Podziękowania (17)
O autorze (19)
Przedmowa (21)
CZĘŚĆ II Podstawy zabezpieczeń (27)
Rozdział 1. Zasady dotyczące bezpieczeństwa informacji (29)

- Zasada numer jeden: nie ma czegoś takiego jak bezpieczny komputer (30)
- Klasyczne zasady dotyczące zabezpieczeń: poufność, integralność i inspekcja (32)
    - Poufność (32)
    - Integralność (34)
    - Inspekcja (35)
- Wnioski: zasady powstałe na bazie zasad klasycznych (36)
    - Rozbudowana ochrona (36)
    - Psychologiczna akceptacja (39)
    - Zasada najmniejszych przywilejów (40)
    - Wdrażanie zasad zabezpieczeń (41)
    - Podział obowiązków (42)
    - Całkowita mediacja (42)
    - Aktualizowanie na bieżąco (43)
    - Użycie otwartych rozwiązań (43)
    - Zmniejszenie pola ataku (44)
    - Domyślne zabezpieczenia awaryjne (44)
    - Jednoczesne ufanie i kontrolowanie (45)
    - Szkolenie i uświadamianie każdego (45)
    - Ekonomia i różnorodność mechanizmów (45)

CZĘŚĆ II Zabezpieczanie serwera (47)
Rozdział 2. Uwierzytelnianie: dowód tożsamości (49)

- Proces logowania (51)
    - Typy logowania (53)
    - Proces logowania interaktywnego (54)
    - Uwierzytelnianie w domenie i sieci (55)
- Procesy uwierzytelniania w sieci (56)
    - Protokół LM (57)
    - Protokół Kerberos (68)
    - Konfigurowanie protokołu Kerberos za pomocą jego zasad (83)
    - Certyfikaty, karty inteligentne, żetony i dane biometryczne (84)
- Usługa czasu systemu Windows (86)
- Konta komputerów i kontrolowanie uwierzytelniania (89)
    - Tworzenie kont komputerów i ich hasła (89)
    - Przetwarzanie kont komputerów (90)
- Dostęp anonimowy (92)
- Zarządzanie uwierzytelnianiem za pomocą zasad grupy (93)
    - Zasady konta (93)
    - Zasady haseł (98)
    - Zasady blokady konta (98)
    - Ograniczenia konta użytkownika (100)
    - Zasady kont lokalnych i dysk resetowania hasła (102)
- Uwierzytelnianie w lesie i między lasami (104)

    - Relacja zaufania obszaru (105)
- Najlepsze praktyki dotyczące zabezpieczania uwierzytelniania (106)
- Podsumowanie (107)

Rozdział 3. Autoryzacja - ograniczanie dostępu do systemu i kontrolowanie działań użytkownika (109)

- Architektura zabezpieczeń systemu Windows i proces autoryzacji (111)
- Prawa, przywileje i uprawnienia (115)
    - Prawa wbudowane (115)
    - Prawa logowania (116)
    - Dodawanie i usuwanie predefiniowanych praw użytkownika (127)
    - Zalecenia dotyczące ograniczania praw (129)
    - Najlepsze praktyki dotyczące przypisywania praw użytkownika (133)
- Kontrola dostępu za pomocą uprawnień do obiektów (134)
    - Podstawowe informacje na temat uprawnień (135)
    - Łączenie uprawnień (138)
    - Najlepsze praktyki dotyczące przypisywania uprawnień do obiektów (140)
    - Uprawnienia drukarki i prawo własności do niej (140)
- Porównanie systemów kontroli dostępu opartych na regułach i rolach (144)
    - Zastosowanie w sieci z serwerami z systemem Windows Server 2003 kontroli dostępu opartej na rolach (145)
- Domyślne role systemu operacyjnego (147)
    - Domyślne konta użytkowników (148)
    - Systemowe konta użytkowników (149)
    - Grupy (150)
    - Zakres grupy (153)
    - Zarządzanie użytkownikami i grupami (154)
- Tworzenie niestandardowych ról (159)
- Tworzenie dla ról niestandardowych grup (160)
    - Najlepsze praktyki dotyczące lokalnych użytkowników i grup (161)
- Proces kontroli dostępu (162)
    - Zarządzanie informacjami zastrzeżonymi (164)
- Autoryzacja za pomocą opcji zabezpieczeń i wpisów rejestru (164)
- Role komputerowe (168)
- Dostęp anonimowy (169)
    - Podmioty zabezpieczeń, autoryzacja i dostęp anonimowy (169)
    - Anonimowy dostęp do zasobów (170)
    - Ogólnie znane identyfikatory SID (172)
- Ochrona bazy danych haseł kont przy użyciu narzędzia Syskey (181)
- Podsumowanie (184)

Rozdział 4. Ograniczanie dostępu do oprogramowania i kontrolowanie dostępu aplikacji do zasobów (185)

- Narzędzie Menedżer autoryzacji (187)
    - Podstawowe informacje na temat narzędzia Menedżer autoryzacji (191)
    - Inspekcja narzędzia Menedżer autoryzacji (211)
    - Zarządzanie narzędziem Menedżer autoryzacji (212)
- Zasady ograniczeń oprogramowania (213)

    - Możliwości zasad ograniczeń oprogramowania (214)
    - Podstawowe informacje dotyczące zasad ograniczeń oprogramowania (215)
    - Tworzenie i stosowanie zasad ograniczeń oprogramowania (217)
    - Rozwiązywanie problemów związanych z zasadami ograniczeń oprogramowania (236)
    - Najlepsze praktyki dotyczące zasad ograniczeń oprogramowania (238)
- Zabezpieczanie aplikacji COM, COM+ i DCOM za pomocą usługi Usługi składowe (240)
- Podsumowanie (254)

Rozdział 5. Kontrolowanie dostępu do danych (257)

- Kontrolowanie dostępu do plików i folderów za pomocą uprawnień NTFS (258)
    - Uprawnienia do plików i folderów (259)
    - Domyślne uprawnienia (263)
    - Interpretowanie uprawnień (266)
    - Struktura systemu plików NTFS dysku (266)
    - Dziedziczenie uprawnień (267)
    - Porównanie atrybutów i wydajności systemu plików NTFS z jego zabezpieczeniami (280)
- Kontrolowanie dostępu do udziałów (281)
    - Uprawnienia udziałów (283)
    - Tryb udostępniania plików i drukarek (283)
    - Domyślne udziały (284)
    - Proste udostępnianie plików - nowy model stworzony dla systemu Windows XP (285)
    - Tworzenie udziałów (288)
    - Zdalne zarządzanie udziałami (291)
    - Najlepsze praktyki dotyczące udostępniania plików i drukarek (291)
- Kontrolowanie dostępu do folderów sieci Web za pomocą protokołu WebDAV (293)
    - Uaktywnianie protokołu WebDAV (297)
    - Tworzenie folderu przeznaczonego do udostępnienia i przypisanie mu uprawnień NTFS (297)
    - Tworzenie katalogu wirtualnego (297)
    - Konfigurowanie zabezpieczeń dla katalogu wirtualnego (299)
    - Konfigurowanie klienta (300)
- Kontrolowanie dostępu do kluczy rejestru (301)
    - Domyślne uprawnienia do rejestru (301)
    - Stosowanie uprawnień do rejestru (303)
- Praktyczne zagadnienia związane z wdrażaniem zabezpieczeń (305)
    - Kwestie dotyczące uprawnień starszych aplikacji (305)
    - Alternatywne strumienie danych (308)
    - Definiowanie uprawnień za pomocą szablonów zabezpieczeń (311)
    - Przywracanie i odporność na błędy (312)
    - Klastry (312)
    - System DFS (313)
    - Skuteczne zarządzanie opcjami zabezpieczeń i prawami użytkowników (314)
    - Kontrolowanie dostępu do dzienników zdarzeń (316)
- Podsumowanie (318)

Rozdział 6. System EFS - podstawy (319)

- Czym jest System szyfrowania plików EFS? (320)
- Różnice między wersjami systemu Windows dotyczące funkcji szyfrowania (321)
- Podstawowe operacje (322)
    - Szyfrowanie i odszyfrowywanie (324)
    - Archiwizowanie certyfikatów i kluczy (328)
    - Importowanie certyfikatu i kluczy (333)
    - Usuwanie klucza prywatnego (334)
    - Przywracanie plików (335)
    - Uzyskiwanie kluczy szyfrujących (336)
    - Dodawanie agenta przywracania (337)
- Wpływ standardowych operacji na zaszyfrowane pliki (338)
- Architektura systemu EFS (340)
    - Operacje wykonywane przez system plików (341)
    - Algorytmy szyfrowania, odszyfrowywania i przywracania (343)
    - Typy i siła szyfrowania (346)
- Zapobieganie utracie danych - planowanie przywracania (347)
    - Plan przywracania dla komputerów autonomicznych i domen pozbawionych urzędów certyfikacji (348)
    - Zasada przywracania i wyłączanie systemu EFS (350)
    - Narzędzia służące do przywracania (354)
- Specjalne kwestie i operacje (356)
    - Zmiana algorytmu szyfrowania (356)
    - Umieszczenie w menu programu Eksplorator Windows poleceń Szyfruj i Odszyfruj (357)
    - Archiwizowanie zaszyfrowanych plików (357)
    - Przetwarzanie plików trybu offline (358)
    - Udostępnianie zaszyfrowanych plików (358)
    - Ochrona przed skutkami resetowania hasła (362)
    - Wyróżnianie kolorami nazw zaszyfrowanych plików i folderów w oknie programu Eksplorator Windows (363)
    - Stosowanie zewnętrznych certyfikatów systemu EFS (364)
    - System EFS i funkcja Przywracanie systemu (364)
    - Wykrywanie i przeglądanie certyfikatów (364)
- Magazyn zdalny (365)
    - Udziały SMB (366)
    - Protokół WebDAV (368)
- Pewne strategie dla przedsiębiorstwa (368)
- Narzędzia (370)
    - Program cipher (370)
    - Program esfinfo (372)
- Rozwiązywanie problemów (372)
- Podsumowanie (373)

CZĘŚĆ III Zabezpieczanie usług domeny (375)
Rozdział 7. Rola usługi Active Directory w bezpieczeństwie domeny (377)

- Usługa Active Directory a bezpieczeństwo (378)
- Organizacja, struktura i funkcje usługi Active Directory (379)

    - Struktura hierarchiczna (380)
    - Replikacja (384)
    - Zasady grupy (386)
    - Delegowanie uprawnień administracyjnych (391)
    - Zależność od usługi DNS (392)
- Instalacja usługi Active Directory: zmiany w czasie wykonywania dcpromo (393)
- Zarządzanie użytkownikami i komputerami za pomocą usługi Active Directory (397)
    - Wpływ domyślnego obiektu GPO (398)
    - Tworzenie i konfigurowanie użytkowników, grup i komputerów w domenach usługi Active Directory (400)
    - Delegowanie administracji - użycie Kreatora delegowania kontroli (413)
    - Poznajemy listy ACL usługi Active Directory (418)
- Narzędzia zasad grupy (425)
    - Edytor zasad grupy (426)
    - Konsola Group Policy Management (439)
- Różnice w zarządzaniu obiektami GPO w Windows 2000 (463)
- Najlepsze praktyki dotyczące zasad grupy (463)
- Podsumowanie (464)

Rozdział 8. Zaufanie (465)

- Nowe funkcje zaufania w Windows Server 2003 (466)
- Typy zaufania (467)
    - Międzydomenowe relacje zaufania Kerberos (468)
    - Skrót zaufania (469)
    - Zaufania Windows NT 4.0 (470)
    - Z (471)
    - Relacje zaufania z obszarem Kerberos innym niż Windows (473)
    - Zaufanie lasu (474)
- Relacje zaufania (474)
    - Zalety zaufania lasu (475)
    - Poziom funkcjonalności lasu i domeny (480)
    - Zakres grupy (489)
    - Typy grup (489)
    - Grupy przedsiębiorstwa (490)
    - Funkcja wykazu globalnego (491)
- Procedury tworzenia zewnętrznych relacji zaufania (495)
    - Tworzenie zewnętrznej relacji zaufania (497)
    - Tworzenie zewnętrznego zaufania z domeną Windows NT 4.0 (502)
- Zaufanie lasu (507)
    - Przychodzące i wychodzące zaufania lasu (508)
    - Uwierzytelnianie i autoryzacja między lasami (510)
    - Tworzenie zaufania lasu (511)
    - Zabezpieczanie lasów w relacji zaufania między lasami przed atakiem podnoszącym uprawnienia (516)
- Zasady grupy w scenariuszach z lasem i wieloma lasami (517)
    - Zastosowanie konsoli GPMC w lasach wielodomenowych oraz w wielu lasach (518)
    - Zastosowanie tabel migracji (519)
- Przebijanie granic zabezpieczeń - zasadniczy problem przy projektowaniu lasu (523)

    - Filtrowanie identyfikatorów SID - przechwytywanie fałszywych identyfikatorów SID (525)
    - Uwierzytelnianie selektywne - firewall zaufania (527)
- Najlepsze praktyki zaufania (527)
- Podsumowanie (528)

Rozdział 9. Usuwanie problemów z zasadami grupy (529)

- Określanie, czy zostały zastosowane zasady grupy (533)
    - Zastosowanie konsoli GPMC (533)
    - Zastosowanie wynikowego zbioru zasad (537)
    - Zastosowanie GPResult (539)
- Sprawdzanie, czy projekt zasad grupy został prawidłowo zaimplementowany (541)
- Rozwiązywanie problemów z siecią (552)
    - Rozwiązywanie problemów z uwierzytelnianiem (553)
    - Rozwiązywanie podstawowych problemów z siecią (553)
    - Rozwiązywanie problemów z usługą DNS (554)
    - Zastosowanie DCDIAG oraz NetDiag do znalezienia problemów z usługą DNS (560)
    - Zastosowanie programu Portqry (563)
    - Ręczne wyszukiwanie problemów w rekordach DNS (563)
    - Wykorzystanie polecenia nslookup do testowania serwera DNS (563)
    - Analizowanie zdarzeń z dziennika systemowego (564)
- Rozwiązywanie problemów z replikacją usługi Active Directory oraz FRS (565)
    - Problemy z relacjami zaufania (565)
    - Problemy z replikacją usługi Active Directory (566)
    - Zastosowanie programu DNSLint do testowania replikacji (567)
    - Wykorzystanie replmon.exe do kontroli replikacji (569)
    - Zastosowanie repadmin.exe do kontrolowania łączy między partnerami replikacji (571)
    - Użycie aplikacji GPOTool.exe, Podgląd zdarzeń oraz konsoli GPMC do kontroli brakujących lub uszkodzonych plików (577)
    - Rozszerzone rejestrowanie (577)
- Rozwiązywanie problemów z projektem obiektów zasad grupy (586)
- Monitorowanie stanu obiektów GPO (588)
- Podsumowanie (591)

Rozdział 10. Zabezpieczanie usługi Active Directory (593)

- Fizyczne zabezpieczenie kontrolerów domeny (595)
    - Fizyczne bezpieczeństwo wszystkich kontrolerów domeny (595)
    - Fizyczne bezpieczeństwo biur oddziałów i małych biur (602)
    - Fizyczne bezpieczeństwo ekstranetów i sieci brzegowych (607)
- Tworzenie konfiguracji zabezpieczeń (608)
    - Podstawowa konfiguracja zabezpieczeń kontrolera domeny (609)
    - Konfiguracja szablonów zabezpieczeń i zasad domeny (610)
    - Zasady lokalne (617)
    - Ustawienia dziennika zdarzeń (624)
    - Usługi systemowe (626)
    - Rejestr i system plików (627)

- Dodatkowa konfiguracja zabezpieczeń (630)
- Zapewnienie bezpiecznych praktyk administracyjnych (630)
    - Problemy z personelem (631)
    - Zabezpieczanie roli administratora (631)
    - Zabezpieczenie aplikacji oraz dostępu użytkowników do kontrolerów domeny (636)
- Wdrażanie bezpiecznych kontrolerów domeny (637)
    - Przygotowanie (638)
    - Automatyzacja instalacji kontrolera domeny (643)
    - Bezpieczna replikacja (644)
- Podsumowanie (645)

Rozdział 11. Zabezpieczanie ról infrastruktury (647)

- Szablony zabezpieczeń (648)
- Jak korzystać z szablonów zabezpieczeń do zabezpieczenia komputerów według roli (651)
    - Tworzenie i modyfikowanie szablonów (654)
    - Tworzenie podstawowych szablonów do zabezpieczania wszystkich serwerów (657)
    - Przegląd przykładowych szablonów i ich dostosowanie do konkretnego środowiska (659)
    - Zastosowanie szablonów przyrostowych i innych technik do zapewnienia bezpieczeństwa komputerom infrastruktury (671)
    - Rozszerzanie koncepcji na inne role (684)
- Zastosowanie szablonów zabezpieczeń (685)
    - Zastosowanie projektu Active Directory do zabezpieczenia ról komputerów (685)
    - Zastosowanie narzędzia Konfiguracja i analiza zabezpieczeń (687)
- Podsumowanie (693)

CZĘŚĆ IV Infrastruktura klucza publicznego (695)
Rozdział 12. Infrastruktura PKI - podstawy (697)

- Wprowadzenie do infrastruktury PKI (698)
    - Procesy kryptograficzne klucza publicznego (698)
    - Składniki infrastruktury PKI (702)
- Architektura infrastruktury PKI w Windows Server 2003 (711)
    - Magazyn certyfikatów (712)
    - Szablony certyfikatów (714)
    - Zasady praktyk oraz pliki zasad praktyk (720)
    - Urzędy certyfikacji (723)
    - Hierarchia urzędów certyfikacji (724)
    - Lista odwołań certyfikatów (CRL) (728)
    - Różnicowe listy CRL (730)
    - Role urzędu certyfikacji (731)
- Działanie usług certyfikatów (735)
    - Cykl życia certyfikatu (735)
- Podsumowanie (758)

Rozdział 13. Wdrażanie bezpiecznej infrastruktury PKI (761)

- Instalowanie głównego urzędu certyfikacji w trybie offline (762)
  - Przygotowanie serwera (763)
  - Tworzenie pliku capolicy.inf (765)
  - Instrukcja instalacji głównego urzędu certyfikacji w trybie offline (766)
  - K (770)
- Instalowanie i konfiguracja podrzędnego urzędu certyfikacji (784)
  - Instalowanie podrzędnego urzędu certyfikacji (785)
  - Włączenie obsługi ASP dla serwera IIS (785)
- Zastosowanie własnych szablonów do konfigurowania archiwizacji kluczy dla EFS (803)
- Podsumowanie (809)

CZĘŚĆ V Zabezpieczanie sieci wirtualnej (811)
Rozdział 14. Zabezpieczanie zdalnego dostępu (813)

- Zabezpieczanie tradycyjnych usług zdalnego dostępu (814)
  - Bezpieczna instalacja usługi RRAS i przygotowanie usługi IAS systemu Windows Server 2003 (815)
  - Instalowanie i konfigurowanie usługi RRAS (817)
  - Instalowanie i konfigurowanie serwera IAS (830)
  - Konfigurowanie klientów na potrzeby korzystania ze zdalnego dostępu (836)
  - Określanie właściwości konta użytkownika pod kątem zdalnego dostępu (836)
  - Proces nawiązywania połączenia zdalnego dostępu (848)
  - Konfigurowanie uwierzytelniania i inspekcji dla serwerów RRAS i IAS (849)
  - Zastosowanie technologii VPN (856)
  - Protokół L2TP/IPSec oraz technologie NAT i NAT-T (859)
  - Porty firewalla używane przez protokoły połączenia VPN (860)
  - Kwarantannowa kontrola dostępu do sieci (861)
- Zabezpieczanie dostępu bezprzewodowego za pomocą usługi IAS (868)
  - Wbudowane funkcje zabezpieczeń protokołu 802.11 (868)
  - Standard WPA (870)
  - Zastosowanie technologii VPN (871)
  - Zastosowanie standardu 802.1x (872)
  - Zabezpieczanie klientów bezprzewodowych (882)
- Zabezpieczanie dostępu do wewnętrznych zasobów udzielanego za pośrednictwem serwera WWW (885)
  - Podstawy dotyczące zabezpieczeń serwera WWW (885)
  - Kwestie związane ze zdalnym dostępem (891)
- Podsumowanie (894)

Rozdział 15. Ochrona przesyłanych danych (895)

- Zastosowanie podpisywania pakietów SMB (896)
- Zastosowanie zabezpieczania sesji protokołu NTLM (897)
- Zastosowanie zasad protokołu IPSec (897)
  - Stosowanie protokołu IPSec w systemie Windows Server 2003 (899)
  - Tworzenie zasad protokołu IPSec (905)
  - Operacje realizowane za pomocą specjalnych zasad protokołu IPSec (924)

    - Monitorowanie i diagnozowanie protokołu IPSec (927)
- Zastosowanie protokołu SSL (933)
    - Zasady działania protokołu SSL (933)
    - Zastosowanie protokołu SSL w przypadku serwera IIS (936)
- Podpisywanie przez serwer LDAP (942)
- Podsumowanie (945)

CZĘŚĆ VI Konserwacja i przywracanie (947)
Rozdział 16. Strategie konserwacyjne i praktyki administracyjne (949)

- Strategie konserwacyjne dotyczące zarządzania zmianami (950)
    - Konserwacja zasady zabezpieczeń (951)
    - Aktualizowanie zabezpieczeń (954)
- Strategie konserwacyjne dotyczące zarządzania poprawkami (958)
    - Zarządzanie poprawkami (958)
    - Stosowanie poprawek (962)
- Praktyki dotyczące zarządzania (987)
    - Zastosowanie praktyk dotyczących bezpiecznego zarządzania (987)
    - Ochrona procesu administracyjnego (990)
    - Ochrona kont administracyjnych (990)
    - Zabezpieczanie narzędzi służących do zdalnej administracji (991)
- Podsumowanie (1012)

Rozdział 17. Archiwizacja i odtwarzanie danych - podstawy (1013)

- Zasady, standardy i procedury dotyczące archiwizacji (1015)
    - Podstawowe informacje na temat archiwizowania bazy danych usługi Active Directory (1016)
    - Rola archiwizacji w planie utrzymania ciągłości procesów biznesowych organizacji (1018)
- Zastosowanie narzędzia Kopia zapasowa (1018)
    - Archiwizowanie plików i folderów (1019)
    - Archiwizowanie danych o stanie systemu (1025)
    - Domyślne ustawienia programu Kopia zapasowa i jego opcje konfiguracyjne (1027)
    - Uruchamianie programu Kopia zapasowa z poziomu wiersza poleceń (1030)
    - Odtwarzanie plików i folderów (1031)
    - Odtwarzanie z kopii zapasowej danych o stanie systemu (1035)
- Automatyczne przywracanie systemu (1035)
- Usługa Kopiowanie woluminów w tle (1038)
    - Tworzenie kopii woluminów w tle (1040)
    - Odtwarzanie danych z kopii woluminów w tle (1044)
    - Zarządzanie kopiami woluminów w tle z poziomu wiersza poleceń (1045)
- Różne narzędzia archiwizacyjne (1046)
    - Archiwizowanie danych istotnych dla użytkownika (1047)
- Reanimowanie użytkowników z magazynu usuniętych obiektów (1052)
- Odtwarzanie bazy danych usługi Active Directory (1053)
    - Normalne odtwarzanie (1055)
    - Odtwarzanie autorytatywne (1055)
- Proces archiwizacji danych serwera IIS (1062)

- Archiwizowanie danych urzędu certyfikacji (1064)
- Podsumowanie (1066)

CZĘŚĆ VII Monitorowanie i inspekcja (1067)
Rozdział 18. Inspekcja (1069)

- Tworzenie zasad inspekcji Windows Server 2003 dla lasu (1072)
    - Podstawy zasad inspekcji (1073)
- Inspekcja autonomicznego komputera Windows Server 2003 (1092)
- Inspekcja aplikacji i usług serwera (1093)
    - Inspekcja usług sieciowych (1093)
    - Inspekcja protokołu IPSec (1097)
    - Inspekcja urzędu certyfikacji (1097)
    - Inspekcja dostępu VPN (1098)
    - Inspekcja menedżera autoryzacji (1101)
    - Rejestrowanie debugowania logowania do sieci (1102)
- Inspekcja mechanizmów zabezpieczeń: zgodność z zasadami, określanie słabych punktów oraz testowanie przez penetrację (1103)
    - Inspekcja konfiguracji zabezpieczeń z użyciem konsoli Konfiguracja i analiza zabezpieczeń (1105)
    - Inspekcja konfiguracji zabezpieczeń dla specyficznych komputerów (1107)
    - Wyszukiwanie znanych usterek zabezpieczeń (1109)
    - Testowanie przez penetrację (1114)
- Inspekcja zabezpieczeń fizycznych (1115)
- Inspekcja zasad, standardów oraz procedur (1116)
- Kontrola świadomości bezpieczeństwa (1117)
- Inspekcja osób obcych: wpływ osób postronnych na bezpieczeństwo danych organizacji (1118)
- Podsumowanie (1118)

Rozdział 19. Monitorowanie i ocena (1119)

- Definicja podstaw działania (1120)
- Podstawy usług monitorowania (1122)
    - Monitorowanie serwera DNS i połączeń sieciowych (1122)
    - Monitorowanie serwera DHCP (1127)
    - Monitorowanie infrastruktury PKI (1128)
    - Monitorowanie routingu i zdalnego dostępu (1130)
    - Monitorowanie udziałów (1132)
    - Monitorowanie wszystkich aktywnych usług (1133)
- Monitorowanie usługi Active Directory oraz zasad grupy (1134)
    - Zastosowanie dcdiag do uzyskania ogólnego raportu o stanie kontrolera domeny (1136)
    - Monitorowanie replikacji usługi Active Directory (1140)
    - Monitorowanie replikacji plików (1147)
    - Monitorowanie działania zasad grupy (1153)
    - Zastosowanie monitorowania wydajności (1156)
- Monitorowanie dziennika zdarzeń (1162)
    - Zastosowanie programu EventCombMT (1162)
    - Zastosowanie programu Lockoutstatus (1164)

- Wprowadzenie do odpowiedzi na włamanie (1165)
- Podsumowanie (1167)

Bibliografia (1169)
Skorowidz (1171)