O Autorach (11)
Wprowadzenie (13)
Rozdział 1. Pojęcia kluczowe: ryzyko, zagrożenia i wrażliwość systemu (17)

- Pierwsze kroki (17)
- Określenie zasobów (19)
    - Informacje zastrzeżone i własność intelektualna (19)
    - Reputacja firmy lub jej wizerunek (20)
    - Procesy biznesowe (20)
- Zagrożenia (20)
    - Zagrożenia wewnętrzne (21)
    - Zagrożenia zewnętrzne (23)
- Określanie ryzyka (24)
- Podsumowanie (25)

Rozdział 2. Tworzenie bezpiecznej infrastruktury sieciowej (27)

- Potrzeba bezpieczeństwa (27)
- Co oznacza termin "bezpieczeństwo"? (28)
- Proces zapewnienia bezpieczeństwa (29)
- Ocena i polityka (31)
    - Programy IA (32)
    - Ocena funkcjonalna (34)
    - Tworzenie polityki (37)
    - Tworzenie procedur i dokumentów operacyjnych (38)
    - Ocena techniczna (39)
- Ochrona zasobów (47)
    - Wdrożenie polityki bezpieczeństwa (47)
    - Środki ochronne (48)
- Monitorowanie i wykrywanie (51)
    - Przeglądanie dzienników zdarzeń systemowych (52)
    - Systemy wykrywania włamań (IDS) (53)
    - Fuzja danych (54)
- Reakcja i odzyskiwanie danych (55)
- Podsumowanie (56)

Rozdział 3. Komponenty infrastruktury sieciowej - z dalszej perspektywy (59)

- Podstawowe informacje i połączenie z Internetem (60)
    - Dostawcy usług internetowych (60)
    - Jakie usługi oferuje ISP? (63)
    - Wybór dostawcy usług internetowych a kwestie bezpieczeństwa (64)
- Transport informacji (66)
    - Adresowanie (67)
    - Sieci (67)
    - Wyznaczanie drogi pakietów (68)
    - Ogólny opis TCP/IP (69)
    - Usługa identyfikacji nazw domen (71)
- Zarządzanie Internetem (74)
    - ICANN (75)

    - Rejestracja nazw domen (77)
    - Bazy danych whois (78)
- Co sprawia, że Internet jest (nie)bezpieczny? (79)
    - Brak wbudowanych technologii zabezpieczających (80)
    - Domniemane zaufanie (80)
    - Brak uwierzytelniania (81)
    - Anonimowość (81)
    - Brak prywatności (82)
    - Brak centralnego zarządzania systemami bezpieczeństwa i danymi logowania (82)
    - Codzienne praktyki służące zachowaniu niezbędnego poziomu bezpieczeństwa nie są łatwe! (83)
- Dlaczego Internet jest tak atrakcyjny dla biznesu? (83)
    - Obsługa serwisów sieciowych (84)
    - Przekazywanie danych (85)
    - Usługi informacyjne (85)
    - Usługi finansowe (86)
    - Produkty (86)
- Podsumowanie (87)

Rozdział 4. Protokoły warstw aplikacji i sieci: TCP/IP (89)

- Wprowadzenie: jak ważne są szczegóły? (89)
- Krótka historia pracy w sieci i protokołów (90)
    - ARPANET (91)
    - NSFnet (93)
    - Komercjalizacja Internetu (94)
    - Model OSI i jego związek z protokołami TCP/IP (96)
    - Warstwa łącza danych: przesyłanie informacji przez jeden kanał transmisji (96)
    - Warstwa sieci: przesyłanie informacji przez kilka łączy wykorzystujących protokół IP (100)
    - Protokoły trasowania (106)
    - ICMP (107)
    - System nazw domen (DNS) (108)
    - Ponowna wizyta na warstwie łącza danych: Ethernet i IP (114)
    - Konfiguracja komputera do pracy w sieci IP (117)
- Warstwa transportowa: bezpieczny transfer danych przy wykorzystaniu protokołu TCP (i nie tak znowu bezpieczny przy wykorzystaniu UDP) (118)
    - Multipleksowanie dzięki UDP (118)
    - Zwiększanie niezawodności dzięki TCP (120)
    - Kontrolowanie połączeń TCP (122)
    - Najczęściej wykorzystywane porty (124)
- Najczęściej spotykane protokoły warstwy aplikacji (126)
    - Najbardziej znane protokoły internetowe (126)
    - Zdalne wywołania procedury (RPC) w systemie Unix (126)
- SNMP (128)
- Protokoły sieciowe Microsoft i TCP/IP (129)
    - Krótka historia IBM i sieci Microsoft Networks (129)
    - Nazwy NetBIOS (130)

    - NetBIOS over TCP (NBT) (130)
    - SMB i dzielenie plików (132)
    - Otoczenie sieciowe i Browser Protocol (132)
    - RPC w sieciach Microsoft (132)
    - Ogólne wskazówki dotyczące konfiguracji sieci domowych (133)
    - Podsumowanie zagadnień dotyczących protokołów sieciowych z rodziny Microsoft (133)
- Krótka wzmianka o innych protokołach sieciowych (133)
- Podsumowanie (135)

Rozdział 5. Protokoły bezpieczeństwa (137)

- Bezpieczne protokoły (138)
    - Implementacja protokołów bezpieczeństwa (138)
    - Rozwiązania zwiększające bezpieczeństwo - warstwa sieci (139)
- Protokoły wirtualnych sieci prywatnych i kapsułkowanie (140)
    - IPSec (141)
    - Połączenia punkt-punkt z tunelowaniem (protokół PPTP) (148)
    - L2F (149)
    - Layer 2 Tunneling Protocol (150)
    - Protokół bezpiecznej transmisji danych SSL (151)
    - Algorytm WEP (153)
- Powłoka bezpieczeństwa (SSH) (154)
    - Uwierzytelnianie SSH (154)
    - Uwierzytelnianie serwera SSH (154)
    - Tunelowanie SSH (155)
- Uwierzytelnianie (155)
    - Hasła (157)
    - Mechanizm pytanie-odpowiedź (160)
    - Mechanizmy biometryczne (161)
    - Certyfikaty cyfrowe (162)
- Podsumowanie (165)

Rozdział 6. Przykłady architektury sieciowej i analiza konkretnych rozwiązań (167)

- Tworzenie bezpiecznej sieci (167)
- Sieć korporacyjna (168)
    - Typowa sieć zakładowa (169)
    - Zagrożenia z zewnątrz (169)
    - Zabezpieczanie łączy zewnętrznych (172)
    - Łącza wewnętrzne i zagrożenia (186)
- Sieć SOHO (195)
- Witryny internetowe (197)
    - Zewnętrzne serwery hostingowe (197)
    - Witryny dostarczające treści (197)
    - Witryny e-commerce (199)
- Podsumowanie (201)

Rozdział 7. System operacyjny i oprogramowanie serwera (203)

- Koncepcje bezpieczeństwa w systemach Windows NT i 2000 (204)
  - Uwierzytelnianie, środki dostępu, identyfikatory bezpieczeństwa (205)
  - Lista kontroli dostępu do obiektów (206)
  - Zdalne wywołania procedur (RPC) i model obiektów składowych (COM) (208)
  - Mechanizmy bezpieczeństwa RPC/COM (209)
  - Umacnianie Windows (210)
  - Ograniczanie praw użytkowników w systemach Windows (214)
- Inspekcja zdarzeń bezpieczeństwa (215)
- Koncepcje bezpieczeństwa w systemach Linux (216)
  - Spojrzenie na jądro systemu operacyjnego Linux (216)
  - Spojrzenie na przestrzeń użytkownika z systemie Linux (217)
  - Prawa dostępu do plików w systemie Linux (217)
  - Mechanizmy uwierzytelniania w systemie Linux (220)
  - Jak działa PAM? (220)
  - Struktura /etc/pam.conf (221)
  - Przykłady dyrektyw PAM (223)
- Uniksowe usługi sieciowe i sposoby ich zabezpieczenia (224)
  - Dostęp zdalny i transfer plików (225)
  - Graficzny interfejs użytkownika (226)
  - RPC (229)
  - NFS (230)
- Bezpieczeństwo oprogramowania (232)
  - Zaczynamy od bezpiecznego systemu operacyjnego (232)
  - Bezpieczeństwo serwera sieciowego (234)
  - Bezpieczeństwo serwera poczty (235)
  - Bezpieczeństwo serwera nazw (238)
  - Bezpieczeństwo serwerów ftp (243)
- Podsumowanie (243)

Rozdział 8. Scenariusze ataków (245)

- Ataki DoS (246)
  - Jeden strzał, jeden zabity - ataki DoS (246)
  - Wyczerpanie zasobów systemowych - ataki DoS (247)
  - Nadużycie sieci (249)
  - Amplification attack (250)
  - Fragmentation attack (251)
  - Rozproszony atak typu "odmowa usług" (DDoS) (251)
- Techniki penetracji systemów (253)
- Rekonesans (255)
  - Zbieranie informacji o sieci (256)
  - Próbkowanie sieci i techniki uniknięcia wykrycia (258)
  - Omiatanie sieci (network sweeps) (259)
  - Informacje trasowania sieci (260)
  - Zbieranie informacji o konkretnych systemach (260)
- Określenie słabych punktów i wybór celów (265)
- Zdobycie kontroli nad systemem (267)
  - ./0wnit (267)
  - Zgadywanie haseł (268)

    - Wykorzystanie specjalnie stworzonych wirusów i koni trojańskich (268)
    - Sięgamy głębiej (269)
    - Podsłuchiwanie ruchu (269)
    - Wykorzystanie relacji zaufania (269)
- Podsumowanie (270)

Rozdział 9. W obronie twojej infrastruktury (271)

- Co powinna robić zapora sieciowa? (272)
- Funkcje zapory sieciowej (273)
- Pomocnicze funkcje zapory sieciowej (274)
- Podstawowe typy zapór sieciowych (276)
    - Zapora filtrująca pakiety (276)
    - Zapora sieciowa z inspekcją stanów (279)
    - Pośredniczące zapory aplikacyjne (282)
    - Hybrydy (284)
    - "Szczelina powietrzna" (285)
- Drugorzędne funkcje zapory sieciowej (286)
    - Translacja adresów (286)
    - Antispoofing (290)
    - Korzystanie z wirtualnych sieci LAN (VLAN) (292)
    - Funkcje VPN (293)
    - Funkcje zarządzania (295)
    - Uwierzytelnianie (295)
    - Dyspozycyjność (HA - High Availability) (297)
    - Platformy zapór sieciowych (299)
    - Integracja funkcji (303)
    - Narzędzia ochrony przed DoS (305)
    - Wydajność i efektywność pracy (306)
- Implementacja i wskazówki (308)
    - Architektura zapory sieciowej (308)
    - Wykrywanie włamań (309)
    - Zagadnienia związane z translacją adresów (309)
    - Złożone zestawy reguł (311)
    - Rejestracja danych dziennika zdarzeń, monitorowanie i audyt (311)
- Słabości zapór sieciowych (313)
    - Ukryte kanały (313)
    - Błędy i wady zapór sieciowych (314)
- Podsumowanie (314)

Rozdział 10. Obserwacja sieci - systemy wykrywania włamań (317)

- Co to jest IDS? (317)
- W jaki sposób wykorzystuje się systemy IDS w ośrodkach internetowych? (318)
    - Różne typy systemów IDS (319)
    - Możliwości IDS (322)
- Testy protokołów TCP/IP (326)
- NetBIOS w TCP/IP (NBT) (327)
- Inne protokoły sieciowe (328)
- Ethernet i inne nagłówki w warstwie danych (328)

    - Protokoły warstwy aplikacyjnej (330)
    - Dane aplikacji (332)
    - Integralność pliku (332)
    - Przetwarzanie danych z dzienników zdarzeń systemowych (334)
- Obrona przed systemami IDS (335)
    - Złożoność analizy (335)
    - Fragmentacja IP i segmentacja TCP (336)
    - Uniknięcie wykrycia przez IDS dzięki kodowaniu w warstwie aplikacji (339)
    - Inne techniki unikania wykrycia przez IDS (341)
    - Atak typu DoS na system IDS (342)
- Praktyczne zagadnienia związane z implementacją systemów IDS (343)
    - Sieci przełączane (344)
    - Szyfrowanie (345)
- Dostrajanie czujników IDS (347)
- Zarządzanie systemem IDS (351)
    - Odpowiedzialność za bezpieczeństwo (351)
- Personel (352)
    - Prywatność (353)
- Reakcja na incydent i odzyskiwanie (354)
    - Stopień zagrożenia powodowanego przez zdarzenia raportowane przez IDS (354)
    - Reakcja automatyczna (355)
    - Odpowiedź operatorów grupy reagowania (356)
    - Reakcja na prawdziwe incydenty (356)
    - Kontratak - nie ma mowy! (357)
- IDS - na własną rękę czy stałe podwykonawstwo? (358)
- Podsumowanie (359)

Rozdział 11. Reakcja na incydent i zagadnienia prawne (361)

- Co oznacza termin "reakcja na incydent"? (361)
- Przygotowanie na incydent (362)
    - Zachowywanie dzienników zdarzeń (363)
    - Zachowywanie kont użytkowników (364)
    - Określanie czasu zdarzenia (364)
    - Tworzenie banerów (364)
    - Tworzenie sum kontrolnych (365)
- Reakcja na incydent w czasie rzeczywistym (365)
    - Polityka reakcji (365)
    - Procedury reagowania (366)
    - Rola i zakres odpowiedzialności jednostek wewnątrz organizacji (366)
    - Szkolenie (367)
    - Wyciąganie wniosków (367)
- Co oznacza termin "przestępstwo elektroniczne"? (368)
    - Dopuszczalność dowodów cyfrowych (369)
    - Łańcuch dowodowy i dokumentacja (369)
    - Dlaczego ważne jest korzystanie z licencjonowanego oprogramowania? (371)
    - Wiarygodność osoby prowadzącej dochodzenie (372)
    - Zagadnienia odpowiedzialności prawnej i prawa do prywatności (372)
- Techniki dochodzeniowe (373)

    - Zabezpieczenie miejsca przestępstwa (373)
    - Wyłączanie urządzeń (374)
    - Kopiowanie dysków twardych i dyskietek (374)
    - Przeszukiwanie dysków twardych (375)
    - Prowadzenie audytu systemu (378)
    - Śledzenie intruza (383)
- Analiza przypadków (386)
    - Hakowanie witryny sieciowej (386)
    - Niestabilni pracownicy IT (387)
    - Nadużycie zasobów przedsiębiorstwa (388)
    - Kilka słów na temat anonimowych publikacji (389)
- Współpraca z wymiarem sprawiedliwości (390)
- Podsumowanie (391)
- Bibliografia (392)

Rozdział 12. Tworzenie bezpiecznych aplikacji sieciowych (393)

- Najpowszechniejsze źródła błędów programistycznych (394)
- Metaznaki (395)
    - Niebezpieczeństwo związane z metaznakami (396)
    - Bezpieczna praca z metaznakami (397)
- Wykorzystanie kodu wykonawczego (400)
    - Przepełnienie bufora (401)
    - Przykład: funkcje łańcuchów w C (403)
    - Jak hakerzy wykorzystują przepełnienie bufora (404)
    - Błędy formatowania łańcucha (405)
    - Kilka ostatnich uwag odnośnie do nadużyć kodu wykonawczego (406)
- Bezpieczeństwo na poziomie aplikacji (407)
    - Pliki cookies (407)
    - Adresy IP źródła (408)
    - Efektywne zarządzanie sesją (409)
    - Replay Attacks i bezpieczeństwo sesji (410)
    - Sprawdzanie tożsamości użytkowników aplikacji (411)
    - Przykład: kontrola dostępu dla systemu z sygnalizacją błędów (412)
- Standardy kodowania i przegląd kodu programistycznego (414)
- Podsumowanie (415)

Skorowidz (417)