędu w momencie jego włożenia. Domyślnie, Windows XP automatycznie odtwarza wszystkie CD-ROMy włożone do napędu. To pozwala na uruchomienie wykonywalnej zawartości płyty bez ingerencji w ten proces. Autoodtworzenie floppy i dysków sieciowych jest domyślnie wyłączone. Aby wyłączyć autoodtworzenie na wszystkich napędach wykonaj następujące czynności:

- § Przejdź do opcji Computer Configuration\Administrative Templates\System
- § W prawym panelu, kliknij dwukrotnie na Wyłącz Autoodtworzenie
- § Kliknij przycisk radiowy Włączone
- § W rozwijanym menu Wyłącz Autoodtworzenie: wybierz wszystkie napędy
- § Kliknij OK

Blokowanie portów NetBIOS i SMB w obwodzie sieci

W środowisku Windows, NetBIOS wyznacza interfejs programowy i zasady wpisywania nazw. NetBIOS przez TCP/IP (NetBT) zapewnia interfejs programowy poprzez protokół PCP/IP. Windows XP i 2000 używają NetBT do komunikacji z Windows NT i starszymi wersjami Windows (np. 9x). Do komunikacji z innym Windows 2000 lub XP, system wykorzystuje łącze bezpośrednie. Łącze bezpośrednie wykorzystuje DNS, zamiast NetBIOS, do wprowadzania nazw i używa portu TCP 445 zamiast 139. Blok Wiadomości Serwerowych używa współdzielenia zasobów sieciowych bezpośrednio poprzez TCP/IP, bez używania NetBIOS jako "pośrednika".

Komunikacja przez porty NetBIOS i SMB (porty 135-139 i 445) może dostarczyć wielu informacji o systemach i może ułatwić atak na bramę. Dlatego zaleca się zabronienie zewnętrznym systemom na połączenie się do wewnątrz przez te porty.

Zaleca się blokadę przychodzącego ruchu na portach 135,137,138,139 i 445 na routerze i/lub firewallu. Liczba ataków i możliwość wejścia do systemu jest mniejsza jeżeli ruch na portach SMB jest zablokowany.

Modyfikacje dla Windows XP w Domenie Windows NT

Windows XP Professional może być użyty jako klient w domenie Windows NT 4.0. Jednakże kilka modyfikacji ustawień zalecanych w tym przewodniku musi być dokonanych aby Windows XP poprawnie pracował w tym środowisku. Ten rozdział opisuje znane problemy przy dodawaniu klienta Windows XP do domeny zawierającej kontrolery Windows NT 4.0

Brak Polis Grupowych

Windows NT 4.0 nie obsługuje Aktywnych Katalogów, w wyniku czego nie obsługuje Polis Grupowych. Jednakże ustawienia zabezpieczeń mogą być ustawione lokalnie na komputerze z Windows XP przez narzędzie Analiza i Konfiguracja Zabezpieczeń opisane wcześniej w tym dokumencie i /lub poprzez lokalną Polisę Grupową.

Ustawienie NTLM i LanManager'a

W Rozdziale 5, zaleca się aby poziom autoryzacji opcji zabezpieczeń Sieciowych: LAN Manager był: Wyślij tylko odpowiedź NTLMv2\zabraniaj LM i NTLM. Jednakże, podczas pierwszego logowania do domeny NT z klienta XP, ta opcja powinna być ustawiona na Wyślij LM & NTLM - użyj Zabezpieczeń Sesji NTLMv2 jeżeli wynegocjowano. To musi być zrobione dla każdego nowego klienta XP.

- § Start—Uruchom —»gpedit.msc
- § w lewym panelu, przejdź do Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options
- § W prawym panelu, kliknij dwukrotnie na Network Security: LAN Manager Authentication Level
- § Zaznacz Wyślij LM & NTLM - użyj Zabezpieczeń Sesji NTLMv2 jeżeli wynegocjowano. Kliknij OK
- § Zamknij okno Polis Grupowych.

Po pierwszej autentyfikacji zaleca się przywrócenie tego ustawienia na Wyślij tylko NTLMv2\zabraniaj LM i NTLM.

Klucz Strong Session

W Rozdziale 5, zaleca się włączenie opcji zabezpieczeń Członek Domeny: Wymagaj klucza Strong Session (Windows 2000 lub późniejszy). W domenie Windows NT ta opcja musi być wyłączona.

- § Start Uruchom —»gpedit.msc
- § W lewym panelu, przejdź do Computer Configuration\Windows Settings\Security Settings\l_ocal Policy\Security Options
- § W prawym panelu, kliknij dwukrotnie na Członek Domeny: Wymagaj klucza Strong Session (Windows 2000 lub późniejszy)
- § Wybierz Wyłączone
- § Kliknij OK
- § Zamknij okno Polis Grupowych

Autorekrutacja

Domyślnie, Windows XP próbuje automatycznie rekrutować nowe certyfikaty kluczy publicznych. Ta funkcja wymaga Aktywnych Katalogów. W domenie Windows NT 4.0 ta funkcja nie występuje, więc automatyczna rekrutacja nie będzie działała i będzie co pewien czas wpisywać błąd do logów.

Aby wyłączyć autorekrutację, edytuj Lokalną Polisy Grupową Windows XP.

- § Start- Uruchom —gpedit.msc
- § W lewym panelu, przejdź do Computer Configuration\Windows Settings\Security Settings\Public Key Policies
- § W prawym panelu, kliknij dwukrotnie na Ustawienia Autorekrutacji
- § Kliknij Nie rekrutuj certyfikatów automatycznie
- § Kliknij OK
- § Zamknij okno Polis Grupowych

Patrz Microsoft Knowledge Base Article Gł046aat
<http://support.microsoft.com/support/kb/articles/Qł0/46/a .asp> po więcej informacji o tym problemie.

Przykładowy Bander Logon

Użytkownicy DoD używają standardowego baniera ostrzegawczego, który można pobrać z United States New INFOSEG Web Information Service <http://infosec.nosc.mil/infosec.html>. Zaznacz tekst pod United States Department of Defense Warning Statement i skopiuj go do schowka. Ten baner powinien wywołać następującą wiadomość:

"To jest komputer systemu Departamentu Obrony. Ten komputer, włączając powiązany sprzęt, sieć i urządzenia sieciowe (w szczególności dostęp z Internetu) jest przeznaczony tylko dla autoryzowanych użytkowników Rządu U.S. Systemy DoD mogą być monitorowane do celów prawnych, włączając upewnianie się, że ich użycie jest autoryzowane do obsługi systemu, aby wytworzyć ochronę przed niepowołanym wstępem i aby zweryfikować procedury zabezpieczeń, wytrzymałość i zabezpieczenia operacyjne. Monitoring wlicza aktywne ataki dokonane przez autoryzowanych pracowników DoD aby sprawdzić bezpieczeństwo systemu. Podczas monitoringu, informacje mogą być badane, nagrywane, kopiowane i użyte do autoryzowanych celów. Wszystkie informacje, wliczając personalne, wprowadzone lub wysłane przez ten system mogą być monitorowane. Użycie tego komputera DoD, autoryzowane lub nie, wyraża zgodę na monitorowanie tego systemu. Nieautoryzowane użycie może doprowadzić do wszczęcia postępowania prawnego przeciw użytkownikowi. Dowody nieautoryzowanego dostępu zgromadzone podczas monitoringu mogą być użyte do celów administracyjnych, kryminalnych lub innych. Użycie tego systemu wyraża zgodę na monitorowanie w takich celach."

Windows XP wyświetla okno z podpisem i tekstem, który może być skonfigurowany przed załogowaniem użytkownika do komputera. DoD wymaga od organizacji wyświetlania ostrzeżenia o możliwości pociągnięcia użytkownika do odpowiedzialności prawnej jeżeli będzie on próbował załogować się bez autoryzacji. Nieobecność takiej notatki może być postrzegana jako zaproszenie bez restrykcji do załogowania się i przeglądania systemu.

Literatura:

- Bartock, Paul, et. al., *Guide to Securing Microsoft Windows NT Networks version 4.q*, National Security Agency, September 2000.
- DiMaria, Vincent, et.al., *Guide to Securing Microsoft Windows 2000 Terminal Services*, National Security Agency, July 2, 200a.
- Haney, Julie, *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset*, National Security Agency, January 2002.
- MacDonald, Dave, Warren Barkley, "Microsoft Windows 2000 TCP/IP Implementation Details," white paper,
<http://secinf.net/info/nt/2000ip/tcpipimp.html>.
- McGovern, Owen, Julie Haney, *Guide to Securing Microsoft Windows 2000 File and Disk Resources*, DISA and National Security Agency, May 2002.
- Microsoft Technet, <http://www.microsoft.com/technet>.
- Microsoft Windows XP Professional Resource Kit Documentation*, Microsoft Press, 200a.
- "No Password Expiration Notice Is Presented During the Logon Process," KB Article Q141494,
<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q141494>. Microsoft, March 2002.
- "Problems When the Autoenrollment Feature Cannot Reach an Active Directory Domain Controller," KB Article Q14046a,
<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q14046a>.

Microsoft, March 2002.

Schultze, Eric, "Windows XP Security: Everything you've always wanted to know...and a little bit more," as presented at InfoSec World 2002 conference.

"Upgrading Windows 2000 Group Policy for Windows XP," Microsoft KB article <http://support.microsoft.com/default.aspx?scid=kb:en=us:Q107900>. Microsoft, November 2002.