

Spis treści

Podziękowania.....	9
Wprowadzenie.....	11
Dla kogo jest ta książka?	12
Zawartość książki.....	12
Wskazówki ułatwiające efektywną lekturę.....	13
Rozdział 1. Podstawowe informacje o bezpieczeństwie.....	15
Dlaczego komputery nie są bezpieczne?.....	15
Historia bezpieczeństwa komputerów.....	20
Do roku 1945.....	21
1945 – 1955.....	22
1955 – 1965.....	23
1965 – 1975.....	23
1975 – 1985.....	24
1985 – 1995.....	26
1995 – 2005.....	28
Po roku 2005.....	30
Pojęcia związane z bezpieczeństwem	31
Zaufanie.....	31
Uwierzytelnianie.....	31
Ciąg upoważnień	33
Rozliczanie kont	33
Kontrola dostępu	34
Ważne pojęcia	36
Pytania kontrolne	36
Rozdział 2. Hakerstwo	39
Na czym polega hakerstwo	39
Typy hakerów.....	40
Specjaliści ds. bezpieczeństwa	40
Skrypciaki.....	41
Dorośle osoby zatrudnione poniżej swoich kwalifikacji.....	42
Hakerzy ideologiczni.....	42
Kryminaliści	43
Szpierzy przemysłowi.....	44
Sfrustrowani pracownicy.....	44

Drogi, którymi chadzają hakerzy	45
Ataki bezpośrednie	45
Połączenia modemowe	46
Internet	47
Sieci bezprzewodowe	47
Techniki hakerów	48
Wybór celu	48
Zbieranie informacji	51
Ataki	53
Ważne pojęcia	61
Pytania kontrolne	61
Rozdział 3. Szyfrowanie i uwierzytelnianie	63
Szyfrowanie	63
Szyfrowanie z tajnym kluczem	66
Funkcje jednokierunkowe (skróty)	66
Szyfrowanie z kluczem publicznym	68
Kryptosystemy hybrydowe	70
Uwierzytelnianie	71
Uwierzytelnianie za pomocą haseł	71
Uwierzytelnianie na bazie sesji	74
Uwierzytelnianie z kluczem publicznym	76
Uwierzytelnianie na bazie certyfikatów	77
Uwierzytelnianie biometryczne	78
Ważne pojęcia	80
Pytanie kontrolne	80
Rozdział 4. Zarządzanie bezpieczeństwem	83
Tworzenie regulaminu bezpieczeństwa	83
Szkielet regulaminu	84
Regulamin bezpieczeństwa w praktyce	89
Implementacja regulaminu bezpieczeństwa	96
Automatyzacja reguł	97
Ludzie a zabezpieczenia	98
Aktualizacje regulaminu bezpieczeństwa	101
Cykl działań ochronnych	101
Ważne pojęcia	102
Pytania kontrolne	103
Rozdział 5. Bezpieczeństwo granicy	105
Podstawy bezpieczeństwa granicy	105
Działanie ścian ogniowych	108
Najważniejsze funkcje ścian ogniowych	109
Usługi poufności ścian ogniowych	118
Wirtualne sieci prywatne	119
Inne usługi graniczne	120
Wybór ściany ogniowej	121

Ważne pojęcia	123
Pytania kontrolne	123
Rozdział 6. Wirtualne sieci prywatne.....	125
Funkcjonowanie wirtualnych sieci prywatnych.....	125
Enkapsulacja IP	126
Uwierzytelnianie kryptograficzne	128
Szyfrowanie ładunku danych	128
Cechy charakterystyczne sieci VPN	128
Popularne implementacje sieci VPN.....	130
IPSec.....	131
L2TP	133
PPTP	135
PPP/SSL lub PPP/SSH	136
Sieci VPN w praktyce	138
Ważne pojęcia	141
Pytania kontrolne	141
Rozdział 7. Zabezpieczanie użytkowników zdalnych i domowych	143
Problemy ze zdalnym bezpieczeństwem.....	144
Luki w zabezpieczeniach wirtualnych sieci prywatnych	144
Laptopy.....	144
Zabezpieczanie zdalnych maszyn	145
Połączenia VPN.....	147
Ochrona danych i niezawodność	149
Kopie zapasowe i archiwizacja	150
Ochrona przed zdalnymi użytkownikami	151
Ważne pojęcia	152
Pytania kontrolne	152
Rozdział 8. Ochrona przed szkodliwym oprogramowaniem i wirusami	155
Czym jest malware	155
Wirusy	157
Ochrona przed wirusami	163
Zapobieganie	163
Naturalna odporność.....	164
Aktywna ochrona.....	165
Robaki i konie trojańskie	166
Ochrona przed robakami	168
Implementowanie zabezpieczeń antywirusowych	168
Zabezpieczanie klientów	169
Zabezpieczanie serwerów.....	171
Zabezpieczanie bramy pocztowej.....	171
Zabezpieczenia na bazie ścian ogniowych	172
Antywirusowa ochrona przedsiębiorstwa.....	172
Ważne pojęcia	173
Pytania kontrolne	173

Rozdział 9. Tworzenie odporności na błędy	175
Przyczyny utraty danych	176
Błędy użytkowników	176
Częste awarie	177
Przestępstwa	179
Zdarzenia losowe	182
Środki odporności na błędy	183
Kopie zapasowe	184
Zasilacze awaryjne (UPS) i generatory prądu	189
Tablice RAID	190
Uprawnienia	193
Zabezpieczenia granicy	193
Audyt	193
Składowanie danych poza siedzibą przedsiębiorstwa	193
Archiwizacja	194
Testowanie systemów	195
Nadmiarowe łącza	196
Zabezpieczenia fizyczne	196
Serwery pracujące w klastrach	197
Ważne pojęcia	201
Pytania kontrolne	201
Rozdział 10. Bezpieczeństwo systemu Windows	203
Lokalne bezpieczeństwo Windows	203
Identyfikatory bezpieczeństwa	206
Logowanie	207
Dostęp do zasobów	209
Obiekty i uprawnienia	211
Uprawnienia w systemie plików NTFS	215
Encrypting File System (EFS)	217
Bezpieczeństwo sieci Windows	217
Active Directory	218
Uwierzytelnianie Kerberos i bezpieczeństwo domeny	219
Reguły grupy	222
Bezpieczeństwo udziałów	226
IPSec	230
Ważne pojęcia	232
Pytania kontrolne	232
Rozdział 11. Bezpieczeństwo serwerów uniksowych	235
Krótka historia Uniksa	235
Podstawowe informacje o bezpieczeństwie Uniksa	240
Uniksowe systemy plików	240
Konta użytkowników	245
Zabezpieczenia systemu plików	250
Listy kontroli dostępu	252

Uprawnienia wykonywania	252
Ważne pojęcia	256
Pytania kontrolne	256
Rozdział 12. Bezpieczeństwo sieci uniksowej	259
Podstawowe informacje o bezpieczeństwie sieci uniksowej	259
Bezpieczeństwo zdalnego logowania	261
Zdalny dostęp	263
PAM (Pluggable Authentication Module)	265
Rozproszone logowanie	266
Rozproszone pliki <i>passwd</i>	267
NIS i NIS+	267
Kerberos	269
Zabezpieczenia udostępniania plików	272
File Transfer Protocol (FTP)	273
Network File System (NFS)	276
HTTP (Hypertext Transfer Protocol)	277
Samba	279
Zabezpieczanie komputerów uniksowych ścianami ogniowymi	281
IPTables i IPChains	281
TCP Wrappers	283
Firewall Toolkit (FWTK)	284
Ważne pojęcia	285
Pytania kontrolne	285
Rozdział 13. Bezpieczeństwo serwera WWW	287
Problemy z bezpieczeństwem usługi WWW	287
Implementowanie bezpieczeństwa serwera WWW	288
Popularne rozwiązania	290
Bezpieczeństwo serwera Apache	303
Bezpieczeństwo serwera IIS	307
Ważne pojęcia	314
Pytania kontrolne	315
Rozdział 14. Bezpieczeństwo poczty elektronicznej	317
Szyfrowanie i uwierzytelnianie maili	317
S/MIME	319
PGP	320
Fałszowanie wiadomości pocztowych	321
Wirusy pocztowe	322
Wirusy programu Outlook	323
Komercyjne bramowe skanery antywirusowe	324
AMaVIS	325
Ochrona przed groźnymi załącznikami	326
Usuwanie wszystkich załączników	327
Zezwalanie tylko na określone załączniki	328
Usuwanie tylko niebezpiecznych załączników	329

Obce serwery pocztowe.....	332
Spam.....	333
Uwierzytelnianie SMTP	335
Systematyczna walka ze spamem.....	338
Ważne pojęcia	342
Pytanie kontrolne	343
Rozdział 15. Wykrywanie włamań	345
Systemy wykrywania włamań.....	345
Inspektory	347
Przynęty	348
Audyty	350
Dostępne systemy IDS	351
System Windows	351
Tripwire	352
Snort	353
Demarc PureSecure	354
Wykrywacz włamań do sieci NFR	355
Ważne pojęcia	356
Pytania kontrolne	356
Dodatek A. Odpowiedzi na pytania kontrolne	357
Rozdział 1.....	357
Rozdział 2.....	358
Rozdział 3.....	360
Rozdział 4.....	361
Rozdział 5.....	362
Rozdział 6.....	363
Rozdział 7.....	364
Rozdział 8.....	365
Rozdział 9.....	366
Rozdział 10.....	368
Rozdział 11.....	369
Rozdział 12.....	370
Rozdział 13.....	372
Rozdział 14.....	373
Rozdział 15.....	374
Słownik.....	377
Skorowidz	399