

O Autorze (9)

Przedmowa (11)

- Bezpieczeństwo w systemie Windows 2000 (12)
- Dla kogo jest przeznaczona niniejsza książka? (12)
- Nowości w systemie zabezpieczeń Windows 2000 (13)
- Układ książki (13)
- W jaki sposób korzystać z niniejszej książki (15)

Rozdział 1. Bezpieczeństwo w systemie Windows 2000 (17)

- W skrócie (18)
 - o Active Directory w systemie Windows 2000 (18)
 - o Zabezpieczenia rozproszone i protokoły zabezpieczeń (19)
 - o Korzystanie z kart inteligentnych (20)
 - o Szyfrowanie (21)
 - o Bezpieczeństwo protokołu IP (21)
 - o Wirtualne sieci prywatne (22)
 - o Narzędzia do konfigurowania i analizowania zabezpieczeń (22)
- Bezpośrednie rozwiązania (23)
 - o Struktura Active Directory (23)
 - o Zintegrowane zarządzanie kontami zabezpieczeń (24)
 - o Wykorzystywanie obustronnych przechodnich relacji zaufania (25)
- Delegowanie administrowania (27)
 - o Zastosowanie Listy kontroli dostępu do precyzyjnego ustalania praw dostępu (28)
 - o Zastosowanie protokołów zabezpieczeń (29)
 - o Zastosowanie interfejsu dostawcy zabezpieczeń (30)
 - o Zastosowanie protokołu uwierzytelniania Kerberos 5 (32)
 - o Zastosowanie certyfikatów z kluczem publicznym do zapewnienia bezpieczeństwa w Internecie (36)
 - o Implementowanie dostępu między przedsiębiorstwami (41)
 - o Rozwiązania na skalę całego przedsiębiorstwa (42)
 - o Zastosowanie danych uwierzytelniających protokołu NTLM (43)
 - o Zastosowanie danych uwierzytelniających w przypadku stosowania protokołu Kerberos (43)
 - o Zastosowanie par kluczy prywatny-publiczny i certyfikatów (43)
 - o Zastosowanie protokołu IPSec (45)
 - o Zastosowanie Wirtualnych sieci prywatnych (46)
 - o Zastosowanie narzędzi do konfigurowania zabezpieczeń (47)
 - o Zmiana systemu z Windows NT 4 na Windows 2000 (49)

Rozdział 2. Active Directory i Lista kontroli dostępu (51)

- W skrócie (51)
 - o Active Directory w systemie Windows 2000 (51)
- Bezpośrednie rozwiązania (54)
 - o Obsługa standardów otwartych (54)
 - o Obsługa standardowych formatów nazw (55)
 - o Zastosowanie interfejsów API (56)

- o Zastosowanie programu Windows Scripting Host (59)
- o Możliwości rozbudowy (62)
- o Zastosowanie zabezpieczeń rozproszonych (67)
- o Zastosowanie rozszerzenia ustawienia zabezpieczeń edytora zasad grupy (68)
- o Analiza domyślnych ustawień kontroli dostępu (70)
- o Analiza członkostwa w grupach domyślnych (74)
- o Przełączanie pomiędzy kontekstami użytkowników (76)
- o Synchronizacja komputerów po aktualizacji systemu z domyślnymi ustawieniami zabezpieczeń (76)
- o Zastosowanie przystawki Szablony zabezpieczeń (77)
- o Zastosowanie Edytora listy kontroli dostępu (80)

Rozdział 3. Zasady grup (83)

- W skrócie (84)
 - o Możliwości zasad grup i korzyści z ich stosowania (84)
 - o Zasady grup a usługi Active Directory (85)
- Rozwiązania natychmiastowe (88)
 - o Łączenie zasad grup ze strukturą Active Directory (88)
 - o Konfigurowanie przystawki Zarządzanie Zasadami grup (89)
 - o Dostęp do zasad grup domeny lub jednostki organizacyjnej (90)
 - o Tworzenie obiektu zasad grup (91)
 - o Edycja obiektu zasad grup (93)
 - o Nadawanie użytkownikowi prawa do logowania się lokalnie na kontrolerze domeny (94)
 - o Zarządzanie Zasadami grup (95)
 - o Dodawanie lub przeglądanie obiektu zasad grup (96)
 - o Ustanawianie dziedziczenia i zastępowania zasad grup (98)
 - o Wyłączanie części obiektu zasad grupy (101)
 - o Dołączanie obiektu zasad grup do wielu lokacji, domen i jednostek organizacyjnych (102)
 - o Administrowanie zasadami bazujących na Rejestrze (104)
 - o Przygotowywanie skryptów (108)
 - o Ustawianie odpowiednich uprawnień dla poszczególnych członków grup zabezpieczeń (110)
 - o Dopasowanie zasad do danego komputera za pomocą sprzężenia zwrotnego (112)
 - o Konfigurowanie zasad inspekcji (116)

Rozdział 4. Protokoły zabezpieczeń (119)

- W skrócie (119)
 - o Protokoły (119)
 - o Porównanie protokołów NTLM i Kerberos (120)
- Rozwiązania natychmiastowe (121)
 - o Konfigurowanie protokołów ze wspólnym kluczem tajnym (121)
 - o Zastosowanie Centrum dystrybucji kluczy (124)
 - o Podstawowe wiadomości o podprotokołach protokołu Kerberos (127)
 - o Uwierzytelnianie logowania (130)
 - o Analiza biletów protokołu Kerberos (136)

- o Delegowanie uwierzytelniania (139)
- o Konfigurowanie zasad protokołu Kerberos domeny (140)
- o Dostawca obsługi zabezpieczeń Kerberos (141)
- o Zastosowanie interfejsu dostawcy obsługi zabezpieczeń (142)

Rozdział 5. System szyfrowania plików (147)

- W skrócie (147)
 - o Dlaczego konieczne jest szyfrowanie danych (147)
 - o System szyfrowania plików (148)
- Rozwiązania natychmiastowe (153)
 - o Zastosowanie polecenia Cipher (153)
 - o Szyfrowanie foldera lub pliku (154)
 - o Odszyfrowywanie foldera lub pliku (156)
 - o Kopiowanie, przenoszenie i zmiana nazwy zaszyfrowanego foldera lub pliku (157)
 - o Wykonywanie kopii zapasowych plików lub folderów zaszyfrowanych (158)
 - o Odtwarzanie zaszyfrowanego foldera lub pliku (160)
 - o Odtwarzanie plików do innego komputera (162)
 - o Zabezpieczenia domyślnego klucza odzyskiwania na pojedynczym komputerze (165)
 - o Zabezpieczanie domyślnego klucza odzyskiwania dla domeny (166)
 - o Dodawanie agentów odzyskiwania (167)
 - o Ustawianie zasad odzyskiwania dla konkretnej jednostki organizacyjnej (170)
 - o Odzyskiwanie pliku lub foldera (170)
 - o Wyłączanie systemu szyfrowania plików dla określonego zestawu komputerów (171)

Rozdział 6. Klucze publiczne (173)

- W skrócie (173)
 - o Kryptografia z kluczem publicznym (173)
 - o Ochrona i określanie zaufania do kluczy kryptograficznych (175)
 - o Składniki Infrastruktury klucza publicznego systemu Windows 2000 (177)
- Rozwiązania natychmiastowe (180)
 - o Uaktywnianie klientów domeny (180)
 - o Stosowanie zabezpieczeń z kluczem publicznym systemu Windows 2000 (186)
 - o Ustawianie zabezpieczeń sieci Web (188)
 - o Zastosowanie uwierzytelniania za pomocą klucza publicznego w programie Internet Explorer (189)
 - o Konfigurowanie programu Microsoft Outlook, aby korzystał z protokołu Secure Sockets Layer (191)
 - o Konfigurowanie zabezpieczeń poczty elektronicznej z zastosowaniem klucza publicznego (192)
 - o Konfigurowanie zabezpieczeń z zastosowaniem klucza publicznego dla programu Outlook Express (193)
 - o Konfigurowanie zabezpieczeń z zastosowaniem klucza publicznego dla programu Microsoft Outlook (198)
 - o Uzyskiwanie współdziałania (200)

Rozdział 7. Usługi certyfikatów (203)

- W skrócie (203)
 - o Certyfikaty (203)
 - o Instalowanie urzędu certyfikacji w przedsiębiorstwie (206)
 - o Relacja zaufania w strukturach hierarchicznych z wieloma urzędami certyfikacji (207)
- Rozwiązania natychmiastowe (208)
 - o Instalowanie urzędu certyfikacji (208)
 - o Zastosowanie stron internetowych usług certyfikatów (211)
 - o Instalowanie certyfikatów urzędów certyfikacji (213)
 - o Żądanie certyfikatów zaawansowanych (216)
 - o Rejestrowanie za pomocą pliku żądania w formacie PKCS #10 (219)
 - o Konfigurowanie relacji zaufania pomiędzy domeną a zewnętrznym urzędem certyfikacji (220)
 - o Instalowanie automatycznego żądania certyfikatów dla komputerów (222)
 - o Uruchamianie i zatrzymywanie usług certyfikatów (223)
 - o Wykonywanie kopii zapasowych i odtwarzanie usług certyfikatów (223)
 - o Wyświetlanie dziennika i bazy danych usług certyfikatów (226)
 - o Odwoływanie wydanych certyfikatów i publikowanie Listy odwołań certyfikatów (227)
 - o Konfigurowanie modułów zasad i modułów zakończenia dla usług certyfikatów (229)

Rozdział 8. Mapowanie certyfikatów do kont użytkowników (233)

- W skrócie (233)
 - o Dlaczego konieczne jest mapowanie certyfikatów (233)
 - o Rodzaje mapowania (234)
 - o Gdzie dokonywane jest mapowanie? (235)
- Rozwiązania natychmiastowe (236)
 - o Instalowanie certyfikatu użytkownika (236)
 - o Eksportowanie certyfikatu (239)
 - o Instalowanie certyfikatu urzędu certyfikacji (241)
 - o Konfigurowanie Active Directory, dla mapowania głównej nazwy użytkownika (242)
 - o Konfigurowanie Active Directory, dla mapowania jeden-do-jednego (247)
 - o Konfigurowanie Internetowych usług informacyjnych (IIS) dla mapowania jeden-do-jednego (248)
 - o Konfigurowanie Active Directory, dla mapowania wiele-do-jednego (250)
 - o Konfigurowanie Internetowych usług informacyjnych (IIS), dla mapowania wiele-do-jednego (251)
 - o Testowanie mapowania (252)

Rozdział 9. Karty inteligentne (257)

- W skrócie (257)
 - o Co to jest karta inteligentna? (257)
 - o Współdziałanie kart inteligentnych (259)
 - o Obsługiwane karty inteligentne (261)

- o Obsługiwane czytniki kart inteligentnych (262)
- Rozwiązania natychmiastowe (263)
 - o Instalowanie czytników kart inteligentnych (263)
 - o Instalowanie stacji rejestrowania kart inteligentnych (265)
 - o Wydawanie kart inteligentnych (268)
 - o Logowanie za pomocą kart inteligentnych (271)
 - o Logowanie się za pomocą uwierzytelniania klienta (275)
 - o Wdrażanie kart inteligentnych (276)
 - o Rozwiązywanie problemów związanych z kartami inteligentnymi (278)
 - o Zabezpieczanie stacji rejestrowania kart inteligentnych (280)
 - o Umieszczanie aplikacji na kartach inteligentnych (281)
 - o Zastosowanie pakietu Smart Card Software Development Kit (282)
 - o Zastosowanie interfejsów API firmy Microsoft (287)
 - o Zastosowanie interfejsu Java Card API 2.1 (289)
 - o Zastosowanie osnowy aplikacji OpenCard (290)

Rozdział 10. Zabezpieczenia protokołu IP (293)

- W skrócie (293)
 - o Zabezpieczenia za pomocą IP Security (293)
 - o Właściwości IPsec (294)
 - o Skojarzenia zabezpieczeń (296)
- Rozwiązania natychmiastowe (298)
 - o Analiza działania IPsec (298)
 - o Ustawienia IPsec (299)
 - o Konfigurowanie IPsec na pojedynczych komputerach (303)
 - o Konfigurowanie IPsec dla domeny (307)
 - o Zmiana metody zabezpieczeń (308)
 - o Konfigurowanie IPsec dla jednostki organizacyjnej (309)

Rozdział 11. Wirtualne sieci prywatne (313)

- W skrócie (313)
 - o Zastosowanie Wirtualnych sieci prywatnych (313)
 - o Tunelowanie (314)
 - o Uwierzytelnianie (316)
 - o Porównanie protokołów PPTP i L2TP (317)
 - o Protokół RADIUS (318)
- Rozwiązania natychmiastowe (319)
 - o Określanie strategii Wirtualnych sieci prywatnych (319)
 - o Konfigurowanie serwera VPN (324)
 - o Konfigurowanie serwera VPN (326)
 - o Konfigurowanie klienta VPN (327)
 - o Organizowanie kont użytkowników usługi Dostęp zdalny (329)
 - o Tworzenie zasad dostępu zdalnego dla połączeń VPN router-router (330)
 - o Włączanie uwierzytelniania wzajemnego (331)
 - o Automatyczne uzyskiwanie certyfikatu komputera (332)
 - o Dodawanie portów L2TP i PPTP (333)
 - o Konfigurowanie serwera usługi RADIUS (334)

Rozdział 12. Narzędzia do konfigurowania i analizowania zabezpieczeń (335)

- W skrócie (335)
 - o Narzędzia do konfigurowania (335)
 - o Ustawienia szablonów zabezpieczeń (337)
 - o Skonfigurowane wstępnie Szablony zabezpieczeń (338)
- Rozwiązania natychmiastowe (340)
 - o Tworzenie i analizowanie konfiguracji zabezpieczeń (340)
 - o Edytowanie konfiguracji zabezpieczeń (342)
 - o Eksportowanie konfiguracji zabezpieczeń (344)
 - o Edytowanie Szablonów zabezpieczeń (345)
 - o Zastosowanie polecenia Secedit (347)

Dodatek A Słownik (353)

Dodatek B Podstawowe informacje (367)

- Polecenia uruchamiane z linii poleceń (367)
- Dokumenty RFC (367)
- Grupy i organizacje (368)
- Źródła informacji (369)
- Strona powitalna usług certyfikatów Microsoftu (370)
- Magazyny certyfikatów CryptoAPI (370)
- Zawartość biletu protokołu Kerberos (370)
- Domyślne ustawienia zabezpieczeń (372)
- Zdefiniowane wstępnie szablony zabezpieczeń (372)
- Host skryptów Cscript (373)
- Program narzędziowy Cipher (374)
- Polecenie Secedit (375)

Skorowidz (377)