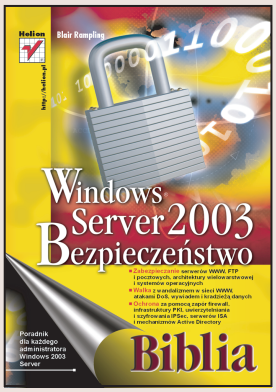
Windows Server 2003. Bezpieczeństwo. Biblia



Autor: Blair Rampling
Tłumaczenie: Paweł Koronkiewicz
ISBN: 83-7361-246-7
Tytuł oryginału: Windows Server 2003 Security Bible
Format: B5, stron: 528

W systemach obsługujących serwery, znaczenie bezpieczeństwa jest trudne do przecenienia. Dotyczy to w szczególny sposób nowych systemów operacyjnych, takich jak Windows 2003 Server, które z racji swojej krótkiej obecności na rynku, są potencjalnie bardziej narażone na skuteczne ataki hakerów. Pojawienie się nowego systemu oznacza jednocześnie początek wyścigu, między hakerami, którzy próbują go złamać, a administratorami, którzy starają się temu zapobiec.

Jeśli chcesz w tym wyścigu wygrać, sięgnij po książkę: „Windows Server 2003. Bezpieczeństwo. Biblia". Jest to opracowanie mające dostarczyć Ci wszystkich informacji niezbędnych do skutecznego zabezpieczanie sieci przed atakami zewnętrznymi i wewnętrznymi. Dowiesz się jak analizować środowisko sieciowe, planować i wdrażać odpowiednie rozwiązania, przygotowywać i prowadzić audyty zabezpieczeń, szyfrować dane oraz uwierzytelniać użytkowników.

Poznasz:

- Potencjalne zagrożenia
- Sposoby planowania i inspekcji systemu zabezpieczeń
- Zabezpieczanie systemu operacyjnego
- Zabezpieczanie aplikacji
- Szyfrowanie danych
- Uwierzytelnianie w systemie Windows Server 2003
- Protokół Kerberos
- Infrastrukturę klucza publicznego i wdrażanie usług certyfikatów
- Tworzenie wirtualnych sieci prywatnych L2TP i PPTP
- Protokół IPSec
- Microsoft Internet Security and Acceleration Server

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Wstęp 13

Część I Podstawy 15

Rozdział 1. Zagrożenia 17

Zagrożenia wewnętrzne a zagrożenia zewnętrzne 18
Zagrożenia wewnętrzne 18
Zagrożenia zewnętrzne 21
Środki bezpieczeństwa wewnętrznego i zewnętrznego 26
Środki bezpieczeństwa zewnętrznego 27
Środki bezpieczeństwa wewnętrznego 27
Typy ataków 28
Wandalizm w sieci WWW 29
Szpiegostwo i kradzież danych 30
Ataki typu Denial of Service 32
Podsumowanie 34

Rozdział 2. Zabezpieczenia sieci i systemu — przegląd 35

Charakterystyka bezpiecznej sieci 36
Wielopoziomowa struktura zabezpieczeń 37
Punkty wejścia i wyjścia 43
Zabezpieczenia systemów komputerowych 45
Zabezpieczenia aplikacji 47
Metody naruszania ochrony danych 49
Przecieki informacji 50
Ataki na zasadzie pełnego przeglądu 51
Przepełnienie bufora 52
Podstawienie ciągu formatującego 54
Zmiana katalogu bieżącego 54
Fałszywy pośrednik 55
Socjotechnika 55
Root kity i konie trojańskie 57
Wykrywanie root kitów 57
Usuwanie szkodliwych programów 58
Podsumowanie 58

Rozdział 3. Planowanie architektury zabezpieczeń 61
Projektowanie bezpiecznej architektury serwera 62
Minimalizacja 63
Wyłączanie zbędnych usług 64
Uaktualnianie systemu 66
Dokumentowanie nowej instalacji 69
Architektura sieci 69
Tworzenie planu czynności konserwacyjnych zabezpieczeń 71
Codzienne czynności administracyjne 71
Uaktualnienia zabezpieczeń 72
Kontrolowanie zmian 73
Plan awaryjny 75
Środki doraźne 75
Gromadzenie dowodów 75
Przywracanie stanu systemu 77
Honeypot (garnek miodu) 77
Podsumowanie 78

Rozdział 4. Inspekcja zabezpieczeń 79
Planowanie inspekcji komputerów 79
Inspekcja zabezpieczeń w systemie Windows 80
Ogólny przegląd zabezpieczeń 80
Przechwytywanie pakietów (sniffing) 82
Inspekcja zabezpieczeń w systemie UNIX 88
Ogólny przegląd zabezpieczeń 88
Skanowanie portów 95
Przechwytywanie pakietów w systemie UNIX 96
Podsumowanie 101

Rozdział 5. Mechanizmy zabezpieczeń w systemie Windows Server 2003 103
Architektura systemu Windows Server 103
Funkcje zabezpieczeń systemu Windows Server 105
Co nowego? 105
Starsze mechanizmy zabezpieczeń systemu Windows 107
Active Directory 112
Architektura Active Directory 113
Zabezpieczenia w Active Directory 114
Microsoft CryptoAPI 114
IPSec 115
Serwer ISA 116
Jaka jest rola usług serwera ISA? 116
Na czym polegają zabezpieczenia serwera ISA? 116
Podsumowanie 117

Część II Zabezpieczenia systemu 119

Rozdział 6. Zabezpieczanie systemu Windows Server 2003 121
Zabezpieczenia sprzętowe 122
Zabezpieczanie systemu operacyjnego 125
Ograniczanie instalacji 126
Uprawnienia dostępu do plików 132
Inspekcja 137

Zasady grup 139
Tworzenie i usuwanie obiektów GPO 140
Modyfikowanie obiektów GPO 142
Zabezpieczenia obiektu GPO 144
Internet Connection Firewall (ICF) 146
Podsumowanie 151

Rozdział 7. Zabezpieczanie aplikacji 153
Zabezpieczanie serwerów WWW i FTP 153
Zabezpieczanie serwerów WWW 154
Zabezpieczanie serwerów FTP 165
Zabezpieczanie serwerów pocztowych 166
Zabezpieczenia serwera 166
Zabezpieczanie przed spamem 167
Zabezpieczanie serwerów DNS 168
Zabezpieczanie innych aplikacji 169
Zabezpieczanie aplikacji różnego typu 170
Zabezpieczanie aplikacji wielowarstwowych 170
Podsumowanie 171

Część III Uwierzytelnianie i szyfrowanie 173

Rozdział 8. Szyfrowanie danych 175
Wprowadzenie do kryptografii 175
Szyfry z kluczem jednorazowym 177
Szyfry z kluczem symetrycznym 178
Szyfry z kluczem publicznym 178
Kryptografia kontrolowana 179
Kryptograficzny podpis 180
Steganografia 181
Encrypting File System (EFS) 181
Czym jest system EFS? 182
Korzystanie z szyfrowania EFS 182
Oprogramowanie kryptograficzne innych firm 196
Podsumowanie 202

Rozdział 9. Zabezpieczanie stron WWW i poczty elektronicznej — protokoły SSL i TLS 203
SSL i TLS — wprowadzenie 205
Wydajność mechanizmów SSL 207
Protokół SSL a bezpieczna komunikacja HTTP 208
Szyfrowanie transmisji pocztowych 209
Słabe strony SSL 210
Protokół SSL w oprogramowaniu serwera Microsoft IIS 211
Szyfrowanie komunikacji SMTP w systemie Windows Server 217
Podsumowanie 219

Rozdział 10. Uwierzytelnianie w systemie Windows Server 2003 221
Proces uwierzytelniania 221
Uwierzytelnianie podstawowe 223
Kerberos 224

Uwierzytelnianie zewnętrzne 225
Metody biometryczne 226
Systemy żetonowe 226
Karty inteligentne 226
Uwierzytelnianie w systemie Windows przy użyciu kart inteligentnych 227
Podsumowanie 234

Rozdział 11. System Kerberos 235
Wprowadzenie 236
Prosty system Kerberos 236
Rozproszony system Kerberos 236
Uwierzytelnianie Kerberos w układzie wieloobszarowym 237
Zaawansowane techniki obsługi biletów Kerberos 239
Projektowanie architektury Kerberos 241
Architektura 241
Znaczenie synchronizacji czasu 243
Kerberos a Windows Server 2003 243
Konfigurowanie zasad grup 244
Współdziałanie z innymi środowiskami 245
Podsumowanie 249

Rozdział 12. Infrastruktura klucza publicznego (PKI) 251
Więcej o PKI 253
Infrastruktura PKI w ujęciu teoretycznym 253
PKI w praktyce 254
Projektowanie infrastruktury PKI 256
Podsumowanie 258

Rozdział 13. Instalowanie i konfigurowanie usług certyfikatów 259
Planowanie wdrożenia usług certyfikatów 259
Instalowanie usług certyfikatów 260
Konfigurowanie urzędu CA 265
Tworzenie szablonów certyfikatów 274
Uaktywnianie szablonów certyfikatów 280
Zgłaszanie żądań certyfikatów 281
Podsumowanie 289

Rozdział 14. Wirtualne sieci prywatne L2TP i PPTP 291
Sieci VPN typu LAN-LAN 292
Wprowadzenie 292
Konfigurowanie połączenia VPN typu router-router opartego na protokole PPTP 293
Konfigurowanie połączenia VPN typu router-router opartego na protokole L2TP 303
Połączenia VPN zdalnego dostępu 315
Konfigurowanie połączenia VPN zdalnego dostępu opartego na protokole PPTP 316
Konfigurowanie połączenia VPN zdalnego dostępu opartego na protokole L2TP 320
Podsumowanie 324

Rozdział 15. Zabezpieczenia IPSec 325
Czym jest protokół IPSec? 325
Konfigurowanie zabezpieczeń IPSec 326
Wyposażenie sprzętowe 343
Podsumowanie 344

Część IV Microsoft Internet Security and Acceleration Server ... 345

Rozdział 16. ISA Server — podstawy ... 347
Zapory firewall ... 348
Inspekcja stanowa i bezstanowa ... 350
Skalowalność zapory ... 351
Systemy wykrywania włamań (IDS) ... 352
Systemy buforowania treści ... 353
Buforowanie treści — oprogramowanie ... 355
Buforowanie treści — urządzenia ... 355
Skalowanie serwera buforującego ... 356
Metody i protokoły buforowania ... 356
Serwer ISA — przegląd ... 357
Integracja z systemem Windows Server ... 357
Wymagania ... 358
Zapora — przegląd funkcji ... 358
Usługa akceleracji — przegląd ... 363
Podsumowanie ... 368

Rozdział 17. Instalowanie i konfigurowanie zapory firewall ... 369
Instalowanie serwera ISA ... 369
Instalowanie aktualizacji schematu Active Directory ... 369
Instalowanie serwera ISA ... 372
Konfigurowanie zapory firewall ... 378
Kreator konfiguracji (Getting Started Wizard) ... 378
Filtry ... 391
Reguły ... 399
Kontrola ruchu sieciowego ... 408
Filtry aplikacji ... 410
Podsumowanie ... 413

Rozdział 18. Konfigurowanie usługi buforowania ... 415
Konfigurowanie buforowania ... 415
Zasady buforowania i rozmiar bufora ... 416
Buforowanie proste ... 424
Buforowanie odwrotne ... 428
Mostkowanie SSL ... 430
Analizowanie ruchu sieciowego i raporty ... 432
Mechanizmy raportowania i monitorowania serwera ISA ... 432
Liczniki wydajności buforowania ... 436
Rozwiązywanie problemów i optymalizowanie pracy bufora ... 437
Podsumowanie ... 438

Dodatki ... 439

Dodatek A Narzędzia administratora zabezpieczeń ... 441

Dodatek B Źródła informacji o zabezpieczeniach ... 447

Dodatek C Standardowe przypisania portów TCP/IP ... 451

Skorowidz ... 515

Rozdział 6.
Zabezpieczanie systemu Windows Server 2003

W rozdziale:

- Zabezpieczenia warstwy sprzętowej
- Zabezpieczanie systemu operacyjnego
- Zasady grup
- Internet Connection Firewall

Po omówieniu teoretycznych i proceduralnych aspektów zabezpieczeń czas zająć się praktyczną stroną zabezpieczania systemu Windows Server 2003.

Jak pisaliśmy w rozdziale 5., kolejne systemy operacyjne, począwszy od Windows NT 4.0, przez Windows 2000, po Windows Server 2003 były platformą ewolucyjnych zmian w systemach zabezpieczeń. Przykładem jednego z wielu usprawnień może być wprowadzenie mechanizmu Kerberos do uwierzytelniania domenowego.

Aby wzmocnić zabezpieczenia systemu, można korzystać z różnych środków. Podstawowe z nich omówimy w niniejszym rozdziale, a są nimi:

- konfiguracja sprzętowa,
- instalowanie systemu operacyjnego,
- określanie uprawnień do pliku,
- konfigurowanie inspekcji,
- zasady grup.

O ile uwzględnimy potencjalne luki, zastosowanie tych środków może prowadzić do utworzenia stosunkowo bezpiecznej konfiguracji. Pełne zabezpieczenie komputera wymaga dokładnej znajomości konfiguracji sieci i systemu operacyjnego.

Zabezpieczenia sprzętowe

Pierwszą rzeczą, którą powinniśmy wziąć pod uwagę, gdy zabezpieczamy komputer, są zabezpieczenia na poziomie sprzętowym. Bezpieczeństwo wyposażenia to ważny krok w stronę całościowej ochrony systemu.

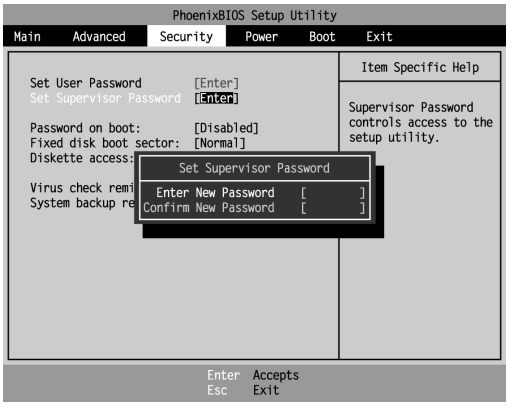
Źle zabezpieczone wyposażenie może umożliwić dostęp do chronionych plików lub naruszenie ochrony całego systemu. Standardowe zabezpieczenia większości platform sprzętowych umożliwiają dowolnej osobie modyfikowanie konfiguracji BIOS-u komputera oraz ładowanie systemu operacyjnego z dyskietki.

Zagadnienie zabezpieczeń sprzętowych wiąże się z istotną „cechą" systemu zabezpieczeń. System plików NTFS może być obsługiwany przez sterowniki systemów DOS i Linux. Po uruchomieniu komputera przy użyciu dyskietkowej wersji jednego z tych systemów operacyjnych wszystkie pliki komputera stają się swobodnie dostępne — sterowniki systemu plików dla systemów DOS i Linux ignorują listy kontroli dostępu (ACL). Brak mechanizmu uwierzytelniania Windows uniemożliwia operowanie odpowiednimi żetonami dostępu. Tak uzyskiwany dostęp do danych jest użytecznym narzędziem do odzyskiwania danych i zapewnia zgodność systemów. Konsekwencją jest jednak konieczność uwzględnienia w zabezpieczeniach dostępu do systemu komputerowego oraz konfiguracji BIOS-u.

Podstawowy problem zabezpieczeń sprzętowych polega na możliwości uruchomienia komputera za pomocą dyskietki i uzyskania — przy użyciu sterowników spoza Windows — dostępu do dysków twardych (wyjątkiem są jedynie pewne konfiguracje RAID obsługiwane przez sterowniki Windows, ich wprowadzenie nie jednak metodą zabezpieczania danych). Po takim ataku można wprowadzać modyfikacje w plikach systemowych, a nawet Rejestrze i bazie danych SAM. Efektem może być zmiana haseł lub innego rodzaju osłabienie mechanizmów zabezpieczeń. Atakujący ma dostęp do wszystkich plików komputera. Inną możliwością może być zainstalowanie nowego systemu operacyjnego. Po zainstalowaniu systemu Windows Server 2003 od nowa, atakujący może skorzystać z praw administratora komputera lokalnego i zastąpić wcześniejsze listy kontroli dostępu do plików.

Atak na poziomie sprzętowym można uniemożliwić kilkoma sposobami. Najprostszą metodą uniemożliwienia załadowania systemu operacyjnego z dyskietki lub dysku CD-ROM jest fizyczna obecność przy komputerze. Dostępne są również specjalne blokady stacji dyskietek, umieszczane w szczelinie napędu i zamykane na klucz. W zamek może być wyposażona również obudowa. Jeżeli komputer jest w szafce, można zamknąć szafkę. Również wejście do centrum obliczeniowego czy sali serwerów może pozostawać stale zamknięte. Warto zadbać o stosowanie tego rodzaju środków odpowiednio do potrzeb organizacji. Po zainstalowaniu systemu operacyjnego nic zazwyczaj nie stoi na przeszkodzie, aby całkowicie usunąć stację CD-ROM i stację dyskietek z komputera. Dalsze oprogramowanie można instalować, korzystając z udziałów sieciowych.

Kolejnym poziomem ochrony jest zmiana konfiguracji BIOS-u komputera. Ustawienia te muszą być zabezpieczone hasłem uniemożliwiającym atakującemu ich zmianę. Rysunek 6.1 przedstawia wprowadzanie hasła BIOS-u w przykładowym komputerze. W większości komputerów hasło zabezpieczające BIOS określa się jako *supervisor password* lub *setup password*.

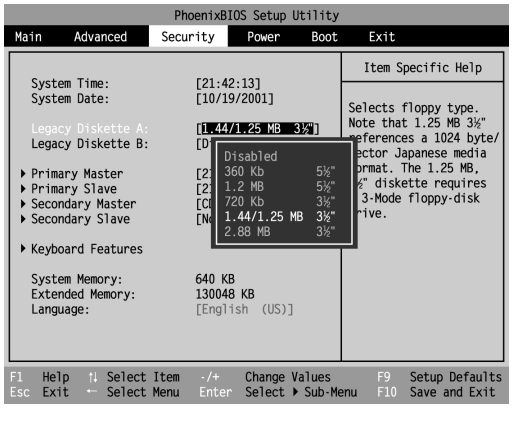


Rysunek 6.1. *Hasło dostępu do ustawień konfiguracyjnych BIOS-u zabezpiecza przed wprowadzeniem niepożądanych zmian*

Oprogramowanie BIOS produkują różne firmy, stąd istotne różnice pomiędzy komputerami. Mimo że konkretne rozwiązania mogą być nieco odmienne, w niemal każdym programie konfiguracyjnym BIOS-u znaleźć można opisywane poniżej opcje konfiguracyjne.

Typową możliwością jest wprowadzenie hasła użytkownika. Komputer może być wówczas uruchomiony wyłącznie po podaniu hasła użytkownika lub hasła dostępu do BIOS-u. Dodatkową możliwością może być ograniczenie możliwości uzyskania dostępu do napędów dysków wyłącznie do sytuacji, gdy przy uruchamianiu komputera podane zostało hasło dostępu do BIOS-u.

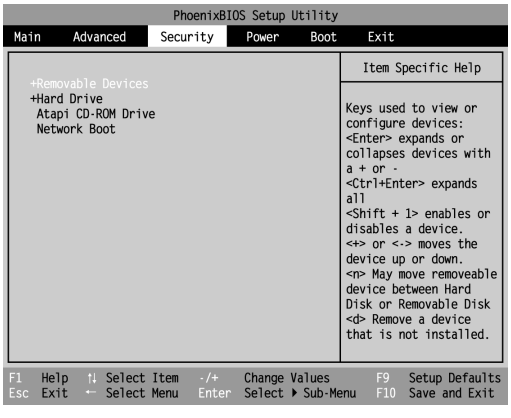
Gdy opcja ograniczenia dostępu do napędów dysków nie jest dostępna, pozostaje określenie haseł oraz wyłączenie dostępu do stacji dyskietek i stacji CD-ROM. Rysunek 6.2 przedstawia opcję konfiguracyjną BIOS-u, która umożliwia wyłączenie stacji dyskietek.



Rysunek 6.2. *Stacja dyskietek powinna zostać wyłączona w programie konfiguracyjnym BIOS-u*

Po wprowadzeniu takiej zmiany, aby załadować system operacyjny z dyskietki, osoba znająca hasło dostępu do BIOS-u musi uruchomić programu konfiguracyjny i włączyć stację. Wyłączenie napędu CD-ROM może być nieco trudniejsze. Jeżeli jest to jedyny napęd przyłączony do danego kanału IDE, można wyłączyć ten kanał. Jeżeli do tego samego kanału przyłączony jest drugi napęd albo CD-ROM korzysta ze złącza SCSI, jedyną dostępną opcją może być wyjęcie stacji z komputera.

Inną możliwości zabezpieczenia komputera przed uruchomieniem z dyskietki lub dysku CD-ROM jest odpowiednie ustalenie kolejności przeglądania napędów w poszukiwaniu systemu operacyjnego. Nie wykluczy to możliwości korzystania ze stacji po uruchomieniu komputera, ale uniemożliwi załadowanie innego systemu operacyjnego. Rysunek 6.3 przedstawia standardową kolejność przeglądania napędów.



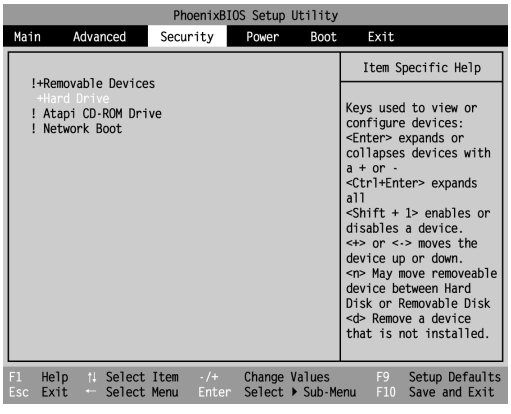
Rysunek 6.3. *Standardowa kolejność przeglądania napędów umożliwia ładowanie systemu operacyjnego ze stacji dysków wymiennych i CD-ROM*

Domyślnie najpierw podejmowana jest próba załadowania systemu operacyjnego ze stacji dysków wymiennych, takiej jak stacja dyskietek. Następnie system jest poszukiwany na dysku twardym, w stacji CD-ROM i, ostatecznie, w sieci. W takim układzie atakujący bez najmniejszego problemu może załadować system operacyjny z dyskietki. Może też odłączyć dysk systemowy i skorzystać z możliwości uruchamiania z dysku CD-ROM lub serwera sieciowego. Wówczas dostępne będą inne dyski systemu (o ile w komputerze jest ich więcej). Jeżeli atakujący zmieni konfigurację dysku rozruchowego i uniemożliwi ładowanie zeń systemu operacyjnego, również i ten dysk będzie dostępny. Po wprowadzeniu zmian zapewniających inny sposób dostępu do systemu konfiguracja dysku może zostać przywrócona.

Rozważenie powyżej wymienionych możliwości prowadzi do wniosku, że prostsza zmiana kolejności przeglądania napędów w poszukiwaniu systemu operacyjnego nie będzie wystarczająca. Niezbędne jest całkowite wykluczenie innych nośników niż dysk twardy (patrz rysunek 6.4). W przedstawionym na rysunku programie konfiguracyjnym BIOS-u wykrzyknik oznacza, że urządzenie zostało wyłączone i nie może zostać użyte do ładowania systemu operacyjnego.

Po wprowadzeniu opisywanych wyżej zmian komputer można uznać za zabezpieczony na poziomie sprzętowym. Zabezpieczenie konfiguracji BIOS-u komputera hasłem jest ważne i skuteczne. Dla osoby nieznającej hasła jedynym sposobem uzyskania dostępu do systemu jest odłączenie zasilania pamięci konfiguracji. Jest to metoda dość radykalna, choć prosta technicznie. Nie można więc zapominać o fizycznym bezpieczeństwie centrum przetwarzania danych.

Wracając do modelu zabezpieczeń opartego na warstwach, ochrona w BIOS-ie i wyłączone urządzenia rozruchowe to jedna warstwa bezpieczeństwa, a zamknięte drzwi centrum komputerowego lub szafki albo zamki w komputerze mogą tworzyć warstwy dalsze. Nawet wymontowanie stacji dysków wymiennych z komputera nie jest stuprocentowo skuteczne — włamywacz może przynieść własne urządzenia. Każda z warstw jedynie utrudnia atak lub ostatecznie zniechęca mniej zdeterminowaną osobę.



Rysunek 6.4.
Stacja dyskietek, stacja CD-ROM i sieć zostały wykluczone z procedur poszukiwania systemu operacyjnego

Zabezpieczanie systemu operacyjnego

Po zabezpieczeniu komputerów na poziomie sprzętowym kolejnym krokiem logicznym będzie instalacja systemu operacyjnego. Pierwszym elementem jest autentyczność nośnika plików instalacyjnych. Kopii dysku, czy to „domowego wyrobu" czy pirackiej, nie można traktować z pełnym zaufaniem. Może się to wydawać nieco przesadnym środkiem bezpieczeństwa, ale dyski powielane przez firmę Microsoft są przed zapakowaniem weryfikowane pod kątem bezpieczeństwa. Nowsze CD mają numer i oznaczenia holograficzne stosunkowo trudne do podrobienia.

Zdarza się, że komputer zostaje zakupiony z zainstalowanym już systemem operacyjnym. W większości przypadków administrator reinstaluje wówczas oprogramowanie zarówno ze względów bezpieczeństwa, jak i dla ułatwienia przyszłej administracji. Jedynie w szczególnych przypadkach wielkie serwery i zainstalowany system Windows Server 2003 Datacenter Edition sprzedawane są jako całość i reinstalacja jest wykluczona. Wówczas pozostaje tylko sprawdzić, czy sprzedawca faktycznie dysponuje prawem do korzystania z logo *authorized reseller*. Bezpieczeństwo w trakcie dostawy może zapewnić odpowiednie plombowanie.

Na dyskach instalacyjnych systemu operacyjnego stosunkowo łatwo umieścić pliki z ukrytym oprogramowaniem typu „tylne wejście". Pracownik kopiujący dysk CD może umieścić na nim zarażony plik. Może się to wydawać przesadną podejrzliwością, ale zasada korzystania z bezpiecznych kopii dysków instalacyjnych jest na tyle prosta, że nie warto podejmować ryzyka. Zabezpieczanie przed lukami w zabezpieczeniach dobrze zacząć od podstaw.

W trakcie instalacji systemu operacyjnego i podstawowych czynności konfiguracyjnych można korzystać z dalszych środków wzmacniających bezpieczeństwo komputera, takich jak:

- minimalizowanie liczby instalowanych składników systemu operacyjnego,
- wyłączenie wszystkich usług innych niż niezbędne po zakończeniu instalacji,
- określenie właściwych uprawnień do plików,

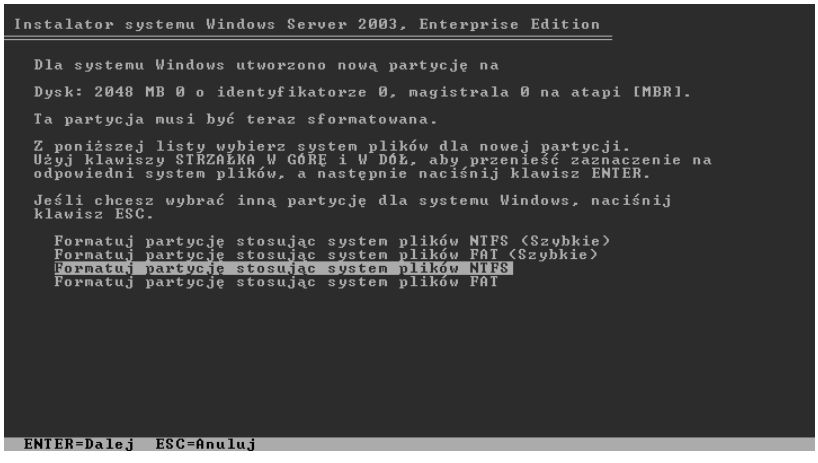
- włączenie inspekcji,
- określenie zasad grup narzucających dodatkowe zabezpieczenia systemu.

System Windows Server 2003 powinien być instalowany na partycji NTFS. Użycie partycji FAT stoi w ostrej sprzeczności z dążeniem do zabezpieczenia komputera. System plików FAT nie zapewnia żadnych mechanizmów zabezpieczeń, takich jak listy kontroli dostępu i szyfrowanie dostępne w systemie NTFS.

Poza środowiskami testowymi system plików FAT nie powinien być stosowany do formatowania żadnych partycji pod kontrolą systemu Windows Server 2003.

Partycję systemową można utworzyć w trakcie instalowania systemu operacyjnego. Rysunek 6.5 przedstawia ekran wybierania systemu plików partycji Windows Server 2003.

Rysunek 6.5. *Aby zapewnić bezpieczeństwo komputera, w trakcie instalowania systemu Windows Server 2003, formatujemy partycję systemową w formacie NTFS*



Ograniczanie instalacji

Minimalizowanie liczby składników systemu operacyjnego to, jak pisaliśmy w rozdziale 3., metoda ograniczania liczby elementów zagrożonych potencjalnymi lukami w zabezpieczeniach. Wcześniej wspomnieliśmy już pojęcie „ograniczania profilu systemu". Każda aplikacja i usługa to kolejny składnik oprogramowania, w którym mogą występować szkodliwe błędy przepełnienia bufora, wykorzystania ciągu formatującego i inne. Gdy taka luka zostanie odkryta w przyszłości, a administrator w porę nie uzyska odpowiedniej informacji, atakujący może uzyskać dostęp do komputera, lokalnie lub zdalnie.

Minimalizowanie liczby składników Windows

W przeciwieństwie do wcześniejszych wersji systemu Windows, w tym Windows 2000 Server i Windows NT 4.0 Server, system Windows Server 2003 nie oferuje w trakcie instalacji możliwości wybierania składników. Standardowo instalowany jest ograniczony zestaw podstawowego oprogramowania serwera. Przed instalacją składników sieciowych wprowadzamy:

- wybór ustawień regionalnych systemu,
- dane użytkownika,
- klucz produktu,
- wybór trybu licencjonowania,
- nazwę komputera,
- hasło administratora,
- datę i godzinę.

Procedura instalowania składników sieciowych zapewnia konfigurację standardową, umożliwiającą wielu komputerom natychmiastowe rozpoczęcie pracy w sieci. Adres IP jest pobierany z serwera DHCP. Włączone zostają również standardowe usługi sieciowe. W większości przypadków nie unikniemy oczywiście wprowadzania ręcznych korekt tej konfiguracji. Można wyłączyć niektóre usługi lub określić statyczny adres IP.

Aby przejrzeć ustawienia sieciowe, klikamy *Ustawienia niestandardowe* (*Custom Settings*), a następnie *Dalej* (*Next*).

Wyświetlone zostanie wówczas okno konfiguracji sieci. Nie będziemy raczej wyłączać klienta sieci Microsoft Networks ani protokołu TCP/IP. Elementem wartym rozważenia jest jednak *Udostępnianie plików i drukarek w sieciach Microsoft Networks* (*File and Printer Sharing for Microsoft Networks*).

Jeżeli konfigurowany komputer nie będzie wykorzystywany jako serwer plików lub serwer drukarek, wyłączamy tę usługę. Jej pozostawienie naraża na luki w zabezpieczeniach wynikające z niewystarczających ograniczeń dostępu do plików lub błędów w oprogramowaniu usługi. Nie ma powodu, aby instalować usługę udostępniania na dedykowanym serwerze WWW lub poczty elektronicznej. Jeżeli zdecydujemy się wyłączyć usługę, klikamy w towarzyszącym jej nazwie polu wyboru. Kolejnym krokiem może być dostosowanie ustawień TCP/IP, po którym klikamy *Dalej* (*Next*), aby przejść do kolejnego okna.

Kolejnym istotnym wyborem jest określenie, czy serwer będzie pracował w domenie czy w grupie roboczej.

Serwer należący do domeny zezwala użytkownikom na dostęp z tej domeny. Inne komputery w domenie są dla niego komputerami godnymi zaufania. Dobrą praktyką jest pozostawianie poza domeną tych serwerów, których funkcja nie wymaga takiej przynależności. Dotyczy to przede wszystkim serwerów WWW, FTP i serwerów pocztowych. Naruszenie zabezpieczeń serwera należącego do domeny ułatwia ataki na inne komputery. Pozostawienie serwerów szczególnie wrażliwych na ataki poza domeną pozwala uniknąć tego problemu.

Włączenie serwera do domeny zapewnia wiele ułatwień. W miejsce zarządzania osobną listą użytkowników każdego serwera udostępniamy zasoby użytkownikom w domenie. Kusi to wielu administratorów do włączania do domeny serwerów WWW i innych, które w rzeczywistości nie wymagają uwierzytelniania domenowego. Problemem jest to, że naruszenie zabezpieczeń tak „otwartych" systemów może służyć do ataków na inne komputery domeny.

Konfiguracja sieci w niektórych organizacjach wymusza pracę pewnych komputerów jako członków domeny. Najlepszym przykładem są serwery plików i drukarek. Jeżeli serwer plików nie jest członkiem domeny, baza danych użytkowników tego serwera jest kopią części bazy użytkowników domeny. Celem istnienia domeny jest jednak właśnie ułatwianie zarządzania użytkownikami. Gdy serwer jest członkiem domeny, na listach ACL można operować nazwami użytkowników i grup domeny, bez ciągłych problemów z kopiowaniem konfiguracji kont między różnymi serwerami.

Niektóre aplikacje pocztowe (a ściślej groupware), jak Microsoft Exchange, wymagają od użytkowników uwierzytelniania domenowego. Podobnie skonfigurować można intranetowy serwer WWW. Wówczas konta domenowe zapewnią efektywny mechanizm uwierzytelniania dostępu do serwera wewnętrznego.

Po określeniu, czy serwer ma pracować w domenie czy w grupie roboczej, podajemy jej nazwę, po czym klikamy *Dalej* (*Next*), aby kontynuować instalację. Na tym kończy się interakcyjna część procesu. Instalator przechodzi do kopiowania plików i generowania wstępnej konfiguracji komputera.

Wyłączanie i konfigurowanie usług

Po zakończeniu pracy instalatora systemu Windows dysponujemy wstępną konfiguracją systemu operacyjnego, która wymaga systematycznego dostosowania do konkretnego zastosowania komputera.

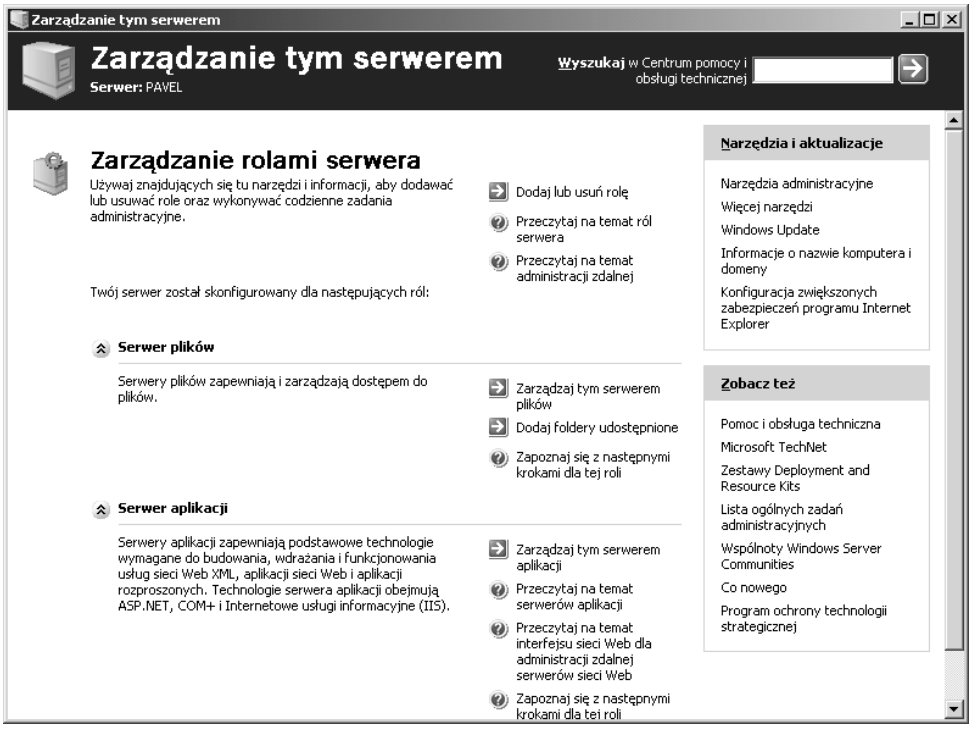
Gdy po raz pierwszy logujemy się w nowo zainstalowanym systemie Windows Server 2003, wyświetlane jest okno narzędzia *Zarządzanie tym serwerem* (*Manage Your Server*), przedstawione na rysunku 6.6. Narzędzie to służy do konfigurowania serwera do pracy w określonej roli. **Rola** (ang. *role*) jest tutaj zestawem plików i usług zapewniających realizację pewnych funkcji komputera, takich jak serwer DNS lub serwer Active Directory.

1. Aby przypisać komputerowi nową rolę, klikamy *Dodaj lub usuń rolę* (*Add or remove a role*).

   Powinniśmy dokładnie przeczytać listę czynności wstępnych, wyświetlaną na pierwszej karcie kreatora konfigurowania serwera. Przypomina ona między innymi o tym, że przed rozpoczęciem pracy z rolami powinniśmy zakończyć konfigurowanie połączenia sieciowego i instalowanie urządzeń peryferyjnych. Klikamy *Dalej* (*Next*).

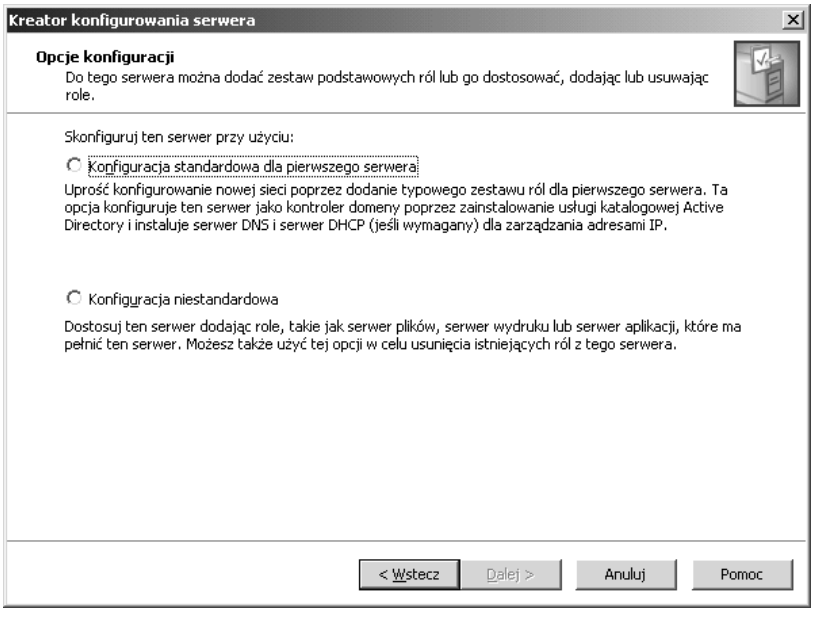
2. Rysunek 6.7 przedstawia kolejny krok kreatora. Opcja *Konfiguracja standardowa dla pierwszego serwera* (*Typical configuration for a first server*) zapewni skonfigurowanie serwera jako pierwszego kontrolera domeny w nowej domenie, wraz z instalacją odpowiednich usług.

   Opcja *Konfiguracja niestandardowa* (*Custom configuration*) pozwala dostosować konfigurację serwera do specyficznych wymagań jego środowiska i przeznaczenia. Wybieramy *Konfiguracja niestandardowa* (*Custom configuration*) i klikamy *Dalej* (*Next*).

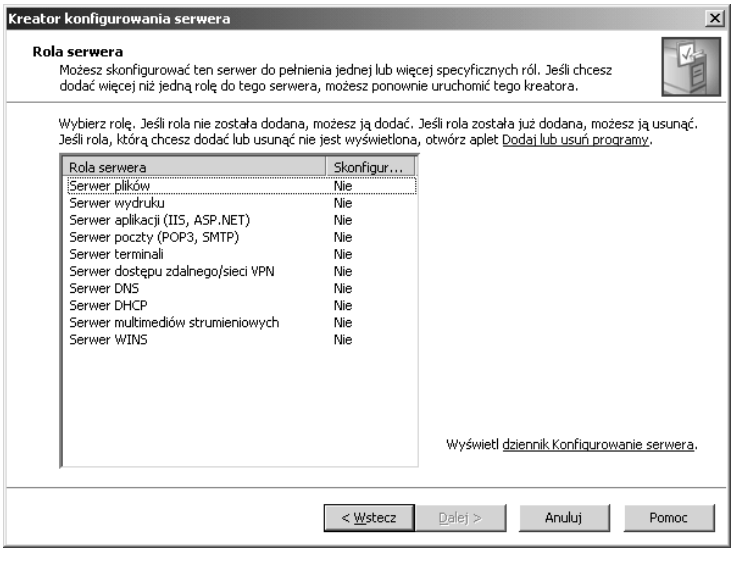


Rysunek 6.6. *Narzędzie Zarządzanie tym serwerem automatycznie konfiguruje serwer do określonej roli*

Rysunek 6.7. *Opcja typowej konfiguracji zapewnia zainstalowanie usług związanych z pracą komputera jako pierwszego kontrolera nowej domeny*



3. Kreator wyświetla listę standardowych ról serwera. Każda z opcji widocznych na rysunku 6.8 zapewnia nieco inne dostosowanie konfiguracji serwera. Wybranie, przykładowo, opcji *Serwer aplikacji* (*Application server*) spowoduje zainstalowanie serwera IIS i bibliotek ASP.NET, zapewniających możliwość uruchamiania aplikacji WWW. Opcja *Serwer multimediów strumieniowych* (*Streaming media server*) wiąże się z instalacją *Windows Media Services* (*Windows Media Services*). *Serwer poczty* (*Mail server*) to serwer usług SMTP i POP3 itd.



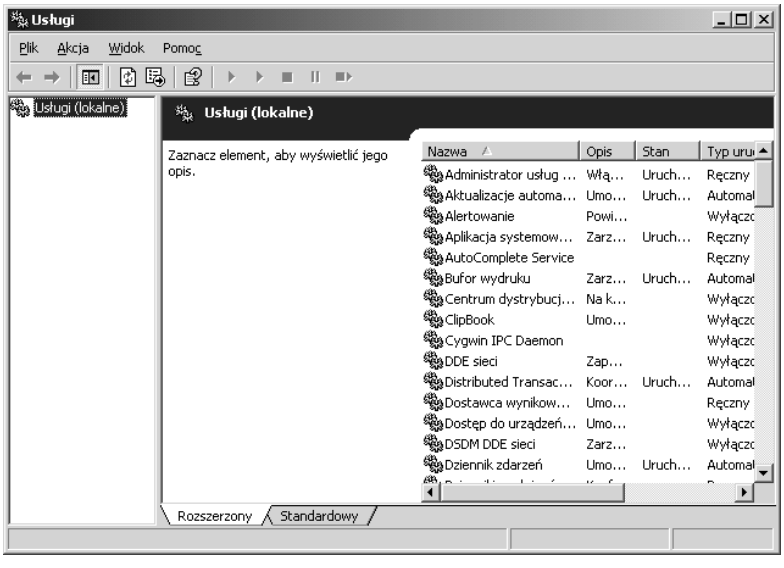
Rysunek 6.8. *Opcja konfiguracji niestandardowej umożliwia wybieranie pomiędzy różnymi typowymi zastosowaniami serwera, do których jest on automatycznie konfigurowany i optymalizowany*

Aby rozpocząć konfigurowanie serwera do pewnej roli, wybieramy jedną z pozycji na liście i klikamy *Dalej* (*Next*). Kliknięcie *Anuluj* (*Cancel*) spowoduje zamknięcie kreatora bez wprowadzania żadnych zmian. Można wówczas przejść do instalowania aplikacji lub dalszego konfigurowania zabezpieczeń systemu operacyjnego.

Po zainstalowaniu wymaganego oprogramowania systemowego przechodzimy do kolejnego kroku, którym jest wyłączanie niepotrzebnych usług. W systemie instalowany jest pewien zestaw standardowych usług i aplikacji. Część z nich nie jest wymagana do realizacji wymaganych funkcji serwera. Klikamy *Start/Narzędzia administracyjne/Usługi* (*Start/Administrative Tools/Services*), aby otworzyć konsolę MMC przedstawioną na rysunku 6.9.

Każdą usługę opisuje szereg kolumn:

- nazwa,
- opis,
- stan,
- typ uruchamiania,
- sposób logowania.



Rysunek 6.9. *Konsola Usługi umożliwia włączanie i wyłączanie usług Windows*

Stan usługi to informacja o tym, czy jest ona w danym momencie uruchomiona (aktywna). Sposób logowania to nazwa konta wykorzystywanego przez usługę w procedurach uwierzytelniania.

Opcja *Typ uruchomienia* (*Startup Type*) może mieć trzy wartości:

- *Automatyczny* (*Automatic*) — usługa jest uruchamiana automatycznie przy każdej inicjalizacji systemu operacyjnego.
- *Ręczna* (*Manual*) — usługa tak skonfigurowana może zostać uruchomiona przez inny program, usługę lub użytkownika (umożliwia to przycisk *Start* przystawki *Usługi*).
- *Wyłączony* (*Disabled*) — usługa wyłączona nie może zostać uruchomiona.

Skonfigurowanie usługi jako *Wyłączony* (*Disabled*) jest najbezpieczniejszą metodą wyłączenia niepotrzebnej usługi. Całkowicie uniemożliwia to jej uruchomienie.

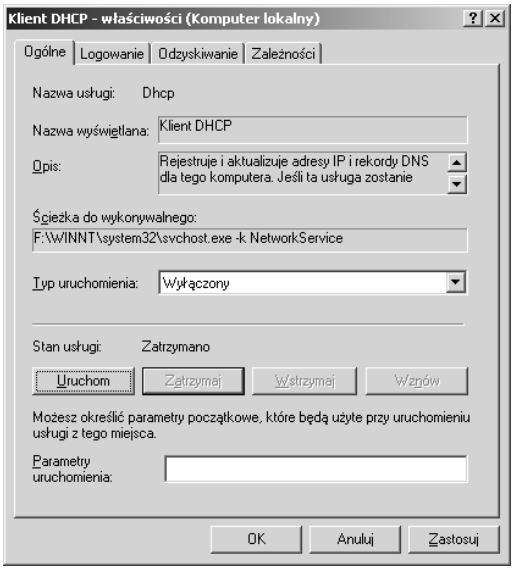
Lista usług jest długa i rośnie wraz z instalowanymi aplikacjami, które niekiedy dodają do niej zarządzanie własnymi składnikami oprogramowania. Istotne jest jednak, aby poznać znaczenie każdej z nich i podjąć właściwą decyzję o jej pozostawieniu lub wyłączeniu.

Prostym przykładem może być usługa klienta DHCP. Jest ona odpowiedzialna za pobieranie danych związanych z adresem IP z serwera DHCP, gdy przyłącze komputera jest skonfigurowane do korzystania z usługi DHCP. Ponieważ serwery najczęściej konfiguruje się do pracy ze statycznymi adresami IP (co uniezależnia je od zakłóceń pracy usługi DHCP), usługa klienta może w większości przypadków zostać wyłączona.

1. Klikamy prawym przyciskiem myszy wiersz usługi DHCP i wybieramy z menu podręcznego polecenie *Właściwości* (*Properties*). Powoduje to wyświetlenie arkusza właściwości usługi.

2. Zmieniamy opcję *Typ uruchomienia* (*Startup type*) na *Wyłączony* (*Disabled*) i klikamy przycisk *Zatrzymaj* (*Stop*). Okno powinno wyglądać wówczas podobnie jak pokazane na rysunku 6.10.

Rysunek 6.10. *Usługa została wyłączona i zatrzymana*



3. Klikamy *OK*, aby zamknąć arkusz właściwości.

Usługa po takich zmianach jest zatrzymana i nie ma możliwości jej ponownego uruchomienia. Odpowiednio zmieniają się też informacje w prawym obszarze okna konsoli usług.

W systemie Windows Server 2003 można doszukać się dużej liczby usług, które są uaktywniane standardowo, a w praktyce są niewykorzystywane. O tym jednak, które z nich faktycznie można wyłączyć, decyduje zawsze środowisko pracy serwera.

Uprawnienia dostępu do plików

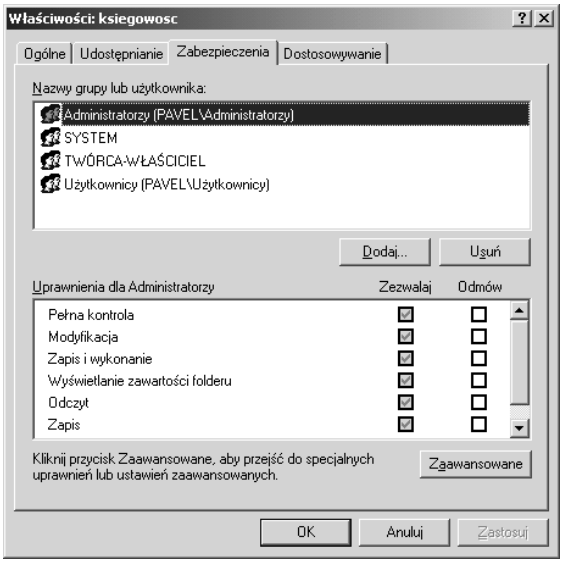
Uprawnienia dostępu do plików (ang. *file permissions*) albo, krócej, uprawnienia do plików to ważny element mechanizmów zabezpieczeń systemu Windows Server 2003. Uprawnienia można przypisywać zarówno plikom zapisywanym przez użytkowników, jak i plikom systemowym.

We wcześniejszych wersjach systemu Windows ważne pliki i katalogi, takie jak pliki systemu Windows, nie były odpowiednio zabezpieczone. W Windows Server 2003 podejście to zostało zmienione.

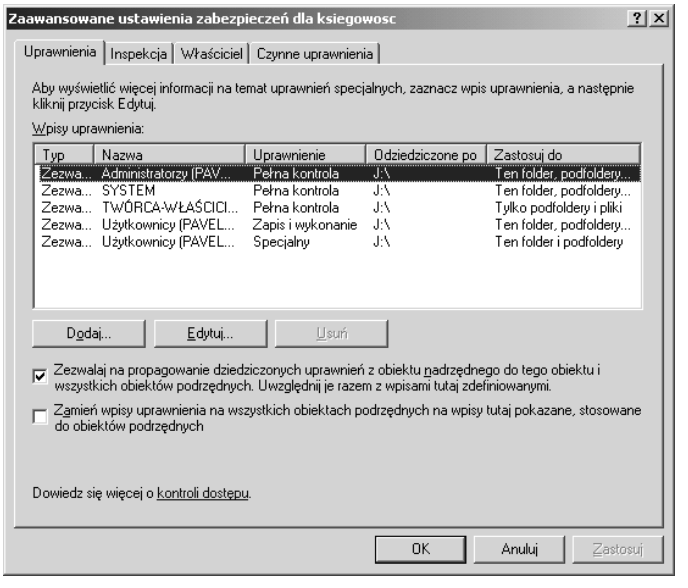
Najbardziej typowym powodem do zmiany domyślnych uprawnień pliku jest konfigurowanie ochrony plików w serwerze. Przykładem może być sytuacja, gdy umieszczamy w serwerze ważne dane grupy *ksiegowosc*. Zazwyczaj pierwszym krokiem jest wówczas utworzenie katalogu.

1. Po utworzeniu katalogu, klikamy prawym przyciskiem jego nazwę i wybieramy z menu podręcznego polecenie *Właściwości* (*Properties*).
2. Klikamy zakładkę *Zabezpieczenia* (*Security*). Domyślne uprawnienia dostępu do pliku przedstawia rysunek 6.11.

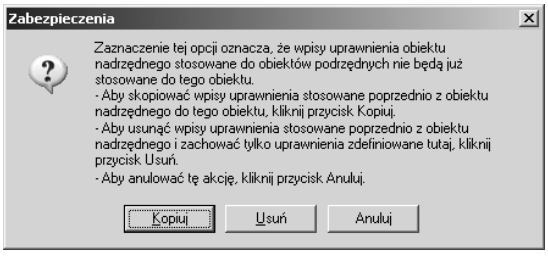
Rysunek 6.11. *Domyślne uprawnienia dostępu do folderu umożliwiają odczyt danych przez każdego uwierzytelnionego użytkownika*



3. Standardowo pełny dostęp do folderu uzyskuje domenowa grupa `Administrators` (Administratorzy) i konto systemowe. Grupa `Users` (Użytkownicy) ma prawa odczytu. W naszym przykładzie istotne będzie usunięcie uprawnień grupy `Users` i przyznanie grupie *ksiegowosc* uprawnień do odczytu i zapisu danych. Zaznaczamy więc pozycję `Users` i klikamy przycisk *Usuń* (*Remove*). Zapewni to istotne ograniczenie uprawnień dostępu, ponieważ użytkownik, któremu dostęp nie został jawnie przyznany, nie może wykonać żadnej operacji na danych. Usunięcie grupy `Users` z karty *Zabezpieczenia* może być jednak utrudnione — folder dziedziczy uprawnienia folderu nadrzędnego. Konieczne jest wówczas wyłączenie dziedziczenia uprawnień.
4. Na karcie *Zabezpieczenia* (*Security*) klikamy przycisk *Zaawansowane* (*Advanced*), aby wyświetlić okno dialogowe zaawansowanych ustawień zabezpieczeń, przedstawione na rysunku 6.12. Wyłączamy opcję *Zezwalaj na propagowanie dziedziczonych uprawnień z obiektu nadrzędnego…* (*Allow inheritable permissions from the parent…*) i klikamy *OK*.
5. Po wyłączeniu dziedziczenia wyświetlane jest okno dialogowe, przedstawione na rysunku 6.13. Możemy wybrać pomiędzy dwiema opcjami — skopiowania istniejących uprawnień dziedziczonych jako bezpośrednie uprawnienia do obiektu lub też porzucenia uprawnień dziedziczonych. W drugim z tych przypadków dotychczasowe uprawnienia dziedziczone zostają całkowicie usunięte. Klikamy *Kopiuj* (*Copy*), aby zachować istniejącą konfigurację uprawnień folderu. Wówczas możemy ponownie kliknąć *OK*, aby zamknąć okno ustawień zaawansowanych. Usunięcie grupy `Users` nie sprawi teraz problemu.

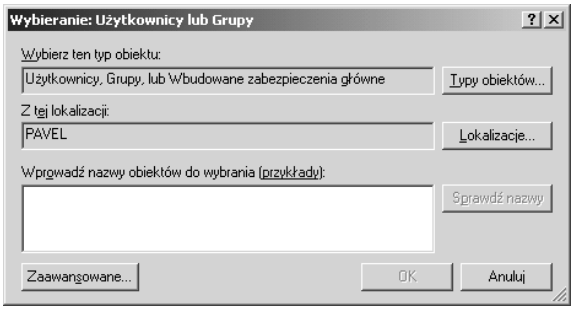


Rysunek 6.12. *Standardowo, uprawnienia są dziedziczone po folderze nadrzędnym. Wprowadzenie poprawnych ograniczeń dostępu wymaga wyłączenia tej funkcji*



Rysunek 6.13. *Gdy wyłączamy dziedziczenie uprawnień, musimy zdecydować pomiędzy zachowaniem istniejącej konfiguracji zabezpieczeń obiektu a całkowitym usunięciem uprawnień dziedziczonych*

6. Klikamy przycisk *Dodaj* (*Add*), aby dodać do listy grupę *ksiegowosc*. Wyświetlone zostaje okno *Wybieranie: Użytkownicy lub Grupy* (*Select Users, Computers, or Groups*), przedstawione na rysunku 6.14.



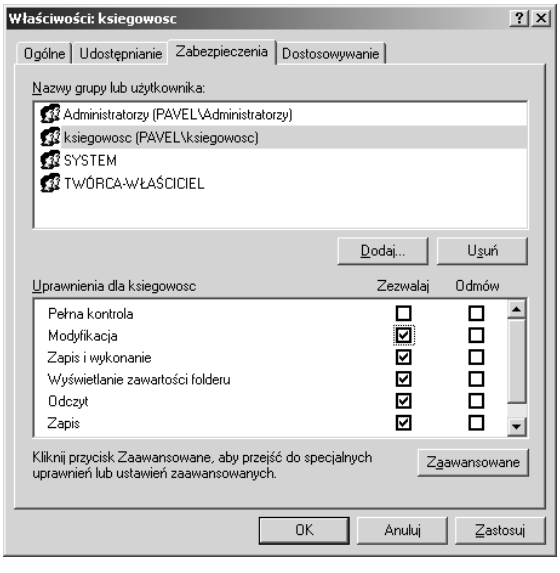
Rysunek 6.14. *Okno Wybieranie: Użytkownicy lub Grupy pozwala dołączać użytkowników lub grupy do listy na karcie Zabezpieczenia arkusza właściwości folderu*

7. W polu *Wprowadź nazwy obiektów do wybrania* (*Enter the object names to select*) wprowadzamy nazwę grupy i klikamy przycisk *Sprawdź nazwy* (*Check Names*). Następnie klikamy *OK*, aby zakończyć dodawanie grupy.

8. Zaznaczamy nową grupę na liście.

9. Uprawnienia domyślne to *Zapis i wykonanie* (*Read & Execute*), *Wyświetlanie zawartości folderu* (*List Folder Contents*) i *Odczyt* (*Read*). Grupa *ksiegowosc* wymaga dodatkowo możliwości modyfikowania plików i tworzenia nowych. Klikamy więc pole wyboru w kolumnie *Zezwalaj* (*Allow*) i wierszu *Modyfikacja* (*Modify*). Po zaznaczeniu uprawnienia do modyfikowania plików, uprawnienie *Zapis* (*Write*) jest uaktywniane automatycznie. Choć znaczenie większości uprawnień jest „samo przez się" zrozumiałe, nieco wątpliwości może wzbudzić *Pełna kontrola* (*Full Control*). Uprawnienie to zapewnia wszystkie pozostałe oraz, dodatkowo, możliwość zmieniania uprawnień do pliku lub folderu. W większości przypadków uprawnienie *Pełna kontrola* (*Full Control*) nie jest potrzebne nikomu poza administratorami. Wyjątkiem będzie sytuacja, kiedy delegujemy zarządzanie. Rysunek 6.15 przedstawia kartę *Zabezpieczenia* (*Security*) z nowym zestawem uprawnień grupy *ksiegowosc*. Aby zapisać wprowadzone zmiany, klikamy *OK*.

Rysunek 6.15. *Uprawnienia domyślne grupy ksiegowosc zostały uzupełnione o uprawnienie Modyfikacja*



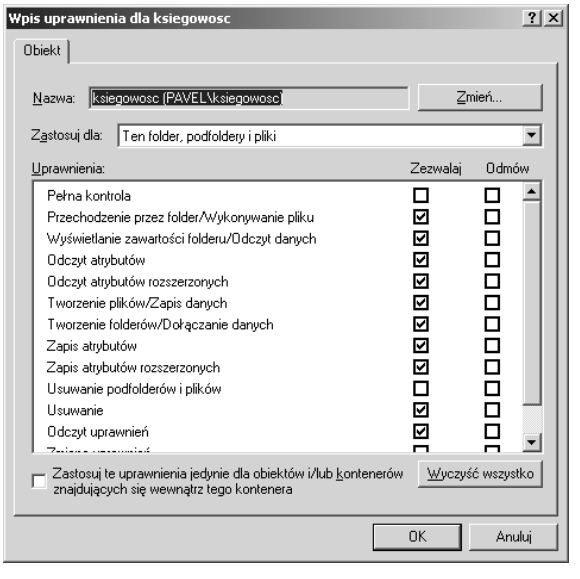
Choć zazwyczaj nie jest to potrzebne, warto pamiętać, że można zarządzać uprawnieniami ze znacznie większą ziarnistością.

1. Na karcie *Zabezpieczenia* (*Security*) klikamy przycisk *Zaawansowane* (*Advanced*), aby wyświetlić okno *Zaawansowane ustawienia zabezpieczeń* (*Advanced Security Settings*).

2. Na karcie *Uprawnienia* (*Permissions*) wyświetlana jest lista przypisanych uprawnień. Zaznaczamy grupę *ksiegowosc* i klikamy *Edytuj* (*Edit*). Wyświetlone zostaje okno *Wpis uprawnienia* (*Permission Entry*), przedstawione na rysunku 6.16.

   Jak łatwo zauważyć, przyznanie uprawnienia *Modyfikacja* (*Modify*) na karcie *Zabezpieczenia* (*Security*) zapewniło przyznanie niemal wszystkich uprawnień z listy. Wyjątkami są uprawnienia pozwalające użytkownikowi lub grupie zmieniać uprawnienia do folderu: *Pełna kontrola* (*Full Control*), *Zmiana uprawnień* (*Change*

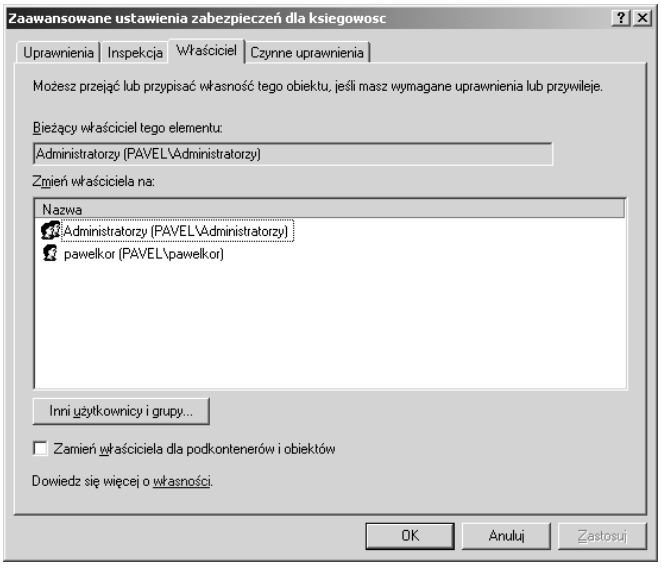
Rysunek 6.16.
Okno Wpis uprawnienia służy do zmieniania uprawnień do obiektu z większą ziarnistością



Permissions) i *Przejęcie na własność* (*Take Ownership*). Uprawnienie *Usuwanie* (*Delete Subfolders and Files*) również nie jest zaznaczone, ponieważ umożliwia usuwanie podfolderów i plików wewnątrz konfigurowanego folderu, a do nich użytkownik nie ma uprawnień. Jeżeli w folderze znajduje się plik i grupa *ksiegowosc* nie ma bezpośredniego uprawnienia do jego usunięcia, uprawnienie *Usuwanie* (*Delete Subfolders and Files*) folderu umożliwiłoby członkom grupy usunięcie tego pliku.

3. Ostatnim pojęciem związanym z uprawnieniami jest własność. Kliknijmy, wciąż w oknie zaawansowanych ustawień zabezpieczeń, zakładkę *Właściciel* (*Owner*). Jest ona przedstawiona na rysunku 6.17.

Rysunek 6.17.
Karta Właściciel okna zaawansowanych ustawień zabezpieczeń służy do zmieniania właściciela obiektu



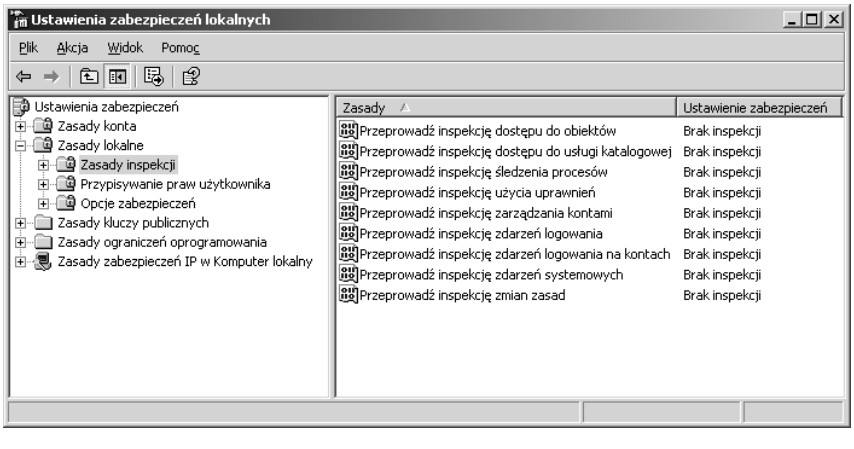
4. Właściciel obiektu może zmieniać uprawnienia do tegoż, nawet gdy nie ma jawnie przypisanego uprawnienia pełnej kontroli. Jest to wygodne, ponieważ administrator może przejąć własność obiektu, nawet jeżeli uprawnienia mają uniemożliwić uzyskanie do niego dostępu. Aby zmienić właściciela obiektu, wybieramy z listy użytkownika, który ma być nowym właścicielem, i klikamy *OK*. Własność mogą przejmować wyłącznie administratorzy i użytkownicy, którym przyznano uprawnienie *Przejęcie na własność* (*Take Ownership*).

Inspekcja

Inspekcja to bardzo użyteczne narzędzie administratora zabezpieczeń. W systemie Windows Server 2003 można rejestrować ogromną ilość różnych typów zdarzeń. Inspekcja polega na zapisywaniu każdej operacji użytkownika, dla której funkcja ta została włączona. Ponieważ zakończyliśmy właśnie omawianie uprawnień do plików, rozpoczniemy od przedstawienia zasad inspekcji plików.

Pierwszym krokiem jest uaktywnienie mechanizmów inspekcji. Jeżeli serwer nie należy do domeny, korzystamy z lokalnych zasad zabezpieczeń, a jeżeli serwer należy do domeny — z zasad grup dotyczących serwera domeny. Sposób włączania inspekcji przy użyciu zasad grup omówimy nieco dalej.

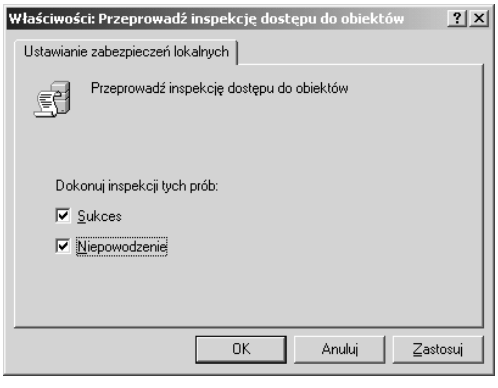
1. W przypadku samodzielnego serwera klikamy *Start/Narzędzia administracyjne/Zasady zabezpieczeń lokalnych* (*Start/Administrative Tools/Local Security Policy*). Otwieramy w ten sposób konsolę MMC zasad zabezpieczeń lokalnych.
2. W lewej części okna podwójnie klikamy *Zasady lokalne* (*Local Policies*), a następnie *Zasady inspekcji* (*Audit Policy*). Lista dostępnych zasad zostaje wyświetlona w prawej części okna. Przedstawiamy ją na rysunku 6.18.



Rysunek 6.18. *Aby uaktywnić procedury rejestrowania, musimy zmienić zasady inspekcji*

3. Dla każdego typu inspekcji, który włączamy, musimy kliknąć prawym przyciskiem myszy odpowiednią pozycję listy i wybrać z menu podręcznego *Właściwości* (*Properties*). W wyświetlanym wówczas oknie wybieramy rodzaj rejestrowanych operacji: *Sukces* (*Success*), *Niepowodzenie* (*Failure*) lub oba (jak na rysunku 6.19). Klikamy *OK*.

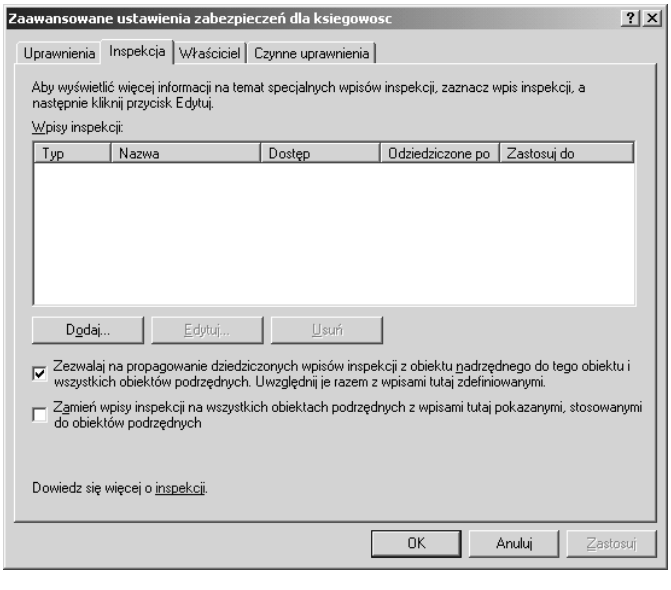
Rysunek 6.19.
Zasada inspekcji może być włączana i wyłączana dla operacji udanych oraz nieudanych niezależnie



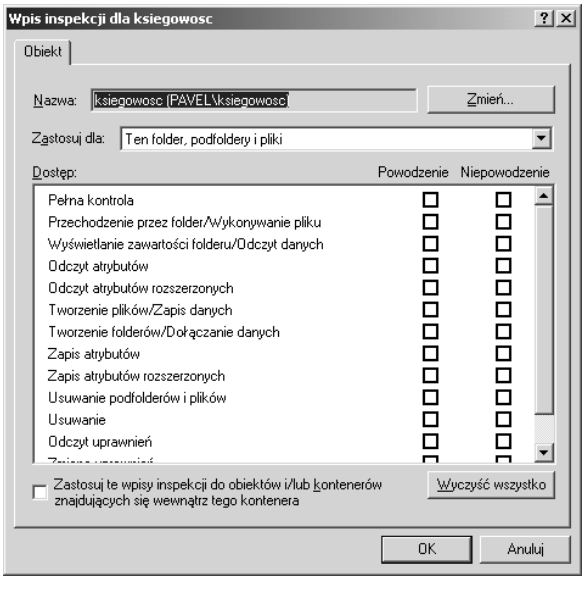
Inspekcję można następnie uaktywniać dla dowolnie wybranych plików i folderów.

1. Aby włączyć inspekcję, klikamy prawym przyciskiem myszy wybrany obiekt i wybieramy z menu podręcznego *Właściwości* (*Properties*).
2. Wywołujemy kartę *Zabezpieczenia* (*Security*) i klikamy przycisk *Zaawansowane* (*Advanced*), aby otworzyć okno zaawansowanych ustawień zabezpieczeń. Klikamy następnie zakładkę *Inspekcja* (*Auditing*), aby wyświetlić kartę przedstawioną na rysunku 6.20.

Rysunek 6.20.
Karta Inspekcja okna zaawansowanych ustawień zabezpieczeń zawiera listę bieżących wpisów inspekcji oraz umożliwia dodawanie nowych



3. Aby wprowadzić nowy wpis inspekcji, klikamy przycisk *Dodaj* (*Add*).
4. Kolejnym krokiem jest wybranie użytkownika lub grupy, której czynności będą rejestrowane. Służy do tego okno *Wybieranie: Użytkownik, Komputer lub Grupa* (*Select User, Computer or Group*). Grupa *Użytkownicy* (*Users*) zapewni rejestrowanie czynności wszystkich użytkowników. W naszym przykładzie włączymy inspekcję dla grupy *ksiegowosc*. Będzie to jedyna grupa mająca dostęp do obiektu. Wprowadzamy jej nazwę i klikamy *OK*. Wyświetlone zostaje okno *Wpis inpekcji* (*Auditing Entry*), przedstawione na rysunku 6.21.



Rysunek 6.21. *Okno Wpis inspekcji służy do uaktywniania funkcji rejestrowania dla określonych zdarzeń dotyczących obiektu*

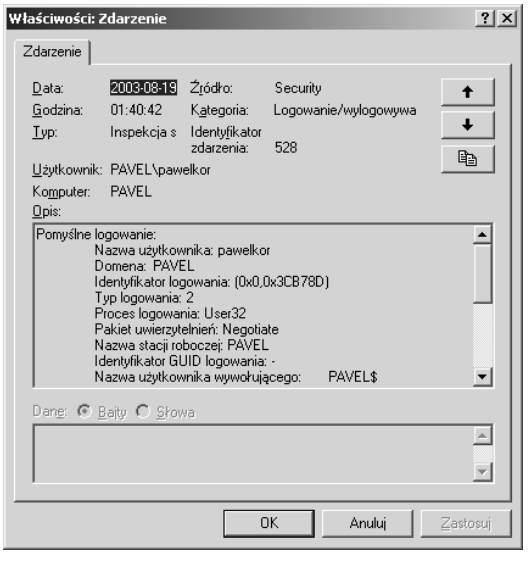
Okno *Wpis inpekcji* (*Auditing Entry*) jest podobne do omówionego wcześniej okna *Wpis uprawnień* (*Permission Entry*). Każdej operacji na liście towarzyszą pola wyboru *Sukces* (*Successful*) i *Niepowodzenie* (*Failed*). Odpowiadają one rejestrowaniu udanych i nieudanych operacji na obiekcie. Aby rejestrować, przykładowo, tworzenie plików, klikamy pole wyboru *Sukces* (*Successful*) dotyczące operacji *Tworzenie plików/Zapis danych* (*Create Files/Write Data*). Zostanie wówczas zarejestrowana każda udana operacja tworzenia pliku.

Poza plikami i folderami inspekcję można włączać dla wielu innych obiektów. W przypadku samodzielnego serwera można rejestrować między innymi operacje logowania. Rejestrowanie tego rodzaju zdarzeń pozostaje związane z odpowiednimi zasadami inspekcji.

Miejscem zapisywania danych inspekcji jest dziennik zabezpieczeń systemu. Zdarzenie logowania zostaje w nim zapisane przy każdym logowaniu użytkownika. Wpisy inspekcji plików i logowania są podobne, ale informacje o logowaniu są obszerniejsze. Przykładowy wpis przedstawia rysunek 6.22.

Zasady grup

Zasady grup (ang. *group policies*) to najbardziej wszechstronne narzędzie do dostosowywania zabezpieczeń systemu Windows Server 2003 dostępne w warunkach infrastruktury Active Directory. Zasady definiuje się przy użyciu narzędzia *Active Directory Users and Computers* (*Użytkownicy i komputery usługi Active Directory*). Mogą dotyczyć wybranych użytkowników, grup lub komputerów łączonych w **jednostki organizacyjne** (ang. *organizational unit*, OU), **lokacje** (ang. *site*) i **domeny**. Każdą pojedynczą zasadę określa się jako *Group Policy Object* (GPO, obiekt zasad grup). Zbiór GPO to zasady grupy. Każda jednostka organizacyjna, lokacja i domena ma domyślny obiekt GPO dotyczący wszystkich obiektów w tej OU, lokacji lub domenie. Poza modyfikowaniem zasad domyślnych istnieje możliwość dodawania nowych, w celu wprowadzenia logicznych podziałów zasad. Zasady wiąże też system priorytetów prowadzący do zastąpienia pewnych zasad



Rysunek 6.22. *Wpis dziennika utworzony po uaktywnieniu zasady Przeprowadź inspekcję zdarzeń logowania zawiera nazwę użytkownika i stacji, z której korzysta, jak również inne, bardziej techniczne informacje*

innymi. Jeżeli domyślny obiekt GPO domeny ma najwyższy priorytet i wprowadzamy w nim pewien parametr, parametr ten zastąpi ustawienia wprowadzone przez dowolne inne zasady.

Poza możliwością definiowania obiektu GPO dla jednostki OU, lokacji lub domeny może on być wiązany z innymi OU, lokacjami lub domenami. Jest to ułatwienie, gdy mamy wiele jednostek organizacyjnych, w których stosowane są te same zasady zabezpieczeń. Obiekt GPO wystarczy wówczas zdefiniować tylko raz.

Tworzenie i usuwanie obiektów GPO

Do konfigurowania zasad grup służy konsola *Active Directory Users and Computers* (*Użytkownicy i komputery usługi Active Directory*).

1. Otwieramy narzędzie, korzystając z polecenia menu *Start/Narzędzia administracyjne/Użytkownicy i komputery usługi Active Directory* (*Start/Administrative Tools/Active Directory Users and Computers*).
2. Klikamy prawym przyciskiem myszy nazwę domeny, lokacji lub jednostki organizacyjnej, dla której konfigurować będziemy zasady grupy. W menu podręcznym klikamy *Właściwości* (*Properties*).
3. Klikamy zakładkę *Zasady grupy* (*Group Policy*), aby wywołać kartę przedstawioną na rysunku 6.23. Na karcie wyświetlana jest lista istniejących obiektów GPO konfigurowanej domeny lub powiązanych z konfigurowaną domeną.

Tworzenie nowego obiektu GPO

Tworzenie nowego obiektu GPO jest stosunkowo proste. Na karcie *Zasady grupy* (*Group Policy*) klikamy w tym celu przycisk *Nowy* (*New*). Wprowadzamy nazwę nowego obiektu GPO i wciskamy *Enter*. Na liście GPO pojawi się wówczas nowy wpis.

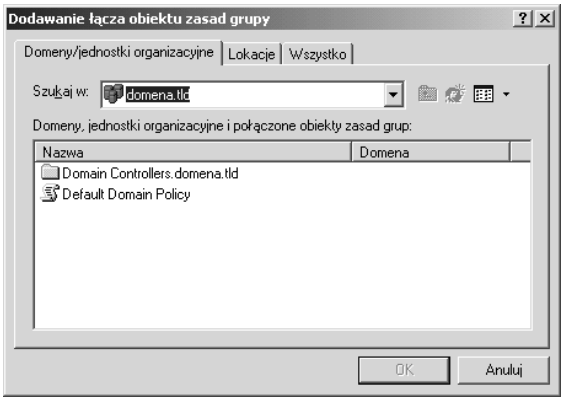
Rysunek 6.23.
Karta Zasady grupy arkusza właściwości domeny służy do konfigurowania zasad grup

Dodawanie połączonych obiektów GPO

Aby dodać łącze do obiektu GPO w innej jednostce organizacyjnej, lokacji lub domenie, wykonujemy następujące czynności:

1. Na karcie *Zasady grupy* (*Group Policy*) klikamy przycisk *Dodaj* (*Add*). Powoduje to otwarcie okna *Dodawanie łącza obiektu zasad grupy* (*Add a Group Policy Object link*), przedstawionego na rysunku 6.24. Standardowo wyświetlane są wyłącznie GPO domen i jednostek organizacyjnych.

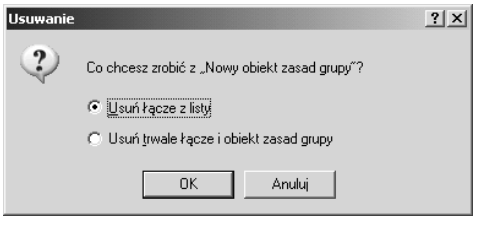
Rysunek 6.24.
Okno Dodawanie łącza obiektu zasad grupy służy do łączenia GPO domeny, lokacji lub OU z inną domeną, lokacją lub OU



2. Klikamy zakładkę *Lokacje* (*Sites*), aby wyświetlić obiekty GPO lokacji lub zakładkę *Wszystkie* (*All*), aby wyświetlić wszystkie obiekty GPO katalogu Active Directory.
3. Z jednej z trzech list wybieramy obiekt GPO i klikamy *OK*. Połączony obiekt GPO zostanie wyświetlony na liście na karcie *Zasady grupy* (*Group Policy*).

Usuwanie obiektu GPO

Aby usunąć obiekt GPO lub łącze do obiektu GPO, wybieramy go z listy na karcie *Zasady grupy* (*Group Policy*) i klikamy przycisk *Usuń* (*Delete*). Wyświetlone zostaje okno dialogowe przedstawione na rysunku 6.25. Umożliwia ono usunięcie albo samego łącza do obiektu GPO, albo łącza wraz z obiektem. Zawsze należy uważać, aby nie usunąć przez pomyłkę obiektów GPO, które zostały powiązane z innymi jednostkami organizacyjnymi, lokacjami lub domenami. Usunięcie obiektu GPO ma charakter globalny i nie będzie on po takiej operacji dostępny. Gdy obiekt GPO wciąż jest w użyciu, wybieramy opcję usunięcia łącza. Kliknięcie *OK* kończy operację.



Rysunek 6.25. *Po kliknięciu przycisku Usuń można wybrać pomiędzy usunięciem obiektu GPO a jedynie łącza do niego*

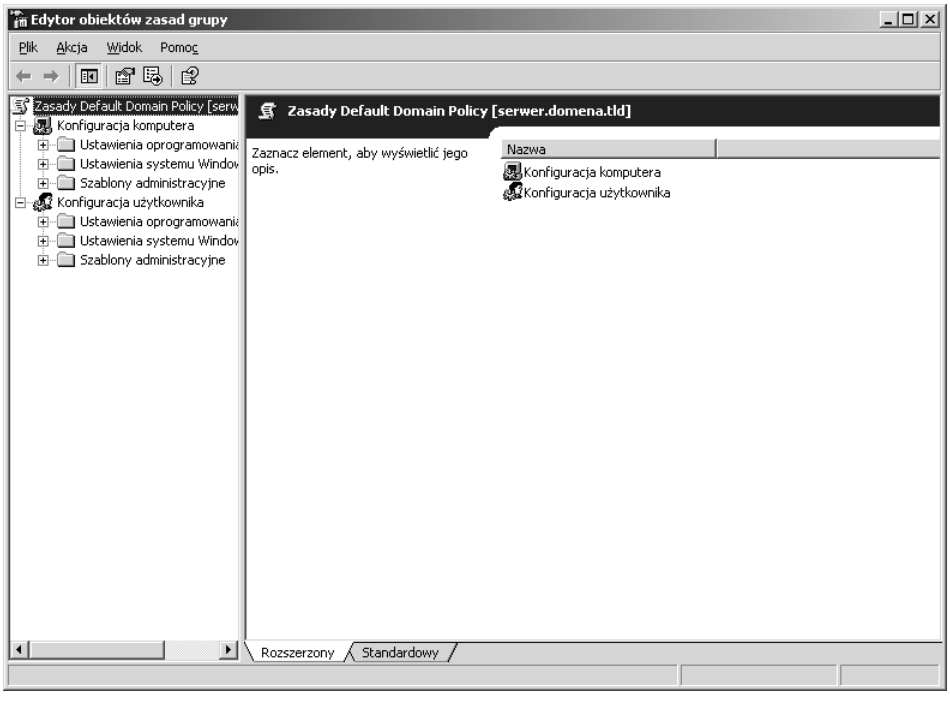
Modyfikowanie obiektów GPO

Modyfikowanie obiektów zasad grup to operacja prowadząca do faktycznego zdefiniowania zasad dla OU, lokacji lub domeny, której obiekt GPO zostanie przypisany. Procedura wprowadzania zmian w GPO polega na wybraniu właściwego obiektu w drzewie narzędzia *Edytor obiektów zasad grup* (*Group Policy Object Editor*) i zmianie ustawień tego obiektu. Rozpoczynamy ponownie od polecenia menu *Start/Narzędzia administracyjne/Użytkownicy i komputery usługi Active Directory* (*Start/Administrative Tools/Active Directory Users and Computers*).

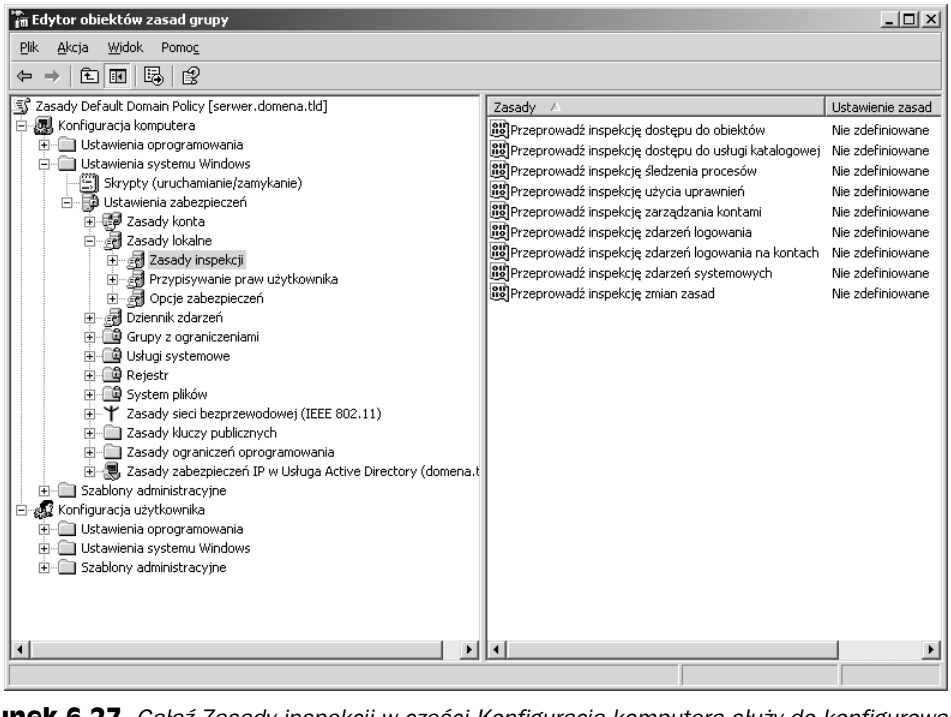
1. W oknie konsoli MMC klikamy prawym przyciskiem myszy nazwę domeny, lokacji lub jednostki organizacyjnej, dla której konfigurować będziemy zasady grupy. W menu podręcznym klikamy *Właściwości* (*Properties*).
2. Klikamy zakładkę *Zasady grupy* (*Group Policy*).
3. Wybieramy obiekt *GPO* i klikamy *Edytuj* (*Edit*), aby wywołać Edytor obiektów zasad grup (*Group Policy Object Editor*), przedstawiony na rysunku 6.26.

Edytor GPO jest podzielony na dwie części — *Konfiguracja komputera* (*Computer Configuration*) i *Konfiguracja użytkownika* (*User Configuration*). Są to kategorie zapewniające logiczne oddzielenie ustawień związanych z komputerami od ustawień związanych z użytkownikami. Jeżeli w jednostce OU, lokacji lub domenie są zarówno komputery, jak i użytkownicy, ustawienia konfiguracji komputera są stosowane w odniesieniu do obiektów typu komputer, a ustawienia konfiguracji użytkownika — do obiektów typu użytkownik.

Nie możemy w tym rozdziale opisać wszystkich ustawień dostępnych w edytorze GPO, ale znaczenie większości z nich jest dość oczywiste. Dla przykładu, przejdźmy do gałęzi *Konfiguracja komputera*/*Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady lokalne/Zasady inspekcji* (*Computer Configuration/Windows Settings/Security Settings/Local Policies/Audit Policy*), jak przedstawia to rysunek 6.27.



Rysunek 6.26. *Edytor obiektów GPO służy do określania zasad zapisanych w wybranym GPO*



Rysunek 6.27. *Gałąź Zasady inspekcji w części Konfiguracja komputera służy do konfigurowania lokalnych zasad inspekcji komputerów*

Nieco wcześniej w tym rozdziale przedstawiliśmy sposób włączania funkcji inspekcji komputera przy użyciu konsoli *Zasady zabezpieczeń lokalnych* (*Local Security Policy*). Wspomnieliśmy również o możliwości wykorzystania zasad grup do prostego włączenia inspekcji w obrębie całej domeny. Otwarliśmy teraz tę część drzewa obiektów zasad grup, która odpowiada za funkcje inspekcji. Wyświetlana lista jest podobna do znanej z narzędzia *Zasady zabezpieczeń lokalnych* (*Local Security Policy*). Aby włączyć rejestrowanie pewnego rodzaju zdarzeń, podwójnie klikamy odpowiedni wpis w prawym obszarze okna lub klikamy prawym przyciskiem myszy i wybieramy polecenie *Właściwości* (*Properties*). Wyświetlone zostaje wówczas okno właściwości dotyczące danej zasady. Przykład przedstawia rysunek 6.28. Można rejestrować zdarzenia udane, nieudane lub wszystkie. Klikamy *OK*, aby zapisać wprowadzone zmiany. Odpowiednio powinna zmienić się wówczas zawartość okna edytora.

Rysunek 6.28.
Okno właściwości zasady służy do jej włączania, wyłączania i określania opcji konfiguracyjnych

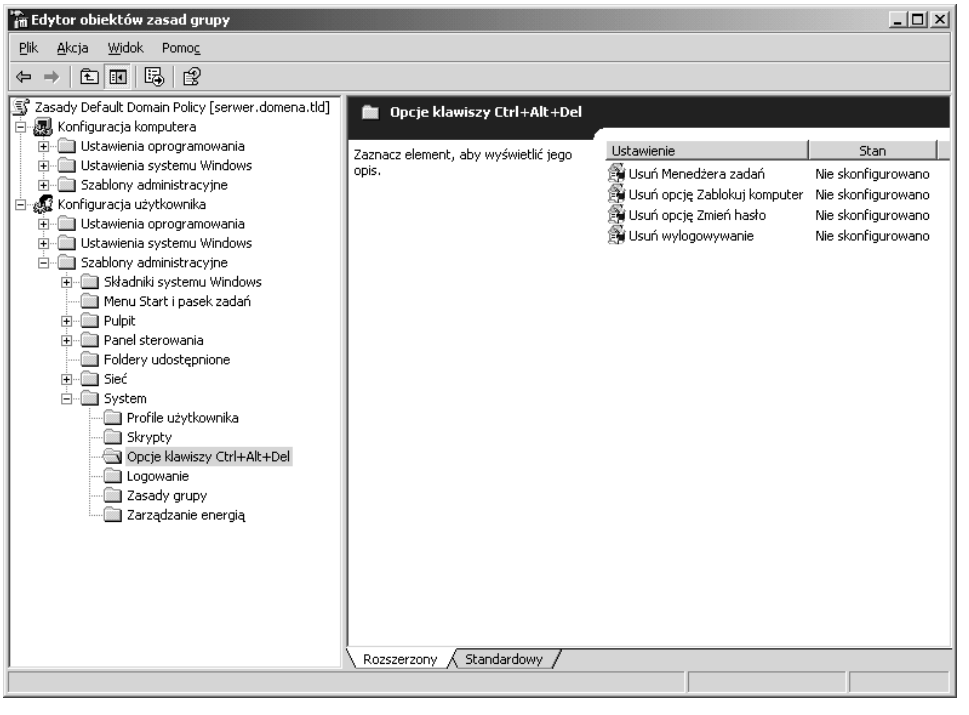
Zmiany wprowadzane w edytorze GPO są bezzwłocznie zapisywane w obiektach GPO.

Przykładem ustawień konfiguracji użytkownika mogą być tzw. opcje *Ctrl+Alt+Del*, przedstawione na rysunku 6.29, dostępne w gałęzi *Konfiguracja użytkownika/Szablony administracyjne/System* (*User Configuration/Administrative Templates/System*). Zbiór dostępnych opcji wyświetlany jest w prawym obszarze okna. Jest to grupa ustawień określających, jakie przyciski zostaną wyświetlone, gdy użytkownik, którego dotyczy GPO, wciśnie kombinację klawiszy *Ctrl+Alt+Del*. Aby wyłączyć wyświetlanie wybranego przycisku, podwójnie klikamy odpowiednie ustawienie, wprowadzamy zmianę ustawienia i klikamy *OK*.

Zasady grup mogą być wykorzystywane do wspomagania najróżniejszych czynności administracyjnych, od zabezpieczania stacji roboczych i określania zasad kont użytkowników po automatyczne instalowanie oprogramowania.

Zabezpieczenia obiektu GPO

Dla samego obiektu GPO można zdefiniować tylko kilka ustawień konfiguracji zabezpieczeń, określających uprawnienia do wykonywania operacji na nim.



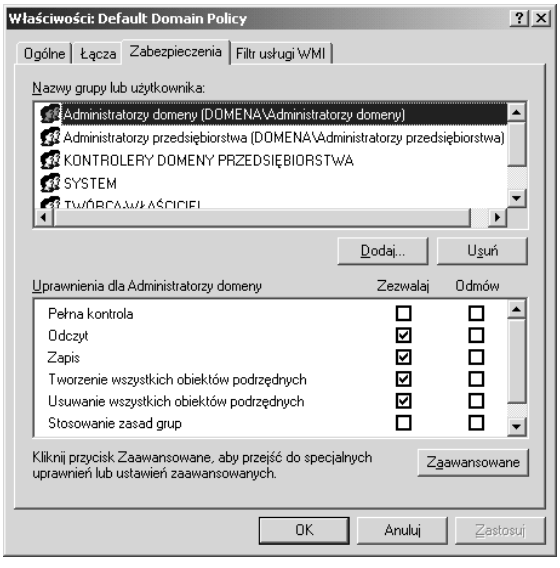
Rysunek 6.29. *Zarówno dla użytkowników i dla komputerów dostępne są ogromne zbiory zasad*

1. W konsoli *Active Directory Users and Computers* (*Użytkownicy i komputery usługi Active Directory*) lokalizujemy OU, lokację lub domenę, której obiekt GPO będziemy modyfikować, klikamy ją prawym przyciskiem myszy i wybieramy polecenie *Właściwości* (*Properties*).
2. Klikamy zakładkę *Zasady grupy* (*Group Policy*), wybieramy obiekt GPO i klikamy przycisk *Właściwości* (*Properties*).
3. W oknie *Właściwości GPO* klikamy zakładkę *Zabezpieczenia* (*Security*), aby wywołać kartę przedstawioną na rysunku 6.30.

Ustawienia zabezpieczeń są podobne do modelu znanego z uprawnień do plików: zapis, odczyt, tworzenie obiektów, usuwanie obiektów itd. Odpowiednia konfiguracja umożliwia delegowanie uprawnień do modyfikowania GPO użytkownikom, którzy nie należą do grupy *Administratorzy domeny* (*Domain Admins*).

Po kliknięciu przycisku *Zaawansowane* (*Advanced*) można konfigurować uprawnienia na bardziej złożonym poziomie. Ich ziarnistość jest tak wielka, że nie wymienimy nawet pełnej listy dostępnych opcji. W większości przypadków podstawowy zestaw prostych uprawnień będzie w zupełności wystarczający.

Rysunek 6.30. *Karta Zabezpieczenia arkusza właściwości GPO służy do konfigurowania zabezpieczeń samego obiektu GPO*



Internet Connection Firewall (ICF)

Internet Connection Firewall (ICF, zapora połączenia internetowego) to element, który raczej rzadko będzie wykorzystywany w konfiguracji systemów Windows Server 2003. W większości środowisk stosuje się kompletną, niezależną zaporę firewall. Zapora ICF pozostaje jednak kuszącym rozwiązaniem dla mniejszych sieci.

Zewnętrzne zapory firewall stosuje się do zabezpieczania przed atakami całych sieci. Zapora ICF jest przydatna w mniej rozbudowanym środowisku, na przykład pojedynczego serwera przyłączonego do Internetu połączeniem DSL lub kablowym.

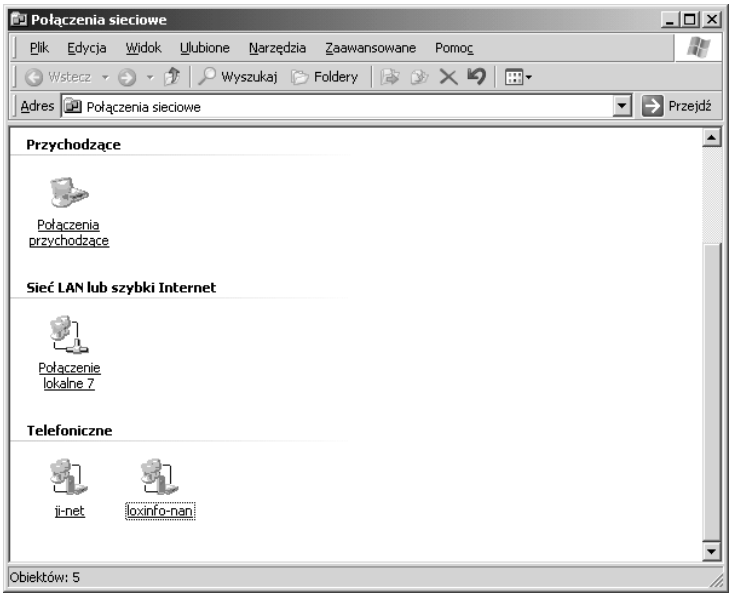
Zagadnienia związane z zewnętrznymi zaporami firewall będziemy omawiać w rozdziale 16. i kolejnych.

W tak prostej implementacji zapora firewall nie ma czasem uzasadnienia finansowego (choć najprostsze produkty tego rodzaju można nabyć już za 1000 zł). Nie można jednak pozostawić serwera całkowicie otwartego na ataki. Wówczas możemy zdać się na zaporę ICF.

Zapora ICF to produkt z rodziny osobistych zapór firewall. Jest to pełna implementacja zapory z inspekcją stanową (mechanizm tego rodzaju opisujemy w rozdziale 16.) chroniąca całość komunikacji przez wybrane połączenie sieciowe.

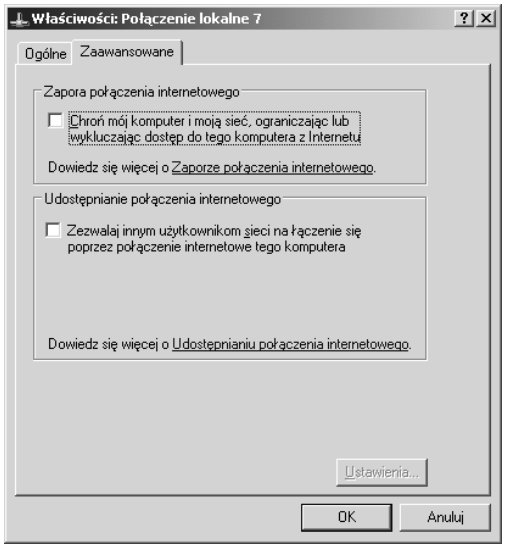
Przed uaktywnieniem zapory ICF musimy wybrać chronione połączenie sieciowe (połączenie z Internetem). Gdy mamy tylko jedno połączenie z Internetem, pozostaje kliknąć prawym przyciskiem myszy ikonę *Moje miejsca w sieci* (*My Network Places*) na pulpicie i wybrać *Właściwości* (*Properties*). Otwarte zostanie wówczas okno *Połączenia sieciowe* (*Network Connections*), przedstawione na rysunku 6.31.

Rysunek 6.31. *Okno połączeń sieciowych prezentuje wszystkie przyłącza sieciowe komputera*



W oknie znajdziemy wszystkie połączenia sieciowe komputera, w tym połączenia LAN, VPN i telefoniczne. W przedstawionym na rysunku przykładzie widzimy dwa przyłącza. Do komunikacji z Internetem wykorzystywane jest pierwsze z nich. Dla niego właśnie włączymy zaporę. Klikamy połączenie prawym przyciskiem myszy i wybieramy *Właściwości* (*Properties*). Następnie wywołujemy kartę *Zaawansowane* (*Advanced*), przedstawioną na rysunku 6.32.

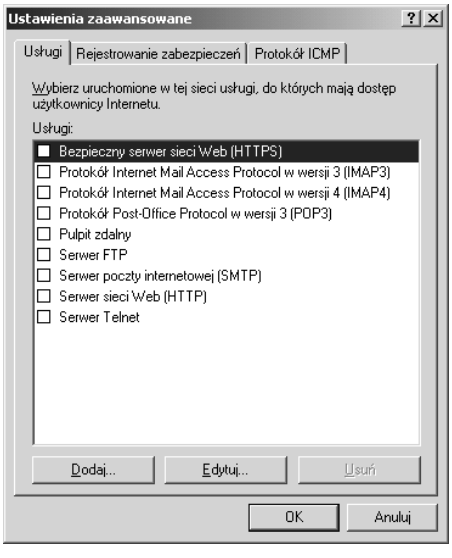
Rysunek 6.32. *Karta Zaawansowane arkusza właściwości połączenia sieciowego służy do uaktywniania i konfigurowania zapory ICF oraz udostępniania połączenia internetowego (ICS)*



Pierwsze pole wyboru pozwala uaktywnić zaporę. Bezpośrednio po uaktywnieniu zapora nie dopuszcza żadnych połączeń przychodzących. Jest to rozwiązanie idealne dla komputera domowego lub stacji roboczej. W przypadku serwera przyłączonego do Internetu będziemy zainteresowani zapewne umożliwieniem dostępu do serwera WWW lub poczty elektronicznej.

Zapora ICF umożliwia wybieranie pojedynczych usług, dla których dopuszczane będą połączenia przychodzące. Jeżeli więc w komputerze pracuje oprogramowanie serwera WWW, musimy zezwolić na komunikację HTTP. Aby otworzyć odpowiednie okno, korzystamy z przycisku *Ustawienia* (*Settings*) na karcie *Zaawansowane* (*Advanced*) arkusza właściwości połączenia. Spowoduje to otwarcie okna ustawień zaawansowanych, przedstawionego na rysunku 6.33.

Rysunek 6.33. *Karta Usługi okna ustawień zaawansowanych służy do otwierania zapory ICF dla określonych rodzajów połączeń przychodzących*

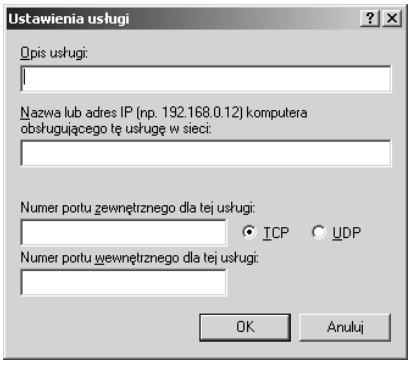


Na karcie *Usługi* (*Services*) jest wyświetlana lista standardowych usług. Zaznaczanie pól wyboru obok nazw powoduje, że zapora przestaje blokować dostęp do nich. W przypadku serwera WWW odpowiednią pozycją będzie *Serwer sieci Web* (*Web Server*). Po zaznaczeniu pola wyboru wyświetlone zostanie okno wymagające podania nazwy lub adresu IP komputera, w którym usługa jest uruchomiona. W tym przypadku będzie to nazwa komputera lokalnego.

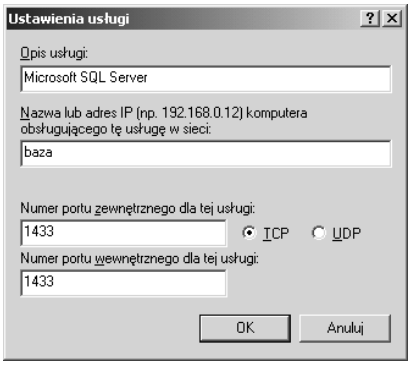
Lista usług jest dość krótka. W komputerze mogą pracować inne usługi, do których również musimy zapewnić dostęp, jak na przykład Microsoft SQL Server. W takich przypadkach dodajemy do listy nową pozycję.

1. Klikamy przycisk *Dodaj* (*Add*), aby otworzyć okno ustawień usługi, przedstawione na rysunku 6.34.
2. Wprowadzamy opis usługi.
3. Określamy, w którym komputerze usługa pracuje, wprowadzając jego nazwę lub adres IP. Definicja usługi może dotyczyć zarówno komputera lokalnego, jak i komputera korzystającego z udostępnianego połączenia internetowego.
4. Określamy numer portu usługi. Microsoft SQL Server korzysta z portu 1433 i protokołu TCP. Rysunek 6.35 przedstawia przykładowe ustawienia usługi Microsoft SQL Server.

Rysunek 6.34.
Okno Ustawienia usługi służy do dołączania lub modyfikowania wpisów usług rozpoznawanych przez ICF



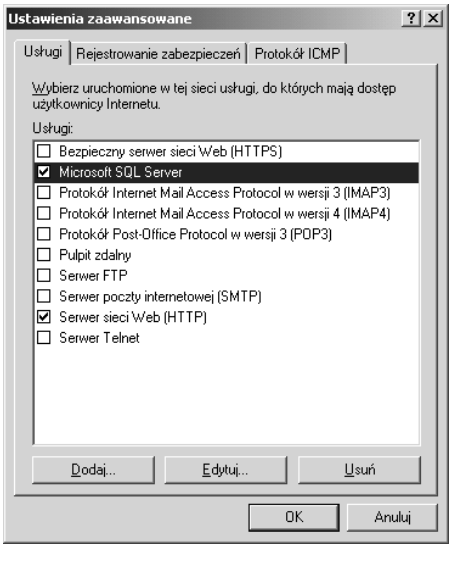
Rysunek 6.35.
Okno ustawień usługi używane do zdefiniowania w konfiguracji zapory połączeń przychodzących z usługą Microsoft SQL Server



5. Klikamy *OK*, aby zapisać definicję.

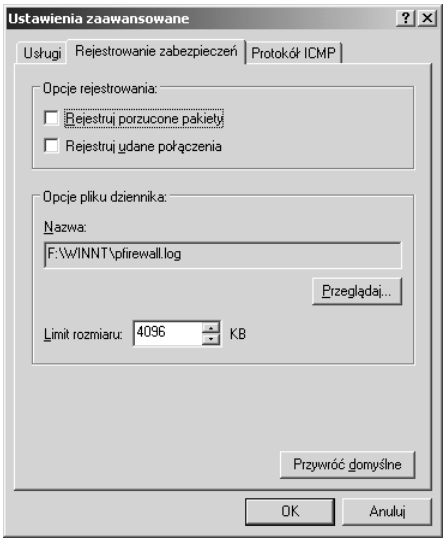
Rysunek 6.36 przedstawia uzupełnioną listę usług na karcie *Usługi*. W tym przykładzie zapora zezwala wyłącznie na połączenia z usługami WWW i Microsoft SQL Serverem. Wszystkie inne wywołania są blokowane.

Rysunek 6.36.
Karta Usługi okna Ustawienia zaawansowane z ustawieniami, które zezwalają na zewnętrzne wywołania lokalnych usług WWW i Microsoft SQL Server



Okno ustawień zaawansowanych pozwala konfigurować dodatkowe funkcje zapory ICF. Zapora ICF może rejestrować nieudane wywołania przychodzące i (lub) udane wywołania wychodzące. Odpowiednie opcje znajdziemy na karcie *Rejestrowanie zabezpieczeń* (*Security Logging*) okna *Ustawienia zaawansowane* (*Advanced Settings*), przedstawionej na rysunku 6.37.

Rysunek 6.37. *Karta Rejestrowanie zabezpieczeń okna Ustawienia zaawansowane służy do włączania i wyłączania funkcji rejestrowania połączeń*



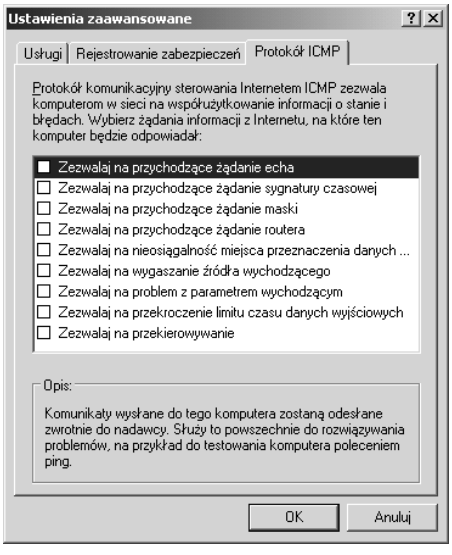
Pierwsza z opcji rejestrowania dotyczy podejmowanych przez użytkowników z zewnątrz i zablokowanych przez zaporę prób dostępu do usług komputera. Druga zapewnia śledzenie połączeń wychodzących.

W dolnej części okna dostępny jest przycisk *Przeglądaj* (*Browse*), umożliwiający określenie położenia pliku dziennika zapory oraz pole limitu rozmiaru. Po jego osiągnięciu najstarsze wpisy w dzienniku są zastępowane nowymi. Warto zwrócić uwagę, że funkcje rejestrowania generują stosunkowo duże ilości danych, zwłaszcza w stacjach roboczych z włączoną funkcją rejestrowania udanych połączeń wychodzących.

Ostatnią kartą w oknie ustawień zaawansowanych jest karta *ICMP* przedstawiona na rysunku 6.38. ICMP to prosty protokół używany do przesyłania stosunkowo niewielkich ilości danych związanych z zarządzaniem pracą stosu TCP/IP. Przykładem wykorzystania procedury wymiany komunikatów ICMP może być praca narzędzia `Ping`.

Standardowa konfiguracja zapory ICF uniemożliwia innym użytkownikom sieci Internet wywoływanie komputera poleceniem `Ping` w celu potwierdzenia jego aktywności. Jest to prosta konsekwencja zasady blokowania wszystkich pakietów przychodzących, która obejmuje również żądania ICMP `echo`. Prostą metodą umożliwienia komputerowi odbierania i odpowiadania na żądania `echo` jest włączenie opcji *Zezwalaj na przychodzące żądania echa* (*Allow incoming echo request*) na karcie ICMP.

Na karcie ICMP można znaleźć także opcje związane z mniej znanymi typami komunikatów ICMP. Lista żądań przychodzących (ang. *incoming*) obejmuje stosunkowo nietypowe żądania, jak zapytania o maskę podsieci lub router domyślny. Potrzeba zezwolenia na ich odbieranie raczej nie powinna się pojawić, zwłaszcza w niewielkiej sieci czy w samodzielnym komputerze.



Rysunek 6.38. *Karta ICMP okna ustawień zaawansowanych służy do konfigurowania ograniczeń wymiany pakierów ICMP, zarówno przychodzących, jak i wychodzących*

Żądania wychodzące (ang. *outgoing*) również nie są w zwykłych konfiguracjach wymagane, zwłaszcza gdy zapora chroni jeden komputer. Mogą być potrzebne, gdy stosowany jest routing do sieci lokalnej.

Ostania opcja na liście dotyczy przekazywania pakietów ICMP `redirect`. Są one przesyłane, gdy zmienia się tabela tras routera zdalnego. Mogą jednak doprowadzić do zniekształcenia zawartości tabeli tras komputera i zakłóceń typu DoS. Nie powinny być odbierane ani przez komputer zapory, ani przez komputery w sieci wewnętrznej.

Po zakończeniu konfigurowania zapory ICF klikamy *OK*, aby zamknąć okno ustawień zaawansowanych. Kolejnym kliknięciem *OK* zamykamy okno właściwości połączenia sieciowego, co ostatecznie uaktywnia zaporę.

Podsumowanie

W rozdziale przedstawiliśmy zwięzłe omówienie zagadnienia zabezpieczeń systemu Windows Server 2003. Przedstawiliśmy kolejne środki zapewniające ochronę komputera: konfigurację sprzętową, właściwą instalację systemu operacyjnego, uprawnienia dostępu do plików, mechanizmy rejestrowania oraz zasady grup. Odpowiednie połączenie tych środków pozwala osiągnąć maksymalnie zabezpieczoną konfigurację komputera. Istotne jest, aby nie pominąć istotnych elementów, takich jak system plików NTFS, jedyny, który powinien być stosowany do formatowania partycji systemowej Windows.