

O autorach (19)

Wstęp (21)

Część I Podstawowe założenia bezpieczeństwa systemu informatycznego (29)

Rozdział 1. Podstawowe założenia strategii bezpieczeństwa systemu informatycznego (31)

- Podstawowe założenia bezpieczeństwa sieci (32)
 - o Poufność (32)
 - o Integralność (32)
 - o Dostępność (32)
 - o Inne ważne terminy (33)
- Procesy formalne (33)
 - o Procesy inżynierii systemów (33)
 - o Zasady technicznego zabezpieczenia informacji (34)
 - o Proces inżynierii bezpieczeństwa systemu informatycznego (39)
 - o Cykl rozwoju systemu (48)
 - o Bezpieczeństwo systemu informatycznego i cykl rozwoju systemu (SDLC) (49)
- Zarządzanie ryzykiem (57)
 - o Definicje (58)
 - o Zarządzanie ryzykiem w ramach cyklu rozwoju systemu (59)
- Podsumowanie (68)

Rozdział 2. Zarządzanie bezpieczeństwem systemu informatycznego (69)

- Polityka bezpieczeństwa (70)
 - o Oświadczenie polityki zarządu (70)
 - o Standardy, zalecenia, procedury i wzorce (72)
- Świadomość bezpieczeństwa (72)
 - o Szkolenie (73)
 - o Pomiar świadomości (73)
- Zarządzanie działaniami natury technicznej (74)
 - o Menedżer programu (74)
 - o Plan zarządzania programem (75)
 - o Plan zarządzania inżynierią systemów (75)
- Zarządzanie konfiguracją (81)
 - o Podstawowe funkcje zarządzania konfiguracją (83)
 - o Definicje i procedury (83)
- Planowanie ciągłości działań biznesowych oraz przywracania systemu po awariach (85)
 - o Planowanie ciągłości działań biznesowych (86)
 - o Planowanie przywracania systemu po awariach (90)
- Bezpieczeństwo fizyczne (94)
 - o Mechanizmy kontrolne (95)
 - o Czynniki środowiskowe (99)
 - o Zabezpieczenia przeciwpożarowe (100)
 - o Ponowne wykorzystanie zasobów i magnetyzm szkodliwy (101)
- Zagadnienia prawne i odpowiedzialność (102)
 - o Rodzaje przestępstw komputerowych (102)
 - o Monitorowanie elektroniczne (102)

- o Odpowiedzialność (103)
- Podsumowanie (103)

Rozdział 3. Kontrola dostępu (105)

- Modele kontroli (105)
 - o Uznaniowa kontrola dostępu (106)
 - o Obligatoryjna kontrola dostępu (106)
 - o Ogólna kontrola dostępu (107)
- Typy implementacji mechanizmów kontroli dostępu (107)
 - o Mechanizmy zapobiegawcze i środki administracyjne (107)
 - o Mechanizmy zapobiegawcze i środki techniczne (108)
 - o Mechanizmy zapobiegawcze i środki fizyczne (108)
 - o Mechanizmy wykrywające i środki administracyjne (108)
 - o Mechanizmy wykrywające i środki techniczne (109)
 - o Mechanizmy wykrywające i środki fizyczne (109)
 - o Scentralizowane i zdecentralizowane mechanizmy kontroli dostępu (110)
- Identyfikacja i uwierzytelnianie (110)
 - o Hasła (111)
 - o Biometryka (111)
 - o Mechanizm pojedynczego logowania (112)
- Bazy danych (116)
 - o Bazy relacyjne (116)
 - o Inne typy baz danych (118)
- Dostęp zdalny (119)
 - o RADIUS (119)
 - o TACACS oraz TACACS+ (119)
 - o Protokół PAP (120)
 - o Protokół CHAP (120)
 - o Oddzwanianie (121)
- Podsumowanie (121)

Część II Systemy operacyjne i aplikacje (123)

Rozdział 4. Bezpieczeństwo systemów MS Windows (125)

- Bezpieczeństwo Windows w sercu systemu ochrony (127)
 - o Kto chciałby mnie skrzywdzić? (127)
 - o Należy się obawiać (129)
 - o Zalecenia firmy Microsoft (129)
- Wzmacnianie świeżo zainstalowanego systemu (132)
 - o Czynności wstępne (132)
 - o Ogólny opis procesu wzmacniania systemu (132)
 - o Przykład czystej instalacji systemu Windows 2003 (135)
 - o Szczegółowe zagadnienia wzmacniania systemu (137)
 - o Zabezpieczanie typowej biznesowej stacji roboczej z systemem Windows (141)
 - o Zabezpieczanie systemu Windows przeznaczonego do gier (142)
- Instalacja aplikacji (143)
 - o Zabezpieczenie antywirusowe (143)
 - o Osobiste zapory sieciowe (145)

- o Secure Shell (SSH) (145)
 - o Secure FTP (146)
 - o Pretty Good Privacy (147)
- Przyłączenie stacji roboczej do sieci (147)
 - o Testowanie wzmocnionej stacji (147)
 - o Bezpieczeństwo fizyczne (148)
 - o Architektura (148)
 - o Zapora sieciowa (149)
 - o Systemy detekcji włamań (149)
- Bezpieczne użytkowanie systemu Windows (150)
 - o Identyfikacja ryzykownych praktyk (150)
 - o Zagadnienia ochrony fizycznej (151)
 - o Konfiguracja (152)
 - o Kontrola konfiguracji (155)
 - o Zagadnienia operacyjne (157)
- Aktualizacja wersji systemu i poprawki (166)
 - o Aktualizacje wersji i poprawki oprogramowania firmy Microsoft (166)
 - o Utrzymywanie aktualności systemu przez instalacje aktualizacji i poprawek (167)
 - o Utrzymanie aktualności sygnatur antywirusowych (168)
 - o Wykorzystanie jak najnowszej wersji Windows (168)
- Utrzymanie i testowanie zabezpieczeń (169)
 - o Poszukiwanie słabych punktów (169)
 - o Testowanie niepewnych aplikacji (169)
 - o Nieoczekiwane zmiany wydajności systemu (170)
 - o Wymiana starych wersji systemu Windows (170)
 - o Okresowa analiza i przebudowa systemu (171)
 - o Monitorowanie (171)
 - o Dzienniki systemowe i audyt (172)
 - o Oczyszczanie systemu (172)
 - o Przygotowanie na wypadek ataku (173)
- Ataki na stacje robocze z systemem Windows (174)
 - o Wirusy (174)
 - o Robaki (175)
 - o Konie trojańskie (176)
 - o Oprogramowanie szpiegowskie i reklamowe (176)
 - o Oprogramowanie szpiegowskie typu "Wielki Brat" (178)
 - o Ataki fizyczne (178)
 - o Ataki TEMPEST (179)
 - o Tylne drzwi (179)
 - o Ataki typu DoS (180)
 - o Rozszerzenia nazw plików (181)
 - o Podśluchiwanie pakietów (181)
 - o Przechwytywanie i wznowianie sesji (181)
 - o Socjotechnika (182)
- Podsumowanie (182)

Rozdział 5. Bezpieczeństwo systemów Unix i Linux (185)

- Zadania zabezpieczeń systemów Unix i Linux (185)

- o Unix jako cel ataku (186)
 - o Unix i Linux jako trudny cel ataków (188)
 - o Otwarty kod źródłowy - zagadnienia (189)
- Bezpieczeństwo fizyczne (191)
 - o Ograniczanie dostępu (191)
 - o Wykrywanie zmian sprzętowych (193)
 - o Podział dysku na partycje (194)
 - o Przygotowanie na ewentualny atak (195)
- Kontrola konfiguracji (196)
 - o Zainstalowane pakiety (197)
 - o Konfiguracje jądra (198)
- Bezpieczna obsługa systemu Unix (205)
 - o Kontrola procesów (205)
 - o Kontrola użytkowników (218)
 - o Szyfrowanie i certyfikaty (225)
- Wzmacnianie systemu Unix (227)
 - o Konfiguracja (227)
 - o TCP wrapper (229)
 - o Sprawdzanie siły haseł (230)
 - o Filtrowanie pakietów z użyciem iptables (230)
- Podsumowanie (231)

Rozdział 6. Bezpieczeństwo przeglądarek i klientów WWW (233)

- Ryzyko powodowane przez przeglądarki WWW (233)
 - o Prywatność a bezpieczeństwo (234)
 - o Wygoda przeglądarek WWW (234)
 - o Wszechstronność i popularność przeglądarki WWW (235)
 - o Ewolucja przeglądarek (236)
 - o Zagrożenia przeglądarek WWW (236)
 - o Czynniki działające na niekorzyść napastnika (237)
- Sposób działania przeglądarek WWW (237)
 - o HTTP - protokół stron WWW (237)
 - o Cookies (240)
 - o Utrzymanie stanu (241)
 - o Buforowanie (243)
 - o SSL (243)
- Ataki na przeglądarki WWW (247)
 - o Atak przechwytyjący (247)
 - o Atak powtórzenia (248)
 - o Pasożyty przeglądarek (249)
- Bezpieczne użytkowanie przeglądarek (250)
 - o Instalacja poprawek (250)
 - o Unikanie wirusów (251)
 - o Wykorzystanie bezpiecznych stron WWW (251)
 - o Zabezpieczanie środowiska sieciowego (253)
 - o Zastosowanie bezpiecznego serwera pośredniczącego (253)
 - o Unikanie ujawniania prywatnych danych (254)
 - o Zalecenia ogólne (254)
- Konfiguracja przeglądarki WWW (256)

- o Cookies (256)
- o Wtyczki (257)
- o Zagadnienia specyficzne dla przeglądarek Mozilla Firefox (261)
- o Zagadnienia specyficzne dla przeglądarek Internet Explorer (262)
- Podsumowanie (267)

Rozdział 7. Bezpieczeństwo WWW (269)

- Protokół HTTP (269)
- Mechanizm działania HTTP (271)
 - o Implementacja HTTP (274)
 - o Połączenia trwałe (276)
 - o Model klient-serwer (278)
 - o PUT (279)
 - o GET (280)
 - o Burstable TCP (280)
 - o HTML (282)
- Obsługa aktywnej zawartości po stronie serwera (282)
 - o Skrypty CGI (283)
 - o Strony PHP (283)
- Obsługa aktywnej zawartości po stronie klienta (284)
 - o JavaScript (284)
 - o Java (285)
 - o ActiveX (287)
- Stan (290)
 - o Stan w aplikacji WWW (290)
 - o Związek stanu z protokołem HTTP (290)
 - o Aplikacje wymagające śledzenia stanu (290)
 - o Śledzenie stanu (291)
 - o Cookies (291)
 - o Pluskwy stron WWW (294)
 - o Śledzenie adresów URL (294)
 - o Ukryte ramki (295)
 - o Ukryte pola formularza (295)
- Ataki wykorzystujące strony WWW (296)
 - o Zbieranie danych o użytkownikach (296)
 - o Wymuszanie kodu SQL (297)
- Projektowanie serwisu e-commerce (298)
 - o Lokalizacja fizyczna (298)
- Podsumowanie (300)

Rozdział 8. Bezpieczeństwo poczty elektronicznej (301)

- Ryzyko związane z pocztą elektroniczną (301)
 - o Podatność danych (301)
 - o Prosta poczta elektroniczna a mechanizmy pracy grupowej (302)
 - o Spam (313)
 - o Poufność poczty elektronicznej (316)
 - o Integralność poczty elektronicznej (316)
 - o Dostępność poczty elektronicznej (317)

- Protokoły poczty elektronicznej (317)
 - SMTP (317)
 - POP (320)
 - IMAP (322)
- Uwierzytelnianie w poczcie elektronicznej (322)
 - Proste logowanie (322)
 - Logowanie uwierzytelniane (323)
 - APOP (324)
 - NTLM, czyli SPA (324)
 - POP before SMTP (325)
 - Kerberos oraz GSSAPI (326)
- Bezpieczne użytkowanie poczty elektronicznej (326)
 - Zachować czujność (326)
 - Konfiguracja programu pocztowego (327)
 - Wersje aplikacji (328)
 - Architektura systemu (328)
 - Tunel SSH (329)
 - PGP oraz GPG (333)
- Podsumowanie (333)

Rozdział 9. DNS (335)

- Zadania DNS (336)
 - Zapytania proste (341)
 - Zapytania odwrotne (341)
- Alternatywne sposoby odwzorowania nazw (343)
- Problemy bezpieczeństwa związane z DNS (344)
 - Błędy konfiguracji (344)
 - Transfery stref (346)
 - Przewidywalne identyfikatory zapytań (349)
 - Zapytania rekurencyjne i iteracyjne (350)
- Ataki na usługę DNS (351)
 - Proste ataki na usługę DNS (351)
 - Zatrucie pamięci podręcznej (352)
- Projektowanie usługi DNS (353)
 - Podzielony DNS (353)
 - Krzyżowy DNS (353)
- Serwery DNS nadrzędne i podrzędne (353)
- Szczegóły architektury DNS (355)
- Podsumowanie (356)

Rozdział 10. Bezpieczeństwo serwerów (357)

- Ogólne zagrożenia serwerów (357)
- Projektowanie z myślą o bezpieczeństwie (358)
 - Właściwe podejście do zagadnień bezpieczeństwa (359)
 - Pozyskanie bezpiecznego środowiska rozwoju aplikacji (364)
 - Bezpieczne praktyki rozwoju oprogramowania (368)
 - Testy, testy, testy (375)
- Bezpieczne użytkowanie serwerów (377)

- o Kontrola konfiguracji serwera (377)
 - o Kontrola użytkowników i dostępu (379)
 - o Hasła (380)
 - o Monitorowanie, audyty i dzienniki systemowe (381)
- Zastosowania serwerów (381)
 - o Wymiana danych (382)
 - o Sieci peer to peer (385)
 - o Komunikatory internetowe i chat (386)
- Podsumowanie (387)

Część III Podstawy bezpieczeństwa sieciowego (389)

Rozdział 11. Protokoły sieciowe (391)

- Protokoły (391)
- Model ISO OSI (392)
- Warstwy modelu ISO OSI (392)
 - o Warstwa aplikacji (392)
 - o Warstwa prezentacji (394)
 - o Warstwa sesji (394)
 - o Warstwa transportowa (395)
 - o Warstwa sieci (396)
 - o Warstwa łącza danych (397)
 - o Warstwa fizyczna (398)
- Model TCP/IP (399)
- Warstwy modelu TCP/IP (400)
- Translacja adresów sieciowych (NAT) (400)
- Podsumowanie (402)

Rozdział 12. Bezpieczeństwo sieci bezprzewodowych (403)

- Spektrum fal elektromagnetycznych (403)
- Sieć telefonów komórkowych (405)
- Wykonywanie połączeń w telefonii komórkowej (407)
- Systemy bezprzewodowej transmisji danych (408)
 - o Wielodostęp w dziedzinie czasu (408)
 - o Wielodostęp w dziedzinie częstotliwości (409)
 - o Wielodostęp kodowy (409)
 - o Typy bezprzewodowych systemów transmisji danych (409)
- Technologie sieci bezprzewodowych (413)
 - o Technologia widma rozproszonego (413)
 - o Podstawy działania technologii widma rozproszonego (415)
- Specyfikacje bezprzewodowych sieci lokalnych IEEE (418)
 - o Warstwa fizyczna PHY (419)
 - o Warstwa kontroli dostępu do nośnika MAC (419)
- Bezpieczeństwo sieci bezprzewodowych 802.11 (420)
 - o WEP (421)
 - o Podnoszenie bezpieczeństwa protokołu WEP (423)
 - o 802.11i (428)
- Bluetooth (433)
- Protokół WAP (434)

- Podsumowanie (436)

Rozdział 13. Podstawy architektury sieci (437)

- Segmenty sieci (438)
 - o Sieci publiczne (438)
 - o Sieci półprywatne (439)
 - o Sieci prywatne (439)
- Ochrona zewnętrzna (439)
- Translacja adresów sieciowych (440)
- Podstawowe elementy architektury (441)
- Podsieci, przełączanie i sieci typu VLAN (444)
- Adresy MAC i protokół ARP (446)
- Protokół DHCP i kontrola adresów (447)
- Zapory sieciowe (448)
 - o Zapory sieciowe filtrujące pakiety (449)
 - o Filtrowanie pakietów na podstawie stanu (451)
 - o Pośredniczące zapory sieciowe (453)
 - o Wady zapór sieciowych (453)
- Systemy wykrywania włamań (454)
 - o Rodzaje systemów wykrywania włamań (455)
 - o Metody i tryby wykrywania włamań (458)
- Reakcje na wykrycie włamania (461)
- Typowe ataki (462)
- Podsumowanie (463)

Część IV Komunikacja (465)

Rozdział 14. Komunikacja utajniona (467)

- Ogólne pojęcia (468)
- Historia kryptografii (469)
 - o Szyfry podstawieniowe (469)
 - o Szyfry, które tworzyły historię (475)
- Cztery podstawowe elementy kryptografii (475)
 - o Generatory liczb losowych (476)
- Obsada (479)
- Szyfrowanie symetryczne (480)
 - o Szyfry strumieniowe (482)
 - o Szyfry blokowe (483)
 - o Współużytkowanie kluczy (485)
- Szyfrowanie asymetryczne (487)
 - o Wykorzystywanie certyfikatów (488)
 - o Sieci zaufania (489)
 - o Podpisy cyfrowe (490)
 - o Funkcje mieszające (491)
 - o Funkcje mieszające korzystające z kluczy (493)
- Łączenie podstawowych elementów kryptografii w celu uzyskania CIA (493)
- Różnice pomiędzy algorytmem a implementacją (495)
- Algorytmy własnościowe i otwarte (496)
- Podsumowanie (497)

Rozdział 15. Tajna komunikacja (499)

- Gdzie kryją się ukryte dane? (499)
- Skąd wzięła się steganografia? (501)
- Dokąd zmierza steganografia? (501)
- Przegląd steganografii (501)
 - o Do czego jest potrzebna steganografia? (503)
 - o Zalety steganografii (503)
 - o Wady steganografii (504)
 - o Porównanie z innymi technikami (504)
- Historia steganografii (506)
 - o Steganografia w walce o imperium rzymskie (507)
 - o Steganografia podczas wojen (507)
- Podstawowe aspekty bezpieczeństwa sieci i ich związek ze steganografią (508)
 - o Poufność (508)
 - o Integralność (509)
 - o Dostępność (509)
 - o Dodatkowe cele steganografii (509)
- Zasady steganografii (510)
- Steganografia a kryptografia (511)
 - o Przykład z zabezpieczaniem pierścionka (511)
 - o Składanie elementów (511)
- Typy steganografii (513)
 - o Pierwotny system klasyfikacji (513)
 - o Nowy system klasyfikacji (515)
 - o Tablice kolorów (518)
- Produkty implementujące steganografię (519)
 - o S-Tools (519)
 - o Hide and Seek (522)
 - o Jsteg (523)
 - o EZ-Stego (526)
 - o Image Hide (526)
 - o Digital Picture Envelope (527)
 - o Camouflage (529)
 - o Gif Shuffle (530)
 - o Spam Mimic (532)
- Steganografia a cyfrowe znaki wodne (533)
 - o Co to jest cyfrowy znak wodny? (534)
 - o Do czego potrzebne są cyfrowe znaki wodne? (534)
 - o Cechy cyfrowych znaków wodnych (534)
- Typy cyfrowych znaków wodnych (535)
 - o Niewidoczne znaki wodne (535)
 - o Widoczne znaki wodne (535)
- Cele stosowania cyfrowych znaków wodnych (536)
- Cyfrowe znaki wodne a steganografia (536)
 - o Zastosowania cyfrowych znaków wodnych (537)
 - o Usuwanie cyfrowych znaków wodnych (537)
- Podsumowanie (539)

Rozdział 16. Aplikacje bezpiecznej i tajnej komunikacji (541)

- E-mail (542)
 - o Protokoły POP/IMAP (542)
 - o PGP (542)
 - o Kerberos (544)
- Serwery uwierzytelniające (545)
- Model praktyczny (546)
- PKI - infrastruktura klucza publicznego (549)
 - o Klucze prywatne i publiczne (549)
 - o Zarządzanie kluczami (551)
 - o Sieć zaufania (552)
- Wirtualne sieci prywatne (553)
 - o Problemy projektowania (553)
 - o Sieci VPN wykorzystujące protokoły IPsec (555)
 - o Tryby pracy protokołu IPsec (556)
 - o Wirtualne sieci prywatne związane z protokołami PPTP/PPP (558)
 - o SSH (559)
- SSL/TLS (560)
- Protokół uzgodnień SSL - SSL handshake (560)
- Podsumowanie (564)

Część V Zagrożenia i reakcja (565)

Rozdział 17. Wykrywanie włamań i reagowanie na atak (567)

- Szkodliwy kod (567)
 - o Wirusy (567)
- Przegląd popularnych ataków (569)
 - o Blokada usług i rozproszona blokada usług (569)
 - o Tylne drzwi (570)
 - o Fałszowanie adresu (570)
 - o Człowiek w środku (570)
 - o Odtworzenie (571)
 - o Przejmowanie sesji TCP (571)
 - o Fragmentacja (571)
 - o Słabe klucze (572)
 - o Ataki matematyczne (572)
 - o Inżynieria społeczna (572)
 - o Skanowanie portów (573)
 - o Nurkowanie w śmieciach (573)
 - o Atak metodą dnia urodzin (574)
 - o Odgadywanie haseł (574)
 - o Wykorzystywanie luk w oprogramowaniu (575)
 - o Niewłaściwe wykorzystanie systemu (575)
 - o Podśluch (576)
 - o Rozpoznanie mobilne (576)
 - o Ataki z wykorzystaniem numerów sekwencyjnych TCP/IP (576)
 - o Rozpoznanie telefoniczne (576)
- Mechanizmy wykrywania włamań (576)
 - o Systemy antywirusowe (577)
 - o Wykrywanie włamań i reagowanie na atak (577)
 - o Systemy IDS oparte na sieci (578)

- Garnki miodu (581)
 - o Cele (582)
 - o Kategorie garnków miodu (583)
 - o Kiedy należy używać garnka miodu? (583)
 - o Kiedy nie należy używać garnka miodu? (584)
 - o Obecne rozwiązania (585)
 - o Honeynet Project (585)
- Reakcja na incydenty (586)
 - o Zalecenia CERT/CC (587)
 - o Zalecenia Internet Engineering Task Force (591)
 - o Ochrona wielowarstwowa a systemy IDS (592)
 - o Zespoły ds. bezpieczeństwa komputerowego i reakcji na incydenty (593)
 - o Proces powiadamiania o incydentach naruszenia bezpieczeństwa (594)
 - o Zautomatyzowane mechanizmy powiadamiania o atakach i usuwania ich skutków (595)
- Podsumowanie (596)

Rozdział 18. Szacowanie, testowanie i ocena zabezpieczeń (597)

- Metodologie oceny poziomu bezpieczeństwa informacji (597)
 - o Systems Security Engineering Capability Maturity Model (SSE-CMM) (597)
 - o Infosec Assessment Methodology (IAM) (598)
 - o Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) (600)
 - o Federal Information Technology Security Assessment Framework (FITSAF) (600)
- Certyfikacja i akredytacja (601)
 - o National Information Assurance Certification and Accreditation Process (NIACAP) (601)
 - o Cztery fazy procesu NIACAP (602)
 - o DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (603)
 - o Cztery fazy procesu DITSCAP (604)
- Federal Information Processing Standard 102 (604)
- Okólnik OMB A-130 (605)
- Wytyczne oceny opracowane przez National Institute of Standards and Technology (606)
 - o SP 800-14 (607)
 - o SP 800-27 (607)
 - o SP 800-30 (608)
 - o SP 800-64 (610)
- Testowanie penetracyjne (611)
 - o Wewnętrzny test penetracyjny (612)
 - o Zewnętrzny test penetracyjny (612)
 - o Test z pełną wiedzą o sieci (612)
 - o Test z częściową wiedzą o sieci (612)
 - o Test bez wiedzy o sieci (612)
 - o Test na systemie zamkniętym (613)
 - o Test na systemie otwartym (613)
- Inspekcje i monitorowanie (613)

- o Inspekcje (613)
- o Monitorowanie (614)
- Podsumowanie (615)

Rozdział 19. Łączenie wszystkiego w całość (617)

- Kluczowe problemy, z którymi zmagają się organizacje (617)
 - o Jak przekonać kierownictwo, że bezpieczeństwo jest ważne i że warto za nie zapłacić? (617)
 - o Jak radzić sobie ze zwiększoną liczbą ataków? (618)
 - o Jak sprawić, aby pracownicy byli częścią rozwiązania, a nie częścią problemu? (619)
 - o Jak analizować dane z dzienników? (619)
 - o Jak poradzić sobie z różnymi systemami w moim przedsiębiorstwie i upewnić się, że są bezpieczne? (620)
 - o Skąd mam wiedzieć, czy jestem celem szpiegostwa korporacyjnego albo innych ataków? (621)
 - o Dziesięć najczęstszych pomyłek (621)
- Ogólne wskazówki dotyczące zabezpieczania sieci (623)
 - o Dogłębna ochrona (623)
 - o Zasada minimalnych przywilejów (624)
 - o Wiedza o oprogramowaniu działającym w systemie (624)
 - o Prewencja to ideał, ale wykrywanie to konieczność (625)
 - o Stosowanie i testowanie poprawek (625)
 - o Regularne kontrolowanie systemu (626)
- Podsumowanie (626)

Dodatki (627)

Skorowidz (629)