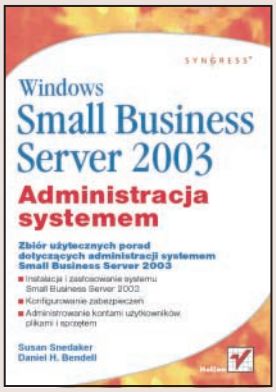
Windows Small Business Server 2003. Administracja systemem



Autorzy: Susan Snedaker, Daniel H. Bendell
Tłumaczenie: Sławomir Dzieniszewski, Marcin Jędrysiak, Piotr Pilch
ISBN: 83-7361-795-7
Tytuł oryginału: How to Cheat at Small Business Server 2003
Format: B5, stron: 440

W wielu firmach administrowaniem serwerami zajmuje się nie administrator, tylko pracownik, dla którego jest to tylko jedno z dziesiątek zadań. Takie osoby rzadko mają czas na poznawanie zawiłości administrowania systemami – potrzebują skutecznych porad ułatwiających szybką i efektywną pracę, a nie precyzyjnych opisów każdej linijki pliku konfiguracyjnego. Dla takich „administratorów mimo woli" zbiór wskazówek może okazać się podstawową lekturą wykorzystywaną w pracy.

Książka „Windows Small Business Server 2003. Administracja systemem" jest przeznaczona właśnie dla tych ludzi, na których znienacka spadło zadanie administrowania firmową siecią opartą na Small Business Server. Książka przedstawia kluczowe zadania realizowane przez serwer, zawiera niezbędne objaśnienia i okna programów, na które natknie się administrator. Nie zasypuje czytelnika zawiłościami technicznymi – koncentruje się raczej na sposobach szybkiego i sprawnego wykonania określonych zadań.

- Komponenty systemu Small Business Server 2003
- Projektowanie sieci komputerowych
- Instalowanie Small Business Server 2003
- Zabezpieczenia systemu i zarządzanie systemami plików
- Administrowanie użytkownikami, grupami i prawami dostępu
- Archiwizowanie i przywracanie danych
- Konfigurowanie serwera poczty elektronicznej
- Zdalny dostęp
- Monitorowanie i analiza działania Small Business Server 2003

Jeśli administrowanie systemem Small Business Server 2003 to tylko jedno z Twoich zadań, znalazłeś wreszcie książkę, której szukałeś.

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

Spis treści

Przedmowa **17**

Rozdział 1. Podstawowe informacje o systemie Windows Small Business Server 2003 ..... **19**

Do czego zmierzamy 19
Funkcje systemu Windows Small Business Server 2003 20
Uproszczone administrowanie i zarządzanie systemem 20
Ulepszony system zabezpieczeń 20
Łatwy dostęp do internetu i poczty elektronicznej 21
Łatwość przygotowywania intranetu 21
Łatwy zdalny dostęp 21
Uproszczone zarządzanie 21
Łatwiejsze zarządzanie danymi 22
Komponenty wchodzące w skład systemu Windows Small Business Server 2003 22
Windows Server 2003 (Standard, Premium) 23
Exchange Server 2003 (Standard, Premium) 23
Outlook 2003 (Standard, Premium) 24
Usługa Microsoft Shared Fax (Standard, Premium) 24
Microsoft SharePoint Services (Standard, Premium) 24
Server ISA (Premium) 24
SQL Server 2000 (Premium) 25
Office FrontPage 2003 (Premium) 25
Ograniczenia systemu Windows Small Business Server 2003 26
Lokalizacja zainstalowanych komponentów 26
Ograniczenia związane z klientami 27
Licencje dostępu klienta (CAL) 27
Systemy operacyjne klientów 28
Tylko jedna domena 28
Który system operacyjny będzie najwłaściwszy w naszej sytuacji? 30
Jeszcze raz 31

Rozdział 2. Zasady działania i projektowania sieci komputerowych **33**

Czego dowiemy się w tym rozdziale 33
Podstawowe terminy związane z komputerami w sieci 34
Podstawy sieci komputerowych 36
Kto rządzi siecią? 36
Łączenie komputerów ze sobą 37
Komunikacja sieciowa 37

Adresy IP, firewalle i tłumaczenie NAT ... 38
Podstawowe zasady adresowania w protokole IP ... 39
Maski podsieci ... 39
Publiczne i prywatne adresy IP ... 42
Firewalle i tłumaczenie NAT ... 43
Projektowanie własnej sieci komputerowej ... 44
Przegląd potrzebnych i posiadanych komponentów ... 45
Przegląd specyfikacji urządzeń i oprogramowania ... 46
Komputer dla serwera ... 46
Specyfikacje serwera SBS ... 47
Specyfikacje klientów serwera SBS ... 48
Inne urządzenia sieciowe ... 49
Tworzenie schematu sieci ... 49
Łączenie naszej sieci w całość i przygotowywanie zabezpieczeń ... 50
Spis połączeń sieciowych, lokalizacji komputerów i użytkowników ... 53
Połączenia sieciowe i lokalizacja komputerów ... 53
Listy użytkowników ... 54
Okablowanie sieci ... 55
Przełączniki i koncentratory w sieci ... 56
Sieci bezprzewodowe ... 56
Prędkość przesyłu danych w sieciach przewodowych i bezprzewodowych ... 57
Wybór nazw dla domeny i komputerów ... 58
Konwencje nazywania domen ... 58
Konwencje nazywania komputerów ... 59
Podsumowanie ... 59

Rozdział 3. Instalacja systemu Small Business Server 2003 ... 61

Do czego zmierzamy ... 61
Przygotowanie do instalacji ... 61
Czysta instalacja systemu ... 62
Uaktualnianie systemu ... 63
Migracja systemu ... 64
Wybór właściwej ścieżki instalacji ... 65
Przygotowanie do instalacji ... 65
Przygotowanie planu odtwarzania i instalacji, uaktualnienia lub migracji systemu ... 66
Przygotowanie zapasowej kopii naszych danych ... 67
Zaplanowanie układu partycji dyskowych ... 67
Przygotowanie serwera do instalacji ... 70
Weryfikacja konfiguracji sieci ... 71
Konfiguracja adresów IP ... 72
Jeszcze ostatni test ... 74
Instalowanie systemu Small Business Server 2003 ... 75
Faza I — instalacja systemu Windows Small Business Server 2003 ... 76
Faza II — kreator instalacji programu Microsoft Windows Small Business Server ... 80
Uaktualnienie starszych systemów do systemu Small Business Server 2003 ... 83
Przygotowania do uaktualnienia systemu ... 84
Przygotowanie serwera ... 85
Przygotowanie klientów ... 88
Przygotowywanie użytkowników ... 88
Uaktualnianie serwera ... 89
Faza I — Kreator instalacji programu Microsoft Windows Small Business Server ... 90
Faza II — Kreator instalacji programu Microsoft Windows Small Business Server ... 92

Migrowanie do systemu Small Business Server 2003 ... 93
Przygotowanie do migracji ... 94
Wykonywanie migracji do systemu SBS ... 95
Lista zadań do wykonania i inne zadania poinstalacyjne ... 96
Wyświetl najważniejsze wskazówki dotyczące zabezpieczeń ... 98
Połącz z internetem ... 98
Bezpośrednie połączenie szerokopasmowe ... 99
Lokalne urządzenie routera z adresem IP ... 101
Połączenie wymagające nazwy użytkownika i hasła (PPPoE) ... 103
Połączenie telefoniczne ... 103
Konfigurowanie firewalla ... 104
Konfigurowanie poczty elektronicznej ... 107
Konfigurowanie zasad haseł ... 108
Skanowanie w poszukiwaniu ważnych aktualizacji systemu ... 108
Konfigurowanie zdalnego dostępu do sieci ... 109
Zdalny dostęp do sieci za pośrednictwem VPN ... 110
Zdalny dostęp za pośrednictwem linii telefonicznej ... 111
Aktywacja serwera ... 112
Dodawanie licencji klientów ... 113
Migrowanie uprawnień naszych użytkowników ... 113
Zadania związane z zarządzaniem systemem ... 114
Podsumowanie ... 115

Rozdział 4. Zabezpieczenia ... 117
Czego dowiemy się w tym rozdziale ... 117
Ogólne informacje na temat zabezpieczeń serwera Small Business Server 2003 ... 118
Rodzaje zabezpieczeń ... 118
Topologie sieci i konfiguracja firewalla ... 119
Połączenia sieciowe ... 120
Zabezpieczenia sieci bezprzewodowych ... 121
Zabezpieczanie serwera ... 122
Bezpieczeństwo fizyczne serwera ... 122
Zabezpieczanie konfiguracji ... 123
Zabezpieczanie oprogramowania ... 126
Zabezpieczanie stacji roboczych ... 128
Zabezpieczanie kont użytkowników ... 129
Edukowanie użytkowników ... 129
Wymóg stosowania złożonych haseł ... 130
Sprawdzenie, czy użytkownikom przypisano tylko niezbędne uprawnienia ... 131
Monitorowanie, rejestrowanie i inspekcja ... 132
Konfigurowanie monitorowania i raportowania ... 133
Inspekcja kluczowych zdarzeń ... 133
Inspekcja zdarzeń związanych z nieudanymi operacjami logowania ... 133
Inspekcja zdarzeń związanych z blokowaniem kont ... 134
Narzędzie Security Guidance Kit firmy Microsoft ... 134
Podsumowanie ... 137

Rozdział 5. Zarządzanie dyskami ... 139
Czego dowiemy się w tym rozdziale ... 139
Terminologia ... 139
Terminologia związana z dyskami ... 140
Terminologia związana z urządzeniami pamięci masowej ... 141
Zagadnienia dotyczące dysków dynamicznych ... 143
Woluminy podstawowe ... 144
Woluminy rozłożone ... 145

Woluminy paskowane (RAID-0) ... 146
Woluminy dublowane (RAID-1) ... 147
Wolumin paskowany z parzystością (RAID-5) ... 148
Zarządzanie dyskami serwera ... 149
Konsola Zarządzanie dyskami ... 149
Zastosowanie partycji ... 150
Tworzenie partycji ... 151
Tworzenie nowego dysku logicznego partycji rozszerzonej ... 153
Usuwanie partycji lub dysku logicznego ... 154
Konwertowanie dysku podstawowego na dynamiczny ... 154
Zastosowanie dysków dynamicznych ... 155
Tworzenie woluminu ... 155
Usuwanie woluminu ... 156
Montowanie woluminu ... 156
Zastosowanie zestawów dublowanych (lustrzanych) ... 158
Utworzenie zestawu dublowanego ... 158
Usuwanie zestawu dublowanego ... 160
Rozdzielanie zestawu dublowanego ... 161
RAID-5 ... 161
Identyfikowanie problemów z dyskami ... 162
Podsumowanie ... 164

Rozdział 6. Zarządzanie przechowywaniem plików ... 167
Czego dowiemy się w tym rozdziale ... 167
Konfigurowanie przydziałów dyskowych i zarządzanie nimi ... 167
Uzyskiwanie informacji na temat przydziałów dyskowych ... 168
Definiowanie przydziałów dyskowych dla określonych użytkowników ... 171
Importowanie i eksportowanie przydziałów dyskowych ... 173
Raporty dotyczące przydziałów dysków ... 175
Zarządzanie szyfrowaniem plików ... 175
Agent odzyskiwania zaszyfrowanych plików ... 177
Kompresja dysków i plików ... 178
Zagadnienia dotyczące tworzenia kopii w tle ... 180
Uruchamianie wykonywania kopii w tle dla udostępnianych katalogów ... 181
Konfigurowanie klientów pod kątem stosowania kopii tworzonych w tle ... 182
Podsumowanie ... 185

Rozdział 7. Zarządzanie użytkownikami i grupami ... 187
Czego dowiemy się w tym rozdziale ... 187
Zagadnienia dotyczące grup oraz tworzenie ich i zarządzanie nimi ... 187
Zagadnienia dotyczące grup ... 188
Wbudowane grupy ... 188
Zarządzanie grupami ... 190
Grupy zabezpieczeń ... 190
Grupy dystrybucyjne ... 192
Zagadnienia dotyczące kont użytkowników oraz tworzenie ich i zarządzanie nimi ... 195
Konta użytkowników ... 195
Tworzenie kont użytkowników ... 196
Dodawanie użytkowników do grup lub ich usuwanie ... 198
Zarządzanie szablonami użytkowników ... 200
Zmiana lokalizacji katalogu Moje dokumenty powiązanego z kontami użytkowników ... 204
Usuwanie lub wyłączanie kont użytkowników ... 205
Zagadnienia dotyczące profili użytkowników i zarządzanie nimi ... 206
Korzystanie z konta Administrator ... 209
Podsumowanie ... 210

Rozdział 8. Uprawnienia, udziały i zasady grupy ... 213
Czego dowiemy się w tym rozdziale ... 213
Ogólne informacje na temat uprawnień ... 213
Kontrola dostępu oparta na uprawnieniach NTFS ... 214
Uprawnienia udziału ... 216
Konfigurowanie uprawnień i zarządzanie nimi ... 217
Reguły i wyjątki ... 217
Zasady dziedziczenia ... 219
Określanie uprawnień czynnych ... 221
Właściciele ... 221
Inspekcja ... 222
Zasady grupy ... 223
Konfigurowanie zasad grupy i zarządzanie nimi ... 225
Tworzenie i usuwanie obiektów zasad grupy ... 226
Zarządzanie kolejnością dziedziczenia ... 230
Zarządzanie kolejnością stosowania ... 231
Przeglądanie i definiowanie zakresu obiektu GPO ... 231
Archiwizowanie i przywracanie obiektów GPO ... 233
Przewidywanie wyników działania obiektów GPO ... 235
Zastosowanie obiektów GPO do automatycznej aktualizacji stacji roboczych ... 238
Zastosowanie obiektów GPO do inspekcji zdarzeń ... 240
Podsumowanie ... 242

Rozdział 9. Zarządzanie stacjami roboczymi ... 245
Czego dowiemy się w tym rozdziale ... 245
Ogólne informacje na temat zarządzania stacjami roboczymi ... 245
Translacja adresów sieciowych i konfigurowanie adresów IP ... 246
Konfigurowanie translacji NAT (firewalla) ... 246
Podstawowe informacje dotyczące protokołu DHCP ... 248
Pula adresów ... 249
Dzierżawa adresów ... 249
Zastrzeżenia ... 250
Opcje zakresu ... 250
Wykluczanie adresów ... 251
Konfigurowanie komputerów i podłączanie ich do sieci ... 252
Konfigurowanie stacji roboczych ... 252
Podłączanie stacji roboczych do sieci ... 254
Korzystanie ze stacji roboczych pracujących pod kontrolą starszych wersji systemu Windows ... 256
Instalowanie aplikacji na komputerach znajdujących się w sieci ... 257
Zastosowanie usług Windows Update i Software Update Services ... 258
Usługa Windows Update ... 259
Ręczne użycie usługi Windows Update ... 259
Automatyczne korzystanie z usługi Windows Update ... 260
Zastosowanie usługi Windows Update przy użyciu zasad grupy ... 261
Usługa SUS ... 264
Podsumowanie ... 266

Rozdział 10. Instalowanie drukarek i zarządzanie nimi ... 269
Czego dowiemy się w tym rozdziale ... 269
Ogólne informacje na temat drukarek ... 269
Drukarki logiczne i fizyczne ... 270
Instalowanie drukarek i zarządzanie nimi ... 272
Dodawanie drukarki lokalnej ... 272
Dodawanie drukarki sieciowej ... 273

Zarządzanie zainstalowanymi drukarkami ... 275
Włączanie inspekcji drukarki ... 277
Tworzenie puli drukarek ... 278
Zarządzanie buforowaniem drukarek ... 278
Zarządzanie priorytetami drukarki przy użyciu sterowników (drukarek logicznych) ... 280
Zarządzanie serwerem wydruków ... 280
Zarządzanie drukarkami faksowymi i udostępnianie usługi faksowania ... 283
Zarządzanie drukarkami faksowymi ... 283
Udostępniona usługa faksowania ... 284
Narzędzie Urządzenia i dostawcy ... 285
Narzędzie Routing przychodzący ... 285
Narzędzie Routing wychodzący ... 285
Narzędzie Strony tytułowe ... 286
Narzędzie Konsola faksu ... 286
Zasady grupy powiązane z drukarkami ... 286
Podsumowanie ... 289

Rozdział 11. Plan awaryjny oraz archiwizowanie i przywracanie danych ... 291
Czego dowiemy się w tym rozdziale ... 291
Plan awaryjny ... 291
Określenie zagrożeń i ustalenie dla nich priorytetów ... 293
Kwestie natury prawnej ... 294
Oszacowanie zasobów ... 294
Reakcja na zdarzenie ... 294
Testowanie planu i zarządzanie nim ... 295
Archiwizowanie danych ... 295
Zagadnienia dotyczące archiwizowania danych ... 296
Nośnik archiwizujący ... 298
Zarządzanie nośnikami archiwizującymi ... 298
Narzędzie Kopia zapasowa ... 299
Automatyczne przywracanie systemu ... 302
Status archiwizacji ... 303
Narzędzie Konsola odzyskiwania ... 305
Przywracanie serwera i danych ... 306
Proces całkowitego przywracania ... 306
Instalacja systemu operacyjnego ... 307
Przywracanie serwera przy użyciu kopii zapasowej ... 307
Sprawdzanie poprawności operacji przywracania ... 309
Częściowe przywracanie plików i katalogów ... 309
Przywracanie katalogów i plików przy użyciu funkcji tworzącej w tle kopie udostępnionych zasobów ... 310
Przywracanie katalogów i plików z nośnika archiwizującego ... 310
Przywracanie usuniętej wiadomości poczty elektronicznej ... 311
Podsumowanie ... 311

Rozdział 12. Serwer Exchange Server i program Outlook 2003 ... 315
Czego dowiemy się w tym rozdziale ... 315
Ogólne informacje na temat serwera Microsoft Exchange Server ... 315
Komponenty serwera Exchange Server ... 316
Sekcja Global Settings ... 317
Sekcja Recipients ... 318
Sekcja Servers ... 318
Sekcja Connectors ... 318

Sekcja Tools ... 319
Sekcja Folders ... 319
Korzystanie z serwera Exchange Server ... 320
Dodawanie grupy dystrybucyjnej ... 321
Zarządzanie pocztą elektroniczną opartą na protokole POP3 ... 322
Tworzenie skrzynki pocztowej POP3 ... 324
Definiowanie harmonogramu dostarczania wiadomości za pomocą protokołu POP3 ... 326
Synchronizowanie wiadomości poczty elektronicznej ... 327
Zmiana hasła poczty elektronicznej ... 327
Tworzenie skrzynek pocztowych dla użytkowników ... 327
Zarządzanie skrzynkami pocztowymi użytkowników serwera Exchange Server ... 329
Narzędzie Queue Viewer ... 330
Monitorowanie serwera i statusu złączy ... 330
Narzędzie Message Tracking Center ... 331
Tworzenie publicznych katalogów i zarządzanie nimi ... 331
Tworzenie hierarchii ... 332
Tworzenie struktury nazw ... 332
Zapisywanie zasad dotyczących przechowywania danych ... 333
Tworzenie zasad dotyczących zarządzania publicznymi katalogami ... 333
Korzystanie z programu Outlook 2003 ... 334
Narzędzie Outlook Web Access ... 335
Łączenie się z serwerem Outlook Web Access ... 336
Narzędzie Outlook Mobile Access ... 337
Narzędzie Exchange ActiveSync 3.7 ... 338
Podsumowanie ... 339

Rozdział 13. Zarządzanie zdalnym połączeniem ... 341

Czego dowiemy się w tym rozdziale ... 341
Ogólne informacje na temat zdalnego połączenia ... 341
Telefoniczny zdalny dostęp ... 342
Konfigurowanie na serwerze telefonicznego zdalnego dostępu ... 343
Wirtualne sieci prywatne ... 344
Konfigurowanie serwera pod kątem połączenia VPN ... 344
Konfigurowanie zdalnego dostępu na stacjach roboczych ... 345
Komputer aktualnie podłączony jest do sieci ... 346
Komputery nie są podłączone do sieci ... 347
Pobieranie programu Menedżer połączeń za pomocą narzędzia Zdalne miejsce pracy w sieci Web ... 347
Określanie ustawień użytkowników związanych ze zdalnym dostępem ... 347
Zastosowanie narzędzia Zdalne miejsce pracy w sieci Web ... 348
Uaktywnianie i konfigurowanie narzędzia Zdalne miejsce pracy w sieci Web ... 349
Konfigurowanie dostępu dla użytkowników ... 350
Funkcje narzędzia Zdalne miejsce pracy w sieci Web przeznaczone dla użytkowników ... 350
Funkcja Odczytaj moją firmową pocztę e-mail ... 351
Dostęp do pulpitu mojego komputera w pracy ... 351
Użyj udostępnianej aplikacji firmowej ... 351
Wyświetl wewnętrzną witrynę sieci Web firmy ... 351
Wyświetl raport o użyciu serwera ... 351
Podłącz mój komputer zdalny do sieci ... 352
Informacje i odpowiedzi ... 352
Funkcje narzędzia Zdalne miejsce pracy w sieci Web przeznaczone dla administratora ... 352

Certyfikaty ... 353
Dostęp bezprzewodowy ... 354
Infrastruktura sieci bezprzewodowych ... 356
Komponenty serwera z systemem Windows związane z siecią bezprzewodową ... 356
Ogólne informacje na temat zabezpieczeń sieci bezprzewodowej ... 357
802.11. Weryfikowanie tożsamości i uwierzytelnianie ... 357
802.11. Szyfrowanie WEP (Wired Equivalency Privacy) ... 358
802.11. WPA (Wi-Fi Protected Access) ... 358
802.1X. Uwierzytelnianie i bezpieczeństwo ... 358
Podsumowanie ... 359

Rozdział 14. Użycie programu SharePoint Services ... 361
Czego dowiemy się w tym rozdziale ... 361
Przegląd programu SharePoint Services ... 361
Składniki programu SharePoint ... 363
Górny pasek nawigacji ... 363
Pasek łączy Szybkie uruchamianie ... 364
Grupy lokacji i uprawnienia użytkowników ... 365
Praca z informacją w programie SharePoint ... 366
Dodawanie elementów ... 366
Ewidencjonowanie dokumentów ... 367
Alerty ... 367
Importowanie i eksportowanie plików ... 368
Strony dyskusji i dokumenty ... 368
Witryny i podwitryny ... 368
Dostosowywanie witryny programu SharePoint ... 369
Widok udostępniony i widok osobisty ... 370
Administracja ... 370
Dostosowywanie ... 371
Zarządzanie moimi informacjami ... 372
Zaawansowane administrowanie witryną programu SharePoint ... 372
Konfiguracja serwera wirtualnego ... 373
Konfiguracja zabezpieczeń ... 374
Konfiguracja serwera ... 375
Konfiguracja składnika ... 375
Tworzenie kopii zapasowej i przywracanie plików programu SharePoint ... 376
Podsumowanie ... 377

Rozdział 15. Monitorowanie, dostrajanie i rozwiązywanie problemów ... 379
Czego dowiemy się w tym rozdziale ... 379
Monitorowanie serwera SBS ... 380
Wyświetlanie usług ... 384
Wyświetlanie protokołu zdarzeń ... 385
Typy zdarzeń ... 385
Właściwości dziennika zdarzeń ... 387
Dzienniki zdarzeń ... 387
Dziennik aplikacji ... 388
Dziennik zabezpieczeń ... 388
Dziennik systemu ... 388
Dziennik usług katalogowych ... 388
Dziennik serwera DNS ... 389
Dziennik usługi replikacji plików ... 389

Otwieranie menedżera zadań ... 389
Zmiana ustawień raportów o stanie serwera ... 390
Zmiana powiadomień o alertach ... 391
Zaawansowane narzędzia do monitorowania ... 391
Konsola wydajności: monitor systemu oraz dzienniki wydajności i alerty ... 392
Health Monitor ... 392
Rozwiązywanie problemów — podstawy ... 393
Podstawowe informacje ... 394
Dostrajanie serwera SBS i rozwiązywanie problemów z nim związanych ... 397
Monitorowanie użycia pamięci ... 398
Monitorowanie aktywności procesora ... 401
Monitorowanie operacji na dysku ... 402
Podsumowanie ... 403

Rozdział 16. Funkcje wersji Premium Edition ... 405
Czego dowiemy się w tym rozdziale ... 405
Serwer Internet Security and Acceleration (ISA) Server 2000 ... 405
Instalowanie serwera ISA ... 408
Konfigurowanie serwera ISA ... 412
Instalowanie klienta firewalla ISA ... 413
Przywracanie zdalnego dostępu do witryny programu SharePoint ... 415
Serwer SQL Server 2000 ... 419
Instalowanie serwera SQL Server ... 419
Tworzenie kopii zapasowych baz danych serwera SQL Server ... 423
FrontPage 2003 ... 424
Podsumowanie ... 425

Skorowidz ... 427

Rozdział 4.

Zabezpieczenia

W tym rozdziale:

- Ogólne informacje na temat zabezpieczeń serwera Small Business Server 2003
- Topologie sieciowe i konfiguracja firewalla
- Zabezpieczanie serwera
- Zabezpieczanie stacji roboczych
- Zabezpieczanie kont użytkowników
- Monitorowanie, rejestrowanie i inspekcja

Czego dowiemy się w tym rozdziale

Po przeczytaniu niniejszego rozdziału będziesz dobrze orientował się, jakie są elementy systemu zarządzania zabezpieczeniami serwera Windows Small Business Server 2003 (SBS), a także jak konfigurować i monitorować istotne ustawienia zabezpieczeń. Zabezpieczenia powiązane są ściśle z wszystkimi elementami serwera SBS. W tym rozdziale zawarto podstawowe informacje pozwalające zarządzać bezpieczną siecią z serwerem SBS.

Odwołania do najlepszych praktyk dotyczących zabezpieczeń znajdują się w prawie każdym rozdziale książki. Niniejszy rozdział ma spełniać rolę przewodnika pozwalającego przybliżyć się do tego typu praktyk. W rozdziale dowiesz się, przy użyciu jakich metod sieć z serwerem SBS może i powinna być zabezpieczana. W kolejnych rozdziałach zawarto omówione krok po kroku procedury wyjaśniające, jak metody te praktycznie zastosować. W celu przypomnienia sobie najlepszych praktyk dotyczących zabezpieczeń, co jakiś czas należy wracać do tego rozdziału, a nawet po przeczytaniu całej książki i odłożeniu jej na półkę.

Drobna uwaga na marginesie

W trakcie określania reguł obowiązujących firmę przy dostępie do sieci często pomocna jest współpraca z zarządem. Sformułowanie zasad w formie pisemnej będzie pomocne w uniknięciu kłopotliwych dla siebie sytuacji. Dodatkowo osiągnie się większą konsekwencję w zakresie sposobu przydzielania uprawnień i uzyska się pewien poziom odpowiedzialności pracowników organizacji. Każdy musi mieć na uwadze zabezpieczenia sieci. Uzyskanie wsparcia ze strony zarządu i działu personalnego (jeśli taki istnieje) w zakresie definiowania i wdrażania zasad dotyczących zabezpieczeń sieci może być pomocne w zarządzaniu nią.

Ogólne informacje na temat zabezpieczeń serwera Small Business Server 2003

Najpierw w skrócie trzeba przypomnieć, że jeśli postępowałeś zgodnie z instrukcjami zawartymi w rozdziale 3. i wykonałeś zadania w kolejności, w jakiej znajdowały się na liście, można powiedzieć, że już poprawnie zdefiniowałeś podstawowe zabezpieczenia serwera Small Business Server 2003. To dobra wiadomość, natomiast zła jest taka, że konfigurowanie zabezpieczeń to nigdy nie kończące się zadanie, którego *nie można* zrealizować raz i o nim zapomnieć. Jeśli jednak na początku prawidłowo skonfiguruje się system i będzie się korzystało z najlepszych praktyk omawianych w książce, uzyska się bezpieczny system i sieć.

Jeśli chcesz mieć gwarancję, że sieć, serwer i stacje robocze cały czas będą bezpieczne, najlepszym rozwiązaniem będzie odłączenie wszystkiego i wyłączenie zasilania. Aktualnie nie ma innej metody zapewniającej stuprocentowe bezpieczeństwo. Ponieważ takie rozwiązanie nie wchodzi w grę, najlepsze, co można zrobić to zredukować stopień dostępności sieci, a zatem zmniejszyć prawdopodobieństwo wystąpienia problemu. Stosując standardowe środki ostrożności, zmniejszamy ryzyko, natomiast przez monitorowanie sieci można szybko zająć się wszystkimi pojawiającymi się problemami, zanim będą powodem większych kataklizmów.

Rodzaje zabezpieczeń

Zabezpieczenia mogą być omawiane na kilku różnych poziomach. Jeśli przyjrzymy się fizycznej warstwie zabezpieczeń, można zdefiniować następujące jego elementy:

- topologia sieci,
- serwer,
- klient (stacja robocza),
- użytkownicy,
- monitorowanie, rejestrowanie i inspekcja całości.

Topologia sieci swoim zakresem obejmuje architekturę i fizyczne okablowanie sieci. Istnieją bezpieczne i nie oferujące bezpieczeństwa metody konfigurowania sieci. Choć o projektowaniu sieci wspomniano w rozdziale 2., w celu uzyskania pewności, że sieć jest przygotowana do zastosowania silnych zabezpieczeń, przyjrzymy się teraz kilku zagadnieniom dotyczącym topologii sieci, które są dla nas ważne.

Oczywiście **serwer SBS** odgrywa w sieci kluczową rolę. Jeśli ktoś uzyska do niego dostęp, będzie mógł sprawować kontrolę nad siecią. Przyjrzymy się kilku różnym metodom zabezpieczania serwera.

Klienta (stacja robocza, komputer stacjonarny) też dotyczą kwestie związane z zabezpieczeniami. Ponieważ stacje robocze nie sprawują kontroli nad siecią, istnieje zagrożenie, że posłużą intruzowi do uzyskania w prosty sposób dostępu do sieci i naruszenia jej zabezpieczeń. Omówimy różne metody zabezpieczania stacji roboczych pomocne w uniknięciu tego typu problemów.

Źródłem problemów z zabezpieczeniami mogą też być **użytkownicy**. Użytkownicy, którzy między innymi zapisują hasła i uruchamiają nieautoryzowane oprogramowanie, mogą doprowadzić do powstania luk w zabezpieczeniach. Jednak istnieją metody na zmniejszenie ryzyka stwarzanego przez użytkowników (celowo lub nieumyślnie), nie wymagające sięgania po drakońskie środki.

Przez regularne i dokładne **monitorowanie, rejestrowanie i inspekcję** można mieć wszystko pod kontrolą. Po takim skonfigurowaniu powyższych operacji, aby automatycznie informowały administratora o tym, co wzbudza podejrzenie, a także przez regularne przeglądanie plików dzienników i raportów można wcześnie wykryć nietypowe zdarzenia i szybko podjąć odpowiednie działania.

Drobna uwaga na marginesie

Prawdopodobnie bezpieczeństwo jest największym wyzwaniem, z jakim obecnie mają do czynienia administratorzy sieci. Niniejszy rozdział ma być pomocny w zrozumieniu różnych elementów zabezpieczeń. Dzięki różnym oferowanym kreatorom serwer SBS znakomicie sprawdza się w procesie definiowania poprawnych początkowych ustawień zabezpieczeń. Jeśli wykona się omówione w rozdziale 3. zadania instalacyjne zawarte na liście, a także będzie się postępowało zgodne z najlepszymi praktykami zamieszczonymi w różnych miejscach książki, poziom zabezpieczeń sieci może być zgodny z oczekiwaniami. Kierujmy się filozofią, która głosi, aby mieć nadzieję na najlepsze i planować najgorsze. Prawdopodobnie w praktyce będziemy mieć do czynienia z czymś znajdującym się pomiędzy.

Topologie sieci i konfiguracja firewalla

Najpierw należy zapoznać się z topologią sieci. Jeśli postępowałeś zgodnie z zaleceniami z rozdziałów 2. i 3., na początku powinieneś dysponować w miarę zabezpieczoną siecią. Aby upewnić się, że tak jest, jeszcze raz przyjrzyjmy się strukturze sieci.

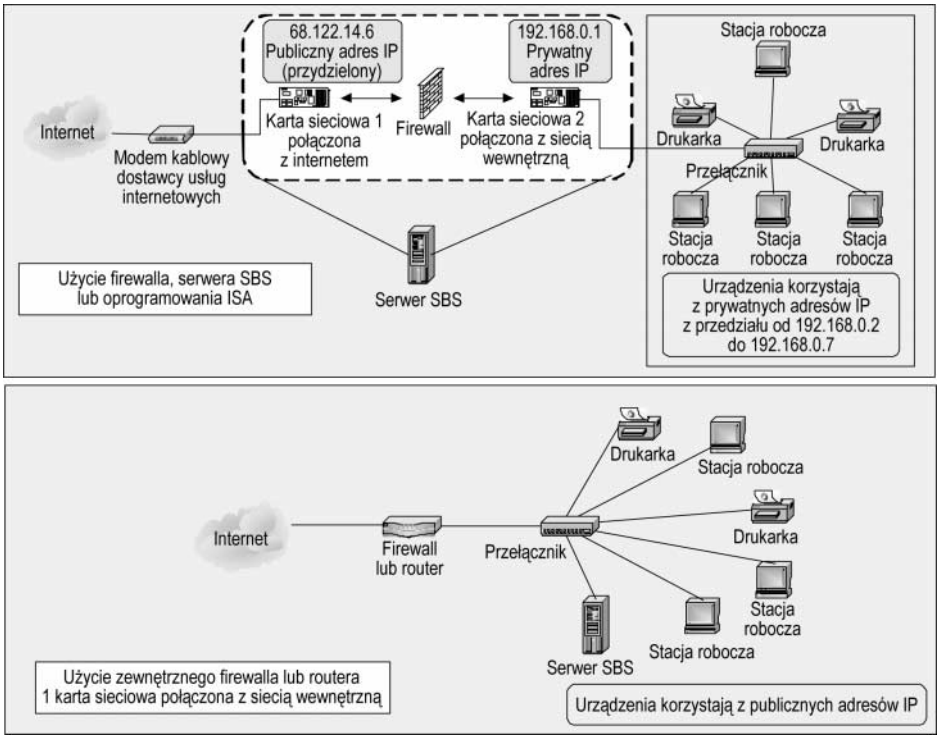
Połączenia sieciowe

W celu ochrony sieci połączonej z internetem konieczne jest skonfigurowanie firewalla. Jak już wspomniano w rozdziale 2., firewall jest rozwiązaniem sprzętowym lub programowym, które filtruje wszystkie dane przychodzące do sieci i z niej wychodzące. Przy filtrowaniu danych firewall decyduje, które pakiety przepuścić, a których nie. Firewall korzysta ze zdefiniowanych dla niego reguł. W trakcie konfigurowania połączenia z internetem przy użyciu *Kreatora konfigurowania poczty e-mail i połączenia internetowego* omówionego w rozdziale 3., zdefiniowano kilka reguł dla firewalla wbudowanego w serwer SBS. Po zainstalowaniu oprogramowania *ISA* (*Internet and Security Acceleration*) *Server* wchodzącego w skład wersji Premium serwera SBS dostępny będzie bardziej zaawansowany firewall (procedura instalacji i konfiguracji oprogramowania zostanie omówiona w dalszej części książki).

W rozdziale 2. wspomnieliśmy również o tym, jakie miejsce w konfiguracji sieci powinien zająć serwer SBS. W większości przypadków serwer powinien być wyposażony w dwie karty sieciowe. Jedna z nich za pośrednictwem modemu kablowego lub routera będzie połączona z internetem, natomiast druga z siecią wewnętrzną firmy. Można sobie wyobrazić, że po uaktywnieniu firewall wbudowany w serwer SBS będzie umiejscowiony między obydwiema kartami. Dane przychodzące z internetu docierają do karty sieciowej połączonej z modemem kablowym dostawcy usług internetowych lub routerem, a następnie analizowane są przez firewall serwera SBS. Jeśli otrzymane pakiety spełnią wymagania reguł, zostaną przekazane do karty sieciowej połączonej z siecią wewnętrzną. W przeciwnym razie pakiety zostaną odrzucone. Taki sam proces ma miejsce w przypadku danych wysyłanych do internetu. Przez zastosowanie w sieci wewnętrznej prywatnych adresów IP i mechanizmu translacji adresów sieciowych NAT (*Network Address Translation*) uzyskuje się dodatkową warstwę zabezpieczeń.

Kolejna metoda zabezpieczania połączenia polega na użyciu zewnętrznego firewalla (specjalizowane urządzenie lub komputer z odpowiednim oprogramowaniem). W tym przypadku komputer z serwerem SBS może dysponować tylko jedną kartą sieciową. Jeśli nie korzystamy z zewnętrznego firewalla (nie znajdującego się na serwerze SBS), komputer z serwerem SBS *powinniśmy* wyposażyć w dwie karty sieciowe i uaktywnić na nim firewall. Jeśli tak jest, należy cofnąć się do rozdziału 3. i zapoznać z krokami drugiej fazy instalacji. Na rysunku 4.1 przedstawiono strukturę sieci, w której zastosowano firewall wbudowany w serwer SBS lub oprogramowanie *Internet and Security Acceleration*, a także strukturę z zewnętrznym firewallem. Należy się upewnić, że zdefiniowana konfiguracja sieci spełnia ogólne wymagania. Jeśli tak nie jest, sieć jest zagrożona i powinieneś dokonać takich zmian w jej konfiguracji, aby spełniała wytyczne.

Warto zauważyć, że w przypadku drugiego wariantu konfiguracji w roli firewalla *konieczne* jest użycie specjalizowanego urządzenia, ponieważ serwer SBS posiada tylko jedną kartę sieciową połączoną bezpośrednio z siecią. Jeśli rolę firewalla ma odgrywać serwer SBS lub oprogramowanie *Internet and Security Acceleration Server* dostępne w jego wersji Premium, komputer musi być wyposażony w dwie karty sieciowe i skonfigurowany zgodnie z pierwszym wariantem przedstawionym na rysunku 4.1.



Rysunek 4.1. *Konfiguracje sieci korzystających z firewalla wewnętrznego i zewnętrznego*

Jeśli zastosowano zewnętrzny firewall (często jest to router z funkcjami firewalla), powinieneś sprawdzić konfigurację, korzystając z dokumentacji dostarczonej przez jego producenta.

Zabezpieczenia sieci bezprzewodowych

Niektóre routery (nazywane czasami stacjami bazowymi) oferują też dostęp do sieci bezprzewodowych urządzeniom, które z nich korzystają. Jeśli nie posiadasz urządzeń bezprzewodowych, należy wyłączyć taki dostęp. Jeśli z nich korzystasz, zaglądając do dokumentacji routera, upewnij się, że został tak skonfigurowany, aby oferować wyłącznie bezpieczny dostęp do sieci bezprzewodowej.

Jeśli używany jest router lub firewall, należy pamiętać o zabezpieczaniu go za pomocą złożonego hasła, które uniemożliwi uzyskanie nieautoryzowanego dostępu do funkcji administracyjnych urządzenia. Nie wolno stosować domyślnego hasła ustawionego przez producenta. Trzeba je zmienić przed uaktywnieniem routera. Hasło należy przechowywać w bezpiecznym miejscu. W zależności od routera, dostęp do sieci bezprzewodowej też powinien być zabezpieczany przy użyciu protokołu uwierzytelniania

WEP (*Wireless Equivalent Privacy*) lub lepszego 802.1x (jeśli jest obsługiwany). Bezpieczniejsza metoda ochrony dostępu bezprzewodowego polega na umieszczeniu punktu dostępowego między firewallem i połączeniem internetowym. W celu uzyskania dostępu do sieci wewnętrznej, w tej metodzie dodatkowo wymaga się od użytkowników nawiązania bezpiecznego połączenia wirtualnej sieci prywatnej VPN (*Virtual Private Network*). Więcej informacji na temat zabezpieczania sieci bezprzewodowej zawarto w dalszej części książki.

Microsoft zaleca

- W przypadku korzystania z firewalla wbudowanego w serwer SBS lub oprogramowania ISA Server należy użyć dwóch kart sieciowych.
- Należy uaktywnić firewall serwera SBS. Jeśli korzysta się z wersji Premium serwera, można zastosować firewall programowy *ISA Server*.
- Wewnętrzny firewall serwera SBS należy wyłączyć, *tylko* gdy zastosowano firewall zewnętrzny.
- Jeśli używany jest zewnętrzny firewall, karta sieciowa serwera SBS będzie połączona z siecią wewnętrzną.
- Jeśli zewnętrzny router (firewall) oferuje dostęp do sieci bezprzewodowych, należy zabezpieczyć urządzenie, a także w celu zapewnienia bezpiecznego dostępu do tego typu sieci zastosować protokół uwierzytelniania WEP lub 802.1x.
- Jeśli zewnętrzny router (firewall) oferuje dostęp do sieci bezprzewodowych, z którego się nie korzysta, należy go wyłączyć. W celu uzyskania informacji dotyczących konfigurowania należy zaglądnąć do dokumentacji dostarczonej przez producenta.

Zabezpieczanie serwera

Można wyróżnić kilka ważnych aspektów związanych z zabezpieczaniem serwera. Jak wspomniano wcześniej, serwer SBS odgrywa w sieci kluczową rolę. W celu uniknięcia problemów dotyczących całej sieci należy go dobrze chronić. Zabezpieczenia serwera swoim zakresem obejmują jego bezpieczeństwo fizyczne, a także zabezpieczenia konfiguracji i oprogramowania.

Bezpieczeństwo fizyczne serwera

Jednym z najprostszych kroków procedury zabezpieczania serwera jest *umieszczenie go w bezpiecznym miejscu*, do którego dostęp może być kontrolowany. Może to być zamykana szafa z dobrą wentylacją, pomieszczenie serwerowe lub biuro innej osoby, do którego dysponuje się kluczem i całodobowym dostępem. Uniemożliwienie postronnej osobie dostania się do serwera pozwala uniknąć różnego typu problemów, takich jak kradzież samego serwera, włamanie do niego w celu uzyskania praw administratora i podłączenie się za pomocą kabli do serwera w celu pobrania lub kradzieży danych.

Kolejnym aspektem związanym z fizycznym bezpieczeństwem jest *wprowadzenie restrykcji dotyczących przydzielania uprawnienia lokalnego logowania* na serwerze. Jeśli użytkownik nie jest osobą, która musi zalogować się lokalnie na serwerze w celu wykonania codziennej kopii zapasowej danych lub kimś, kto ma Cię zastąpić w czasie pobytu na tak bardzo potrzebnym urlopie, nie należy przydzielać tego uprawnienia. *Nie możesz też wykorzystywać serwera w roli stacji roboczej*, sądząc, że używając go w ten sposób zaoszczędzisz pewną kwotę. Jest to możliwe, ale niezalecane. Poza tym, że prawdopodobnie przeciąży się serwer i spowoduje spowolnienie sieci, co odczują wszyscy użytkownicy, instalowanie na nim zwykłych aplikacji może doprowadzić do powstania luk w zabezpieczeniach. Za cenę stacji roboczej, która obecnie nie jest droga nie warto ryzykować bezpieczeństwa sieci przez wykorzystanie serwera SBS w roli własnego komputera stacjonarnego.

Microsoft zaleca

- Serwer należy umieścić w miejscu, do którego dostęp jest kontrolowany.
- Nie wolno używać serwera w roli stacji roboczej.
- Nie należy instalować na serwerze aplikacji użytkowników.

Zabezpieczanie konfiguracji

W tym kontekście zabezpieczanie konfiguracji oznacza przyjrzenie się temu, w jaki sposób serwer SBS skonfigurowano i uruchomiono. Jeśli zapoznałeś się z omówieniem instalacji, listą zadań do wykonania i postępowałeś zgodnie z procedurami zawartymi w rozdziale 3., serwer już powinien być skonfigurowany i oferować podstawowe zabezpieczenia. Poniżej wymieniono dodatkowe elementy konfiguracji serwera, tak aby zarówno on sam, jak i sieć były bezpieczne. Metody szczegółowo omówiono w dalszej części rozdziału.

- Niezbędne jest stosowanie złożonych haseł.
- Należy zmienić nazwę wbudowanego konta *Administrator*.
- Przy wykonywaniu codziennych zadań nie wolno korzystać z konta administratora lub użytkownika zaawansowanego.
- Po zakończeniu pracy należy się wylogować.
- Nieużywane usługi i aplikacje należy wyłączyć lub usunąć.
- Należy przygotować procedurę archiwizacji danych.
- Należy skonfigurować zdalny dostęp do sieci.

W przypadku konfigurowania bezpiecznej sieci pierwszym krokiem jest *wymóg stosowania złożonych haseł*. Więcej na ten temat zawarto też w dalszej części książki. Niezbyt często można usłyszeć o tym zagadnieniu. Przy każdego typu zabezpieczeniach zawsze istnieje równowaga między ustawieniami optymalnymi i praktycznymi. Ustalenie kompromisu między siecią bezpieczną i użyteczną jest trudne, i samemu trzeba przez to przejść. Złożone hasła mogą być stosowane w sposób, który nadal jest przyjazny dla

użytkownika, a jednocześnie nie stwarzają luki w zabezpieczeniach. Jeśli wymagania dotyczące haseł są *zbyt* duże, użytkownicy po prostu będą zapisywać swoje skomplikowane hasła, tym samym niwecząc cel złożonych haseł. Do złożonych haseł można zaliczyć takie, które spełniają następujące wymagania:

- użycie przynajmniej 7 znaków,
- uwzględnienie dużych i małych liter, a także liczb i znaków specjalnych,
- wykluczenie stosowania imienia i nazwiska użytkownika,
- hasło nie zawiera słowa, które można znaleźć w słowniku (*tulip* nie spełnia kryteriów, natomiast *21iP* tak),
- hasło nie zawiera informacji na temat użytkownika, które są ogólnie znane, takich jak imiona żony, męża, dzieci, daty urodzenia itp.

Kolejnym stosunkowo prostym krokiem konfiguracji zabezpieczeń jest *zmiana nazwy wbudowanego konta Administrator*. Włamywacze zawsze najpierw szukają konta o takiej nazwie. Jeśli jego nazwa zostanie zmieniona na łatwą do zapamiętania, a której włamywacz raczej nie odgadnie, znacznie bardziej utrudni mu się działania. Poza tym przy wykonywaniu na serwerze codziennych zadań *nie wolno korzystać z konta administratora lub użytkownika zaawansowanego* (*Power User*), niezależnie od tego, jaką nazwę konto to nosi. Konto użytkownika zaawansowanego jest kolejnym posiadającym znaczne uprawnienia sieciowe, dlatego nie powinno się go używać do realizowania codziennych operacji. Najlepszym rozwiązaniem jest utworzenie kont zwykłych użytkowników dla siebie i innych osób, które mogą pomagać przy administrowaniu. Należy zobligować innych administratorów do korzystania przy wykonywaniu standardowych zadań ze zwykłych kont i logowania przy użyciu kont oferujących większe uprawnienia (konto administratora lub użytkownika zaawansowanego) tylko, gdy realizowane operacje wymagają wyższego poziomu uprawnień. Oczywiście należy pamiętać *o wylogowaniu się po zakończeniu pracy* i o tym, żeby po zalogowaniu się przy użyciu konta o dużych uprawnieniach nie pozostawiać komputera bez nadzoru. Dla funkcji odliczającej czas bezczynności można też ustawić rozsądny czas (5 lub 10 minut), po upływie którego konto zostanie zablokowane.

Kolejnym dość prostym zadaniem jest *wyłączenie lub usunięcie usług, bądź aplikacji, z których się nie korzysta*. Czy pamiętasz, jak w rozdziale 3. korzystałeś z *Kreatora konfigurowania poczty e-mail i połączenia internetowego* i wybierałeś usługi, które miały zostać uruchomione? Wspomnieliśmy nawet o wybieraniu tylko tych usług, z których zamierzałeś korzystać lub już ich używałeś w istniejącej sieci. Utrzymywanie aktywnymi usług, których się nie używa jest jak zamykanie domu i pozostawianie szeroko otwartego okna. Jeśli się wie, czego szukać, niezbyt trudno można się do niego dostać. To samo dotyczy aplikacji i usług. Jeśli nie jest Ci już potrzebna aplikacja lub usługa, należy usunąć ją z serwera. Jest to zalecana operacja pozwalająca utrzymać porządek i zapobiegać powstawaniu luk w zabezpieczeniach, które można przeoczyć. Jeżeli z aplikacji lub usługi nie korzystasz zbyt często, możesz nie pomyśleć o sprawdzeniu jej pod kątem problemów z zabezpieczeniami.

W trakcie instalowania serwera SBS określone udziały tworzone są automatycznie i konfigurowane odpowiednie uprawnienia. Jednak, aby użytkownikom udostępnić dodatkowe katalogi lub pliki, konieczne będzie zrobienie tego we własnym zakresie. Jeśli zależy

Ci na utworzeniu dodatkowych udziałów, trzeba najpierw udostępnić plik lub katalog, a następnie użytkowników umieścić w grupach, a im udzielić odpowiednich uprawnień do udziałów. W dalszej części książki omówimy użytkowników, grupy i uprawnienia, a teraz wystarczy tylko pamiętać o zasadzie, która mówi, że nie wolno przypisywać uprawnień poszczególnym użytkownikom. Zawsze należy umieszczać użytkowników w grupach i im przydzielać uprawnienia, nawet jeśli grupa będzie liczyła tylko jednego członka. Dzięki temu zarządzanie użytkownikami stanie się znacznie prostsze i mniej prawdopodobne będzie pojawienie się z czasem problemów z zabezpieczeniami.

Na skróty

Przeglądanie uprawnień udziałów

Po odszukaniu udziału, dla którego chcesz sprawdzić uprawnienia, prawym przyciskiem myszy należy kliknąć jego nazwę i z menu wybrać pozycję *Właściwości*. Po uaktywnieniu zakładki *Zabezpieczenia* można zapoznać się z listą grup powiązanych z udziałem. Możliwe jest też sprawdzenie uprawnień, jakie przypisano każdej z grup. Jeśli z udziałem nie powiązano żądanych uprawnień, biorąc pod uwagę specyficzne wymagania postawione przez organizację, można do udziału przydzielić grupy użytkowników.

W celu uzyskania dodatkowych informacji na temat zarządzania udziałami, w sekcji powiązanej z serwerem SBS wyświetlanej w oknie narzędzia *Pomoc i obsługa techniczna* (uruchamiane po wybraniu z menu *Start* pozycji *Pomoc i obsługa techniczna*) należy poszukać łańcucha `udostępnianie zasobów sieciowych`.

Przygotowanie procedury wykonującej kopię zapasową danych jest kolejną istotną kwestią dotyczącą zabezpieczeń. Czyż zabezpieczenia nie stają się już trochę bardziej zrozumiałe? Tak naprawdę definiowanie zabezpieczeń jest serią dość prostych zadań, które razem pomagają w stworzeniu bezpiecznej sieci. Ponieważ serwer SBS oferuje wszystkie najważniejsze usługi stosowane w sieci, naprawdę istotne jest opracowanie procedury archiwizacyjnej, która ochroni sieć w przypadku wystąpienia awarii serwera, zaniku zasilania, klęski żywiołowej lub kradzieży. Bardziej dokładnie zajmiemy się tym w dalszej części książki. Jednak teraz ważne jest, aby wiedzieć o istnieniu dwóch podstawowych typów kopii zapasowej. Pierwszym z nich jest nadmiarowość obecna w sprzętowej macierzy dyskowej (woluminy RAID, woluminy lustrzane itp.), natomiast drugim archiwizowanie danych na nośnikach wymiennych. Jeśli korzystasz z woluminów RAID lub lustrzanych, możesz być spokojny, gdy awarii ulegnie jeden z dysków lub kontroler. Jednak co zrobisz, gdy budynek zostanie zalany podczas powodzi, a serwer znajduje się w nim na parterze? Tworzenie kopii zapasowych opartych na rozwiązaniach takich jak woluminy RAID i lustrzane sprawdza się świetnie w roli mechanizmu oferującego nadmiarowość w codziennej eksploatacji i po wystąpieniu określonego typu problemów pozwala szybko przywrócić system do działania. Jednak w przypadku znacznie poważniejszego problemu warto dysponować kompletnym i aktualnym zestawem kopii zapasowych danych oraz co najmniej jednym zestawem przechowywanym w innej bezpiecznej lokalizacji. Jeśli serwer zostanie skradziony lub budynek doszczętnie spłonie, powinno być możliwe jak najszybsze przywrócenie sieci do działania (ubezpieczenie może zmniejszyć straty finansowe, ale straty wynikające z braku możliwości prowadzenia przez firmę działalności może tylko zredukować posiadanie kopii zapasowych). Serwer SBS oferuje zintegrowany system archiwizowania danych, który zostanie omówiony w dalszej części książki. Obecnie do własnej listy zadań do wykonania należy dodać przygotowanie procedury archiwizacji danych.

To, co najlepsze zostawiliśmy na koniec, czyli *konfigurowanie zdalnego dostępu do sieci*. Z pewnością nie chcesz, aby każdy dysponował możliwością uzyskania zdalnego dostępu do sieci. Dobrą wiadomością jest to, że serwer SBS oferuje kilka narzędzi, które są proste w konfiguracji i zarządzaniu. Narzędzia umożliwiają uzyskanie w bezpieczny sposób zdalnego dostępu użytkownikom, którzy go wymagają. Można wyróżnić dwie podstawowe metody pozwalające zaoferować zdalny dostęp. Pierwsza polega na nawiązaniu połączenia VPN, natomiast druga na użyciu narzędzia *RWW* (*Remote Web Workplace*). Narzędzie RWW jest prostsze w konfiguracji i użyciu od tworzenia połączenia VPN. Jednak w obu przypadkach możliwe jest zaoferowanie bezpiecznego zdalnego dostępu. W dalszej części książki omówimy praktyczne zastosowanie obu metod.

Microsoft zaleca

- Należy stosować złożone hasła.
- Należy zmienić nazwę wbudowanego konta *Administrator*.
- W codziennej pracy nie należy korzystać z konta administratora lub zaawansowanego użytkownika. Gdy jest to możliwe, należy korzystać z własnego zwykłego konta i w razie potrzeby wykonywać polecenie `runas`.
- Należy wyłączyć lub usunąć nieużywane aplikacje i usługi.
- Udziałom należy przypisywać uprawnienia.
- Na serwerze należy uwzględnić procedurę, która regularnie będzie wykonywała kopię zapasową danych. Jeden zestaw kopii zapasowych powinien być przechowywany w innej bezpiecznej lokalizacji.
- Przy konfigurowaniu zdalnego dostępu do lokalnej sieci należy korzystać z połączeń VPN lub narzędzia RWW.

Zabezpieczanie oprogramowania

Oprogramowanie zainstalowane na komputerze może negatywnie lub pozytywnie wpływać na bezpieczeństwo sieci. Aby zwiększyć bezpieczeństwo, należy aktualizować oprogramowanie systemowe serwera i zainstalowane na nim aplikacje, a także programy antywirusowe i inne narzędzia.

Microsoft jest świadom tego, że hakerzy cały czas szukają luk w jego produktach, które umożliwią im włamanie się. W związku z tym firma w większym stopniu skoncentrowała się na poprawianiu zabezpieczeń swoich produktów, a zwłaszcza rozwiązań przeznaczonych dla serwerów odgrywających istotną rolę. Windows Server 2003 i jego bliski krewny serwer SBS bezpośrednio po zainstalowaniu są bezpieczniejsze od każdego swojego poprzednika. Skupiając się na udoskonalaniu zabezpieczeń, Microsoft nieustannie udostępnia aktualizacje i poprawki eliminujące luki wykryte w jego produktach. Dobrą wiadomością jest to, że te aktualizacje i poprawki często udostępniane są *zanim* hakerzy stwierdzą, że istnieje luka, którą można wykorzystać. Jednak będzie to dobra wiadomość, tylko gdy w związku z luką w zabezpieczeniach poczyni się odpowiednie starania i uprzedzi się hakerów. Możliwe jest takie *skonfigurowanie systemu, aby automatycznie sprawdzał dostępność aktualizacji*. Korzystając z oprogramowania i konfiguracji serwera, ze strony internetowej Microsoftu możesz pobrać i zainstalować udostępnione aktualizacje.

Można skorzystać z trzech opcji: *Pobierz aktualizacje automatycznie i zainstaluj je zgodnie z określonym harmonogramem* (niezalecane), *Pobierz aktualizacje automatycznie i powiadom mnie, kiedy będą gotowe do zainstalowania* (zalecane) i *Powiadom mnie przed pobraniem aktualizacji i powiadom ponownie przed zainstalowaniem ich na komputerze* (niezalecane). Pierwsza opcja może spowodować ponowne uruchomienie serwera, gdy nie jest to akurat wskazane. Niektóre aktualizacje wymagają ponownego uruchomienia systemu. Jeśli jest to warunkiem poprawnej instalacji aktualizacji, użytkownik zostanie powiadomiony. Trzecia opcja nie jest pożyteczna, ponieważ w chwili udostępnienia aktualizacji nie spowoduje jej pobrania i zainstalowania. W efekcie system może być łatwym celem ataku dla hakerów szukających luk w zabezpieczeniach, których jeszcze nie usunięto. Nietrudno uwierzyć w to, że część hakerów, podobnie jak Ty, jest powiadamiana o dostępności nowych aktualizacji. Po ich pojawieniu się próbują sposobów wykorzystania luk, w związku z którymi aktualizacje udostępniono. Tego typu osoby za pośrednictwem internetu szukają komputerów, na których nie zainstalowano jeszcze aktualizacji. Choć jest to coś w rodzaju przewodnika dla leniwego włamywacza, na swój dziwny sposób bywa skuteczne.

Zalecane jest również szukanie aktualizacji dla aplikacji serwera niewchodzących w skład systemu operacyjnego. W większości przypadków konieczne będzie *okresowe sprawdzanie dostępności aktualizacji aplikacji* (serwera i nie tylko). W niektórych sytuacjach twórca aplikacji może oferować listę wysyłkową, do której można się zapisać w celu powiadamiania, gdy pojawią się aktualizacje i poprawki. Aktualizacji należy szukać na stronie internetowej producenta lub tak skonfigurować kalendarz, aby przypominał o sprawdzeniu ich dostępności raz w tygodniu lub miesiącu.

A teraz pora na kolejny prosty środek pozwalający poprawić zabezpieczenia, czyli *instalację i konfigurację oprogramowania antywirusowego*. Wiele tego typu aplikacji rozpoznaje „robaki", programy szpiegowskie, wirusy poczty elektronicznej (zwykle znajdujące się w załącznikach) i destrukcyjny kod. Należy skorzystać z oprogramowania antywirusowego spełniającego wymagania firmy. Trzeba pamiętać o tym, aby nabyć wersję programu antywirusowego stworzoną specjalnie dla serwera i zgodną z oprogramowaniem SBS 2003. Tego typu program powinien być w stanie wykrywać wirusy znajdujące się na komputerze, a także w wysyłanych i otrzymywanych wiadomościach poczty elektronicznej z uwzględnieniem załączników. Oprogramowanie antywirusowe należy tak skonfigurować, aby od razu po pojawieniu się aktualizacji pliku sygnatur automatycznie je pobierało i instalowało. Plik sygnatur zawiera informacje, które instruują program, jak rozpoznać tysiące aktywnych wirusów krążących w internecie. Bez aktualizowania pliku sygnatur komputer narażony będzie na najnowsze wirusy, nawet jeśli chroniony jest przed tymi starszymi. Zależnie od aktywności twórców wirusów, producenci programów antywirusowych udostępniają aktualizacje codziennie lub co dwa dni, a czasami co tydzień lub dwa. A zatem, dla własnej wygody należy tak skonfigurować oprogramowanie antywirusowe, aby samo pobierało i instalowało aktualizacje. Oczywiście od czasu do czasu warto upewnić się, że poprawnie działa funkcja automatycznej aktualizacji.

Microsoft zaleca

- Należy tak skonfigurować serwer, aby automatycznie pobierał i instalował aktualizacje.
- Należy sprawdzać dostępność aktualizacji aplikacji serwera.
- Należy sprawdzać dostępność aktualizacji innych aplikacji.
- Należy aktualizować oprogramowanie antywirusowe, a zwłaszcza plik sygnatur.

Drobna uwaga na marginesie

Tak naprawdę zabezpieczanie polega na zdefiniowaniu kilku regularnie wykonywanych operacji, które są pomocne w zapewnieniu bezpieczeństwa sieci. Po skonfigurowaniu zabezpieczeń z pewnością nadal trzeba mieć wszystko pod kontrolą. Jednak po zdefiniowaniu zabezpieczeń, ich monitorowanie i dostrajanie powinno być stosunkowo proste. Kluczowe znaczenie ma zawsze rozpoczynanie od zdefiniowania zabezpieczeń od podstaw i właściwe zarządzanie nimi. Zawsze prościej *utrzymać* od początku porządek na serwerze niż wprowadzać go na nim po stworzeniu sporego nieładu (brzmi to podobnie do tego, co mówiła moja mama o moim pokoju, gdy byłem dzieckiem).

Zabezpieczanie stacji roboczych

Gdy już zapoznaliśmy się z zabezpieczaniem serwera, pora na zajęcie się klientami (stacje robocze, komputery stacjonarne lub, zależnie od upodobań, jeszcze inne określenie). Tak naprawdę ze stacjami roboczymi związane są dwie podstawowe kwestie dotyczące zabezpieczeń. Pierwsza polega na tym, że *system operacyjny powinien być aktualny*. Wiąże się z tym aktualizowanie starszych i mniej bezpiecznych wersji systemu operacyjnego. Ze względu na to, że systemy operacyjne oferują lepsze funkcje zabezpieczeń, pod uwagę powinno się wziąć aktualizację starszych wersji systemów. Przykładowo, tak naprawdę obecnie nie powinno się korzystać z systemu starszego od Windows 98. Niezależnie od wersji używanego systemu operacyjnego, trzeba upewnić się, że zainstalowano w nim najnowsze dodatki Service Pack, aktualizacje i poprawki, które oferują najwyższy możliwy w przypadku danego systemu poziom zabezpieczeń.

W sieci z serwerem SBS można zainstalować i skonfigurować usługę SUS (*Software Update Services*), która jest pomocna w gromadzeniu, przeglądaniu i rozprowadzaniu aktualizacji używanych systemów operacyjnych. Usługa SUS zgodna jest z systemami Windows XP Professional, Windows 2000 Professional, Windows 2000 Server i Windows Server 2003. Jeśli korzystasz z innego systemu operacyjnego, takiego jak Windows 95, Windows 98, Windows Me lub Windows NT Workstation 4.0, w celu sprawdzania dostępności ważnych aktualizacji należy skorzystać z usługi *Windows Update*. Więcej informacji na ten temat zawarto w dalszej części książki.

Podobnie jak w przypadku serwera, *aplikacje zainstalowane na stacji roboczej też powinny być aktualizowane*. Producent aplikacji może oferować opcję automatycznej aktualizacji lub prowadzić listę wysyłkową, do której można się zapisać, aby być powiadamianym o dostępności aktualizacji.

Drobna uwaga na marginesie

Choć większość twórców oprogramowania odpowiednio testuje udostępniane aktualizacje, należy zachować wobec nich dystans i w celu ich sprawdzenia początkowo instalować je na jednym komputerze. Trzeba upewnić się, że aktualizacja zgodna jest z innymi aplikacjami (czasami uaktualnienie jednego programu powoduje, że inny przestaje działać), a także że współpracuje z wersją używanego systemu operacyjnego i nie powoduje problemów. Po stwierdzeniu, że wszystko jest w porządku, aktualizację należy zainstalować i przetestować na komputerze z innym systemem operacyjnym (zakładając, że w sieci korzysta się z ich różnych wersji). Najgorsze, co można zrobić, to pobrać aktualizację, zainstalować ją na przykład na 47 komputerach i stracić możliwość uruchomienia któregokolwiek z nich. Z tego powodu należy najpierw aktualizację sprawdzić.

Zabezpieczanie kont użytkowników

Istnieje kilka sposobów zabezpieczania kont użytkowników. Przez ciągłe edukowanie użytkowników i wymaganie od nich stosowania złożonych haseł, można pomóc im w ochronie swoich kont. Dodając użytkowników do grup w celu przypisania im uprawnień i udzielając użytkownikom tylko wymaganych przez nich uprawnień, możesz zminimalizować ryzyko wykonania przez nich w sieci działań, które tak naprawdę nie powinny mieć miejsca.

Edukowanie użytkowników

Pierwszą i najprostszą metodą zapewniania bezpieczeństwa kont jest edukowanie ich użytkowników. Można to zrobić w różny sposób. Niektóre firmy w tworzonych podręcznikach uwzględniają zasady dotyczące zabezpieczeń sieciowych. Z kolei inne przekazują takie informacje podczas szkoleń pracowników lub umieszczają je w sieci intranetowej, biuletynach, bądź przypominających wiadomościach poczty elektronicznej wysyłanych regularnie co jakiś czas do użytkowników. Niezależnie od tego, która metoda w przypadku określonej firmy sprawdzi się najlepiej, trzeba pamiętać o tym, że ciągłe uświadamianie użytkownikom, jak ważną rolę odgrywają zabezpieczenia sieci i jakie w związku z nimi pojawiają się zagrożenia (na przykład wirusy poczty elektronicznej) przyczyni się do zminimalizowania ryzyka. W jaki sposób powinno się edukować użytkowników? Poniżej wymieniono kilka propozycji. Firma może określić dodatkowe wymagania.

- Stosowanie złożonych haseł, które można zapamiętać, ale trudno odgadnąć.
- Niezapisywanie hasła i niepozostawianie go na biurku.
- Nieudostępnianie pod żadnym pozorem hasła innym osobom (włącznie ze znajomymi lub współpracownikami), niezależnie od tego, czy są do tego uprawnione, czy nie. Niektórzy w firmie lub poza nią mogą Cię przekonywać do tego, że udostępnienie nazwy konta i (lub) hasła jest dobrym pomysłem, ma sens, jest konieczne itp. Zdecydowanie nie wolno nigdy tego robić.

- Nieodpowiadanie pod żadnym pozorem na wiadomości poczty elektronicznej, które wymagają podania przez użytkownika nazwy konta i (lub) hasła. Jeśli korzystasz z kont założonych przez firmy internetowe, w celu zarządzania nimi należy logować się w ich witrynach WWW. Nigdy nie wolno odpowiadać na wiadomości poczty elektronicznej, co do których nie ma się pewności, czy zostały wysłane przez firmy, z usług których się korzysta. Odpowiadanie na wiadomości, których się nie spodziewamy, a w których żąda się podania nazwy konta i hasła (często też numerów kart kredytowych lub ubezpieczenia) określane jest anglojęzycznym terminem *phishing*. Jest to sposób na uzyskanie od niczego nie podejrzewających użytkowników danych podawanych przy uwierzytelnianiu. Firmy uprawnione do uzyskania takich danych nigdy nie żądają ich za pośrednictwem poczty elektronicznej.
- Jeśli powyższa zasada została złamana i udostępniono komuś hasło lub uważasz, że ktoś wszedł w jego posiadanie, należy natychmiast skontaktować się z administratorem sieci, aby zmienił hasło. Jeśli dotyczy to konta założonego przez firmę internetową, należy od razu zalogować się i zmienić hasło i (lub) powiadomić firmę.
- Nigdy nie należy pobierać i instalować oprogramowania, które nie zostało zatwierdzone przez administratora sieci i nie posiada podpisu. Jeśli użytkownik postąpi inaczej, może zainstalować program szpiegujący lub inny szkodliwy kod, który może gromadzić nazwy użytkowników, hasła i numery kart kredytowych, a następnie przesyłać je na zewnątrz w miejsce określone przez hakera.

Użytkowników należy na bieżąco informować o pojawieniu się w internecie nowych oszustw, wirusów lub „robaków". Użytkownicy powinni być świadomi zagrożenia, metody ataku i wiedzieć, co mają zrobić, aby uniknąć problemów, a co, gdy już padną ofiarą ataku. Często jest to pomocne, ponieważ użytkownicy zdobytą wiedzę mogą wykorzystać w przypadku własnych domowych komputerów i dzięki temu uniknąć kłopotów. Mogą też powiadomić znajomych. Im więcej osób będzie świadomych zagrożenia, tym lepiej.

Gdy użytkownicy są świadomi tego, że różne ich działania mogą niekorzystnie wpłynąć na sieć i bezpieczeństwo firmy, zwykle naprawdę starają się postępować zgodnie z obowiązującymi zasadami. Jednakże w ludzkiej naturze leży skłonność do bycia niedbałym i utrwalania złych nawyków, dlatego niezbędne jest też regularne uświadamianie użytkowników. W tym przypadku najlepszym rozwiązaniem jest zapobieganie.

Wymóg stosowania złożonych haseł

Poza edukowaniem użytkowników, do najlepszych zalecanych praktyk należy zaliczyć takie konfigurowanie serwera, aby wymuszał stosowanie złożonych haseł. Można wyróżnić typ ataku podejmowanego przez hakera, który nazywa się *słownikowym*. W jego przypadku w celu uzyskania nieautoryzowanego dostępu do hasła włamywacze korzystają ze zautomatyzowanej metody polegającej na sprawdzaniu jako hasła każdego terminu znajdującego się w słowniku. Tego typu atak nazywa się też *siłowym* (*brute force*), ponieważ haker po prostu tak długo próbuje uzyskać dostęp do konta,

aż mu się to wreszcie uda. Jeśli włamywacz zdobędzie nazwę konta uprawnionego użytkownika (obecnie może to być proste zadanie), często najpierw próbuje poznać hasło, stosując metodę ataku słownikowego. Metoda jest zautomatyzowana, dlatego haker może ją uaktywnić i w trakcie jej działania zrobić sobie przerwę na obiad. Właśnie z tego powodu złożone hasła nie mogą zawierać imienia i nazwiska użytkownika, a także wymagają użycia co najmniej 7 znaków i ich kombinacji uwzględniającej małe i duże litery, a także liczby i znaki specjalne.

Powód, dla którego trzeba stosować złożone hasła jest dość prosty. Załóżmy, że w haśle dopuszczalne jest użycie tylko dużych liter, a jego minimalna długość musi wynosić 2 znaki. Oznacza to, że istnieje około 675 różnych kombinacji, które mogą zostać użyte jako hasło. Jeśli zostanie utworzony arkusz kalkulacyjny, w którym wprowadzi się kolejne ciągi od AA do AZ, a następnie od BA do BZ itd., w końcu możliwe będzie odgadnięcie użytego hasła. Im więcej znaków liczy hasło, tym więcej będzie istniało jego wariantów. Liczba wariantów hasła zwiększy się też, gdy wymaga ono zastosowania większej liczby typów znaków. A zatem, gdy wymagane jest użycie 7-znakowego hasła, w przypadku którego dla każdej pozycji dostępnych jest około 176 znaków, liczba kombinacji będzie rosła w sposób wykładniczy. W efekcie złamanie takiego hasła zajmie włamywaczowi naprawdę wiele czasu, o ile mu się to w ogóle uda. Trzeba jednak pamiętać, że tego typu hasła nazywa się złożonymi, a nie niedostępnymi. Oznacza to, że gdy haker ma wystarczającą ilość czasu i mocy obliczeniowej, prawie wszystko może złamać. Jednak większość hakerów szuka innych sposobów na osiągnięcie celu. W dalszej części rozdziału, a także książki przyjrzymy się monitorowaniu, rejestrowaniu i inspekcji. Monitorowanie serwera pomocne jest w wykryciu próby włamania się przez intruza, dzięki czemu można podjąć odpowiednie działania uniemożliwiające złamanie zabezpieczeń.

Sprawdzenie, czy użytkownikom przypisano tylko niezbędne uprawnienia

Jeśli w rozdziale 3. konfigurowałeś konta użytkowników, dodałeś je do grup, korzystając z wcześniej zdefiniowanych szablonów oferowanych przez serwer SBS. Jest to jedna z metod, przy użyciu której serwer SBS ułatwia zarządzanie uprawnieniami. Predefiniowane szablony określają odpowiedni poziom uprawnień, dzięki czemu unika się związanych z nimi problemów pojawiających się, gdy uprawnienia nadaje się użytkownikom. W tym miejscu należy wspomnieć o dwóch następujących podstawowych zasadach „kciuka” (w końcu mamy je tylko dwa):

1. **Zawsze, gdy jest to możliwe należy stosować predefiniowane szablony**. Jeżeli konieczne jest zastosowanie niestandardowego zestawu uprawnień, należy utworzyć grupę, a następnie przypisać jej takie uprawnienia i dodać do niej użytkowników. Predefiniowane szablony pomocne są w konfiguracji standardowego zestawu uprawnień użytkowników, którzy należą do grup takich jak *Users*, *Power Users*, *Backup Operators* itp. Dodatkowo można uniknąć niezamierzonego stworzenia luk w zabezpieczeniach przez niepoprawne przypisanie użytkownikom uprawnień. Szablony zostaną bardziej szczegółowo omówione przy okazji opisu użytkowników i grup zawartego w kolejnych rozdziałach.

2. **Nie wolno przypisywać uprawnień pojedynczym użytkownikom**. Gdy się tak postąpi, bardzo trudno stwierdzić, jaki kto posiada poziom uprawnień. Jeśli dojdzie do złamania zabezpieczeń (na przykład ktoś uzyska dostęp do pliku z płacami pracowników firmy), można sprawdzić, kto jest członkiem grupy, która dysponuje uprawnieniami do pliku i stwierdzić, czy ktoś nie należy do tej grupy. Jeśli nie skorzystano z grup, konieczne będzie sprawdzenie konta każdego użytkownika, co nie jest sposobem spędzania czasu godnym polecenia.

Wniosek z tego jest taki, że ze zdalnego dostępu możemy pozwolić korzystać tylko takim użytkownikom, którzy wymagają go do pracy. Nie należy na to zezwalać tylko dlatego, że ktoś o to prosi lub wydaje się komuś, że *powinien* mieć taką możliwość. Przykładowo, możliwe jest utworzenie zasady, która głosi, że tylko kierownicy działów mogą decydować o przydzieleniu zdalnego dostępu podległym im pracownikom. Dzięki temu utrzymujesz określony poziom odpowiedzialności i zrzucasz z siebie piętno tego złego, który odmawia przyznania dostępu. W większości przypadków raczej nie *Ty* powinieneś decydować o tym, komu się należy przyznanie zdalnego dostępu. Do Ciebie należy zadbanie o to, aby udzielić odpowiedniego dostępu pozwalającego wykonywać zadania związane z działalnością firmy.

Microsoft zaleca

- Regularnie należy edukować użytkowników w zakresie praktyk związanych z zabezpieczeniami i zagrożeniami stwarzanymi przez internet.
- Po pojawieniu się nowego oszustwa lub wirusa należy poinformować użytkowników, jak coś takiego zidentyfikować, jak tego uniknąć i jak o czymś takim zgłosić.
- Należy wymagać stosowania złożonych haseł. Wymagania powinny być do przyjęcia dla użytkowników i wystarczająco rygorystyczne, aby hakerzy nie mogli z łatwością odgadnąć hasła lub złamać go, korzystając z metody ataku siłowego.
- Do przypisywania odpowiednich uprawnień użytkownikom należy używać predefiniowanych lub własnych szablonów.
- Użytkownikom należy nadawać minimalne uprawnienia, jakich potrzebują do tego, aby mogli wykonać powierzone im zadania.
- W przypadku zdalnego dostępu należy stosować zasady i udzielać go tylko tym użytkownikom, którzy uprawnieni są do realizowania czynności związanych z działalnością firmy.

Monitorowanie, rejestrowanie i inspekcja

Po skonfigurowaniu ustawień zabezpieczeń byłoby przyjemnie, gdyby oznaczało to koniec związanej z tym pracy. Niestety, tego typu praca nigdy nie ma końca. A zatem, po zdefiniowaniu zabezpieczeń sieci konieczne jest ich kontrolowanie. Nie musi to oznaczać całkowitego poświęcenia się temu, ale powinno się to robić konsekwentnie

i regularnie. Jeśli wyrobisz w sobie nawyk codziennego sprawdzania kluczowych obszarów sieci, na zarządzanie jej zabezpieczeniami może wystarczyć od 5 do 10 minut. Zadaniom związanym z kontrolą zabezpieczeń przyjrzymy się w dalszej części książki. Jednak w tym miejscu trzeba wiedzieć o kilku najbardziej zalecanych praktykach.

Konfigurowanie monitorowania i raportowania

Jeśli automatycznie nie otrzymujesz raportów związanych z monitorowaniem, powinieneś sprawdzić, czy skonfigurowana została odpowiednia funkcja lub czy adres poczty elektronicznej znajduje się na liście odbiorców (jeżeli właśnie zakończyłeś instalację serwera SBS, konfiguracja funkcji zostanie omówiona w dalszej części książki, dlatego możesz spokojnie poczekać). Serwer SBS oferuje kilka raportów na temat jego wydajności i stopnia wykorzystania. Raporty zawierają wartościowe informacje dotyczące kondycji, a także zabezpieczeń sieci i serwera. Regularne zapoznawanie się z raportami jest pomocne w wykrywaniu wszelkich nietypowych zachowań i podejmowaniu działań mających na celu wyeliminowanie ich w odpowiednim momencie. Możliwe jest takie skonfigurowanie serwera, aby do wysyłanych raportów dotyczących monitorowania automatycznie dołączał pliki dzienników. Dzięki temu będziesz dysponować wszystkimi danymi niezbędnymi do utrzymania sieci w dobrej kondycji.

Inspekcja kluczowych zdarzeń

Inspekcja polega na kontrolowaniu określonych zdarzeń. Tego typu zdarzenia są następnie automatycznie umieszczane w pliku zdarzeń, dzięki czemu można mieć przegląd sytuacji. Jak w przypadku wszystkich praktyk dotyczących zabezpieczeń, zasady i praktyki związane z inspekcją muszą wyznaczać kompromis między wszystkim i niczym. Jeśli zakresem inspekcji objęte zostaną wszystkie zdarzenia, nie tylko system się zawiesi, ale zostaniesz zalany ogromną ilością bezużytecznych danych. W związku z tym zidentyfikowanie istotnych zdarzeń staje się prawie niemożliwe. Jeśli nic nie zostanie poddane inspekcji, nie będziesz miał do czynienia z masą informacji, ale też nie będziesz w stanie stwierdzić, co się dzieje. Można to porównać do prowadzenia samochodu z zamkniętymi oczami. Jeśli zamiast tego zakresem inspekcji obejmiesz kluczowe zdarzenia, prawdopodobnie szybko zidentyfikujesz problemy i zapobiegniesz całkowitej katastrofie. Domyślnie serwer SBS prowadzi inspekcje dla *zdarzeń związanych z nieudanymi operacjami logowania* i *blokadą kont*.

Inspekcja zdarzeń związanych z nieudanymi operacjami logowania

Czy pamiętasz zawarte wcześniej omówienie dotyczące ataku siłowego i słownikowego? Właśnie teraz dowiesz się, jak sprawdzić, czy miały one miejsce. Inspekcja zdarzeń związanych z nieudanymi operacjami logowania oznacza, że każdorazowo, gdy użytkownik spróbuje się zalogować i mu się to nie uda, odpowiednie zdarzenie zostanie zapisane w pliku dziennika. Z pewnością zdarzają się sytuacje, w których ma miejsce nieudana próba zalogowania się, ponieważ użytkownik wcisnął klawisz *Caps Lock* lub po prostu źle wprowadził hasło. Jeśli jednak tego typu zdarzenia powtarzają się dla tego samego konta, można podejrzewać próbę przeprowadzenia ataku siłowego.

Można zweryfikować informacje zarejestrowane w dzienniku zdarzeń — wystarczy skontaktować się z użytkownikiem i upewnić się, że faktycznie nie udało mu się zalogować, i w razie konieczności podjąć dodatkowe działania mające na celu identyfikację potencjalnego włamywacza.

Domyślnie serwer SBS ustawia 50 nieudanych prób zalogowania w ciągu 10 minut. Jeśli do tego dojdzie, konto blokowane jest na 10 minut. Po ich upływie konto jest automatycznie odblokowywane, dzięki czemu użytkownik może z niego skorzystać. Ze względu na to, że mało prawdopodobne jest, aby uprawniony do tego użytkownik w ciągu 10 minut mógł się 50 razy niepoprawnie zalogować, w celu ułatwienia oddzielenia błędów popełnionych przez użytkownika od prób ataku siłowego domyślną wartość należy zmienić na 5 lub 6.

Inspekcja zdarzeń związanych z blokowaniem kont

Blokada konta następuje automatycznie po przekroczeniu wcześniej ustalonego limitu dozwolonych prób zalogowania się. W przytoczonym przykładzie oznacza to, że jeśli użytkownik spróbuje w ciągu 10 minut zalogować się 50 razy i nie uda mu się to, konto zostanie zablokowane na 10 minut. Jeśli ustawi się takie wartości, po zablokowaniu konta administrator i użytkownik mogą za pośrednictwem poczty elektronicznej zostać powiadomieni o tym zdarzeniu. Blokada jest zdejmowania po upływie 10 minut. Jeśli pojawi się drugie powiadomienie, na poważnie trzeba przyjąć, że konto padło ofiarą ataku siłowego i przeciwdziałać temu.

Microsoft zaleca

- Funkcję monitorowania należy tak skonfigurować, aby po wystąpieniu krytycznych dla systemu zdarzeń automatycznie być powiadamianym.
- W celu wykrycia oznak włamania lub prób jego dokonania należy przeglądać pliki dzienników i raporty.
- Domyślnie serwer SBS jest tak skonfigurowany, że przed zablokowaniem konta na 10 minut możliwe jest w ciągu 10 minut wykonanie 50 prób zalogowania się. Warto zauważyć, że większość firm obniża limit nieudanych prób do 5 lub 6 w ciągu 10 minut.
- Należy być na bieżąco z najnowszymi informacjami dotyczącymi zabezpieczeń. W związku z tym warto dokonać subskrypcji na stronie internetowej Microsoftu, aby za pośrednictwem poczty elektronicznej być powiadamianym o zagrożeniach. To samo należy zrobić w przypadku producentów programów antywirusowych lub innych godnych zaufania grup dyskusyjnych poświęconych bezpieczeństwu. Należy powiadamiać użytkowników o najnowszych zagrożeniach i metodach walki z nimi.

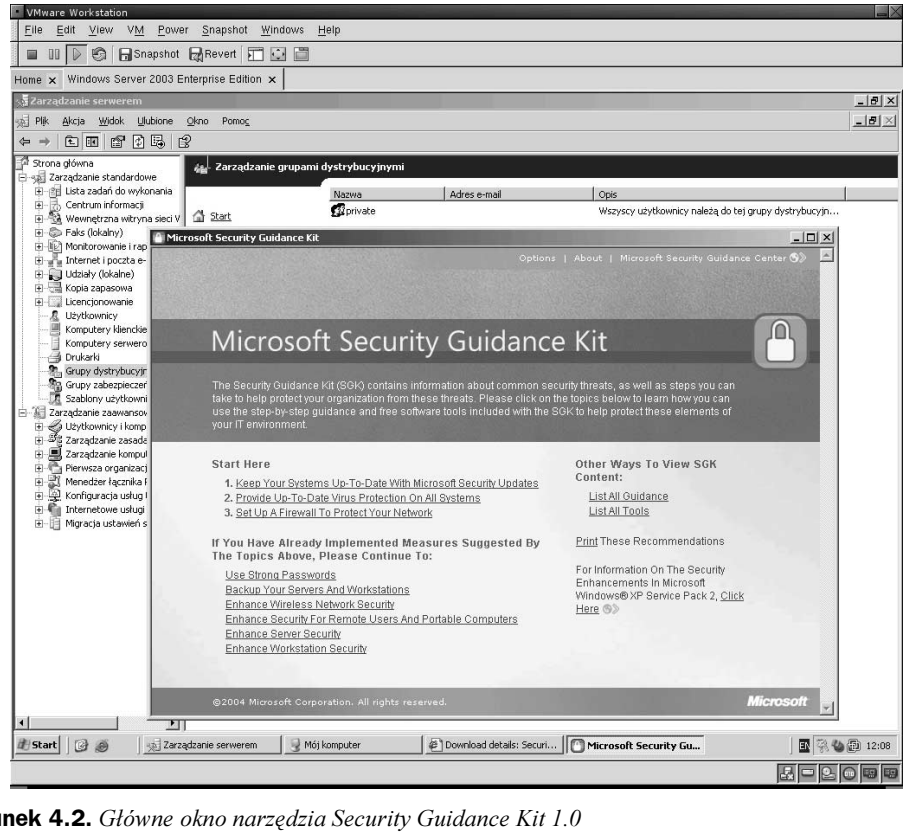
Narzędzie Security Guidance Kit firmy Microsoft

Security Guidance Kit jest przydatnym narzędziem, które można pobrać ze strony internetowej Microsoftu. Dzięki niemu można dowiedzieć się więcej na temat zabezpieczeń sieci lub poszczególnych komputerów. Narzędzie można uruchomić na dowolnej stacji roboczej z systemem Windows Server 2003 (z zainstalowanym serwerem SBS),

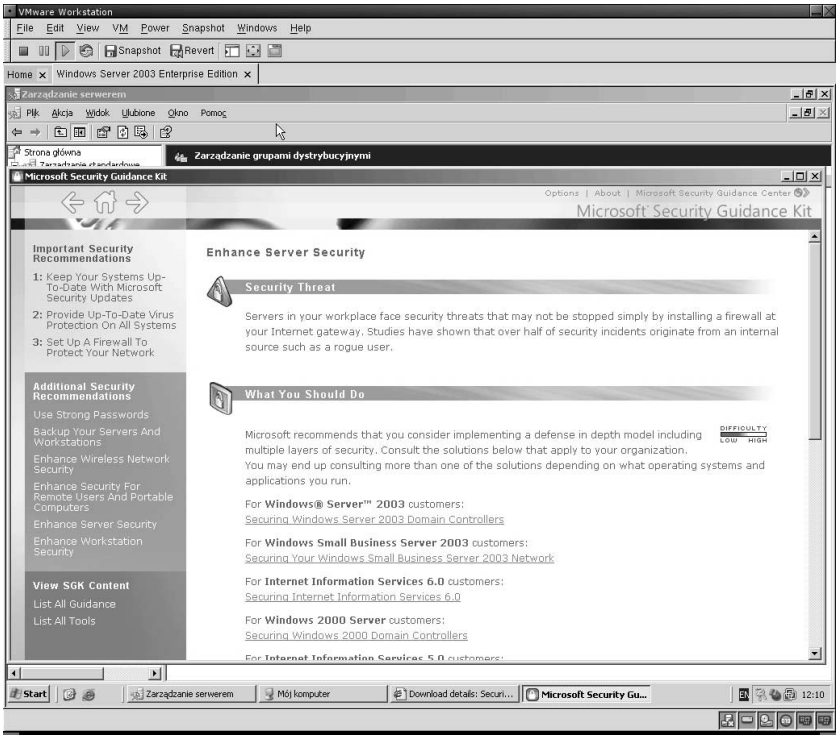
Drobna uwaga na marginesie

Przeglądanie plików dzienników i raportów jest jak comiesięczne zapoznawanie się z wyciągami związanymi z kontem bankowym lub kartą kredytową. Przeważnie wszystko jest w porządku i wtedy zaczynasz się zastanawiać, dlaczego każdego miesiąca dokładnie analizujesz każdy wiersz. Dwa lata później na wyciągu bankowym zauważasz błąd lub dwukrotne wykonanie operacji obciążenia karty kredytowej. Tylko dzięki temu, że poświęcasz czas na przeglądnięcie zawartości wyciągów nie stracisz kilkuset złotych wskutek niesłusznie przeprowadzonych operacji obciążenia. W przypadku plików dzienników i raportów jest identycznie. Zwykle wszystko jest bez zarzutu i jesteś w stanie wyjaśnić wszelkie anomalie. Jednak, gdy coś będzie nie tak, szybko zidentyfikujesz problem i zminimalizujesz jego wpływ na działanie sieci. Warto zatem poświęcić każdego dnia pięć lub dziesięć minut. Przy okazji warto wspomnieć, że pliki dzienników i raporty najlepiej przegląda się przy kawie i ciastkach cynamonowych.

Windows XP lub Windows 2000. Na rysunku 4.2 przedstawiono główne okno narzędzia widoczne po jego zainstalowaniu i uruchomieniu. Z kolei na rysunku 4.3 pokazano okno wyświetlane po kliknięciu w głównym oknie odnośnika *Enhance Server Security*. Na rysunku 4.4 przedstawiono okno widoczne po kliknięciu w głównym oknie odnośnika *List All Tools*. Program jest prosty w użyciu i obsłudze. W celu uzyskania dodatkowych informacji na temat najlepszych praktyk dotyczących zabezpieczeń po pobraniu narzędzia należy mu się bliżej przyjrzeć.



Rysunek 4.2. *Główne okno narzędzia Security Guidance Kit 1.0*



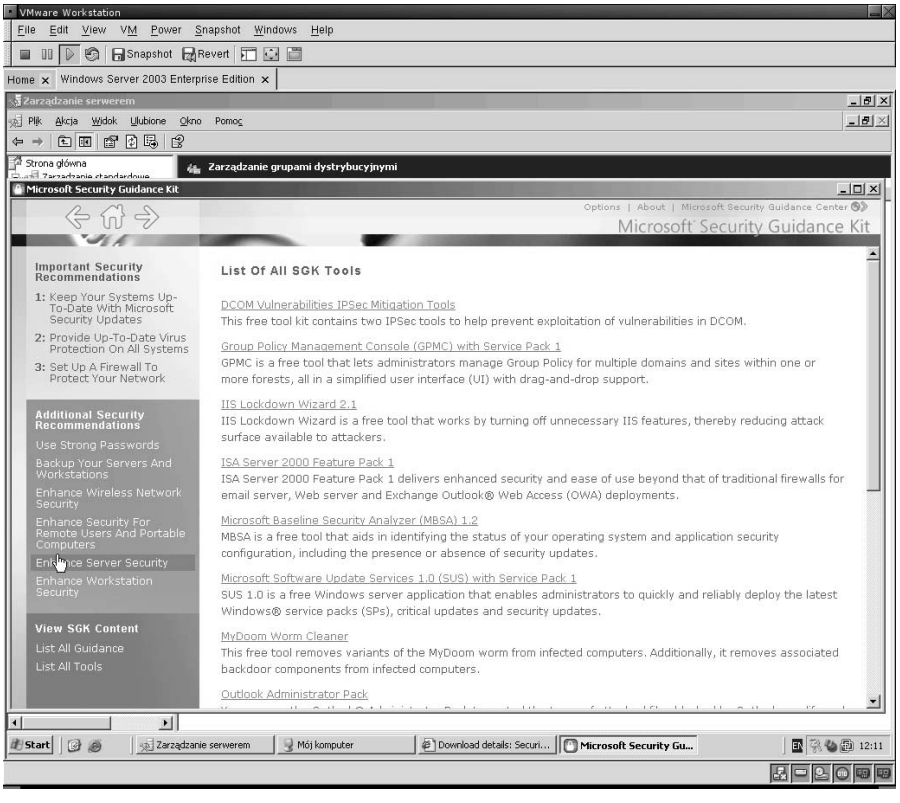
Rysunek 4.3. *Zalecenia dotyczące polepszenia zabezpieczeń serwera zawarte w oknie narzędzia Security Guidance Kit 1.0*

Na skróty

Narzędzie Security Guidance Kit 1.0

Narzędzie można pobrać ze strony internetowej Microsoftu (w polu wyszukiwania należy wprowadzić łańcuch `security guidance kit`). Za pośrednictwem niewielkiej przeglądarki oprogramowanie oferuje informacje dotyczące wykonywania różnych operacji, narzędzia i szczegółowy przewodnik instruktażowy. Oprogramowanie zgodne jest z systemami takimi jak Windows XP, Windows 2000 i Windows Server 2003 (z zainstalowanym serwerem SBS). Wersja instalacyjna aplikacji ma postać pliku wykonywalnego (*SGK_v1.exe*) o wielkości około 150 MB. Po zapisaniu pliku na dysku komputera, w celu jego uruchomienia należy go dwukrotnie kliknąć. Na rysunku 4.3 pokazano opcje widoczne po wybraniu odnośnika *Enhance Server Security*, natomiast na rysunku 4.4 listę dostępnych narzędzi (wyświetlana po kliknięciu odnośnika *List All Tools*).

Jeśli pobrano plik, konieczne będzie umożliwienie mu instalacji szkieletu .NET w przypadku, gdy nie jest dostępny. Kolejną operacją będzie instalacja samego narzędzia *Security Guidance Kit* (dwukrotne kliknięcie pliku *SGK_v1.exe* spowoduje otwarcie okna powitalnego, a następnie zostaniesz poproszony o wykonanie trzech kolejnych kroków). Narzędzie można później odinstalować. W tym celu z menu *Start* należy wybrać pozycję *Panel sterowania/Dodaj lub usuń programy*, a następnie zaznaczyć pozycję *Microsoft Security Guidance Kit* i kliknąć przycisk *Usuń*. Usunięcie programu nie spowoduje usunięcia z systemu szkieletu .NET. Jeśli zaistnieje taka potrzeba, szkielet należy usunąć osobno przez zaznaczenie pozycji *Microsoft .NET Framework 1.1* (również dostępna po wybraniu z menu *Start* pozycji *Panel sterowania/Dodaj lub usuń programy*).



Rysunek 4.4. *Lista narzędzi oferowana przez program Security Guidance Kit 1.0*

Podsumowanie

A zatem, przeczytałeś rozdział poświęcony zabezpieczeniom i powinieneś się czuć naprawdę pewnie w trakcie zarządzania zabezpieczeniami sieci. Wynika to stąd, że wiesz, jakie podjąć działania, aby zabezpieczyć sieć i masz świadomość tego, że nie jest to takie trudne, jak mogłoby się wydawać. Podczas lektury pozostałej części książki trzeba pamiętać o zagadnieniach dotyczących zabezpieczeń i od czasu do czasu powracać do tego rozdziału. W niniejszym rozdziale zapoznałeś się z najlepszymi praktykami związanymi z zabezpieczeniami, dzięki czemu możesz lepiej zabezpieczyć sieć i spędzać więcej czasu na spotkaniach. Chyba coś nie tak, ponieważ akurat to drugie nie jest prawdą.

- Zabezpieczanie jest ciągle trwającym procesem, który jednak można ogarnąć przez zdefiniowanie konsekwentnie stosowanych praktyk, zasad i procedur.
- Na początku należy zapoznać się z konfiguracją sieci, routera, firewalla i serwera. Dzięki temu przez niepoprawną konfigurację nie utworzy się luk w zabezpieczeniach.

- Należy podjąć kroki mające na celu zabezpieczenie serwera. Obejmują one fizyczne zabezpieczenia, konfigurację, a także zastosowanie aktualizacji i poprawek.
- Najlepszą metodą zabezpieczania stacji roboczych jest aktualizacja starszych systemów operacyjnych i instalowanie w nich najnowszych uaktualnień (poprawki i dodatki Service Pack), a także aktualizowanie na bieżąco aplikacji.
- Użytkowników należy edukować w zakresie stosowania bezpiecznych praktyk dotyczących kont i haseł.
- Na bieżąco należy powiadamiać użytkowników o nowych i powstających dopiero zagrożeniach dotyczących zabezpieczeń, a zwłaszcza o wirusach poczty elektronicznej, „robakach", *phishingu* i innych metodach włamań inicjowanych za pośrednictwem internetu.
- Dla kluczowych zdarzeń powiązanych z siecią należy uaktywnić monitorowanie, rejestrowanie i inspekcję. Regularnie należy przeglądać wygenerowane pliki dzienników i raporty pod kątem występowania podejrzanych zachowań.
- Abyś, korzystając z jednego narzędzia, miał możliwość zapoznania się z metodami zarządzania zabezpieczeniami sieci złożonej z komputerów z systemem Windows, powinieneś pobrać oprogramowanie *Security Guidance Kit 1.0*.