

Wstęp (5)

- Dla kogo jest ta książka? (6)
- Układ książki (7)
- Konwencje i oznaczenia (8)

Rozdział 1. Typowe zagrożenia (9)

- Wirusy (10)
- Niechciane programy (22)
- Zgadywanie haseł (28)
- Ataki lokalne (30)
- Socjotechnika (32)
- Lista kontrolna (34)

Rozdział 2. Aktualizacje zabezpieczeń (35)

- Aktualizacja oprogramowania (36)
- Ocena bezpieczeństwa komputera (43)
- Usługa SUS (48)
- Lista kontrolna (56)

Rozdział 3. Bezpieczeństwo systemu operacyjnego (57)

- Konta użytkowników (58)
- Pliki i foldery (65)
- Szablony zabezpieczeń (70)
- Szablony administracyjne (77)
- Ocena bezpieczeństwa systemu (79)
- Lista kontrolna (83)

Rozdział 4. Bezpieczeństwo programów (85)

- Aplikacje internetowe (85)
 - o Internet Explorer (85)
 - o Outlook Express (91)
 - o Komunikatory (96)
 - o Serwer IIS (97)
- Zasady ograniczeń oprogramowania (101)
- Lista kontrolna (106)

Rozdział 5. Bezpieczeństwo danych (109)

- Kontrola dostępu (109)
- Szyfrowanie (115)
 - o Algorytmy symetryczne (115)
 - o Algorytmy asymetryczne (115)
 - o Algorytmy tajne (116)
 - o Algorytmy jawne (116)
 - o Klucze (116)

- o Certyfikaty (117)
 - o EFS (120)
 - o PGPDisk (125)
- Lista kontrolna (127)

Rozdział 6. Bezpieczeństwo sieci (129)

- Linia graniczna (130)
- Komputery (133)
- Sieć lokalna (139)
- Internet (145)
- Sieć bezprzewodowa (146)
- Lista kontrolna (147)

Rozdział 7. Przywracanie komputera do stanu sprzed ataku (149)

- Tworzenie kopii zapasowych (149)
- Odtwarzanie kopii zapasowych (157)
- Lista kontrolna (161)

Dodatek A Windows XP SP2 (163)

Dodatek B Skuteczność strategii wielu warstw (181)

- Przykłady obrony przed znanymi atakami (182)
 - o Code Red (182)
 - o Nimda (183)
 - o Mydoom (185)
 - o Sasser (186)

Posłowie (187)

Skorowidz (189)