

Sadržaj

Uvod	xix
1. Opšti pojmovi sistema zaštite	1
2. Procena rizika	47
3. Infrastruktura i povezivanje	95
4. Praćenje saobraćaja na mreži	153
5. Implementacija i održavanje zaštićene mreže	195
6. Zaštita mreže i radnog okruženja	235
7. Osnovi kriptografije i njeni metodi	281
8. Kriptografski standardi	321
9. Pravilnici i procedure sistema zaštite	355
10. Upravljanje poslovima zaštite	403
Rečnik	437
Indeks	475

1. Opšti pojmovi sistema zaštite 1

Šta predstavlja zaštita podataka?	3
Zaštita fizičkog okruženja	5
Operativne mere zaštite	6
Upravljanje i politika	8
Osnovni ciljevi sistema za zaštitu podataka	11
Kako funkcionišu zaštitni procesi?	12
Antivirusni programi	12
Implementacija kontrole pristupa	12
Kako funkcioniše identifikacija?	14
Kako funkcionišu mrežni servisi i protokoli?	20
Topologije zaštite	22
Definisanje zahteva u pogledu dizajna	22
Kreiranje zaštitnih zona	24
Rad sa novim tehnologijama	29
Poslovna politika u svetlu sistema zaštite	32
Zaključak	36
Teze za ispit	38
Kontrolna pitanja	40
Odgovori	44

2. Procena rizika 47

Procena strategija napada	48
Oblici napada radi neovlašćenog pristupa	49
Napadi radi izmene podataka i napadi poricanja	50
Napadi radi "gušenja" servisa i distribuirano	51
"gušenje" servisa	51
Kako prepoznati uobičajene napade?	53
Napad tipa back door	53
Napad sa lažnim predstavljanjem (spoofing napad)	54
Napad tipa man-in-the-middle	55
Replay napad	56
Napadi sa pogađanjem lozinki	57
TCP/IP protokol i problemi zaštite	58
Rad sa TCP/IP grupom protokola	59
Enkapsulacija	62
Rad sa protokolima i servisima	63
Otkrivanje TCP/IP napada	66
Kako funkcionišu napadi na aplikacije i servise	72
višeg nivoa (software exploitation)?	73
Kako "preživeti" zlonamerni kod?	73
Virusi	74
"Trojanski konji"	80
Logičke "bombe"	80

"Crvi"	80
Antivirusni programi	81
Kako funkcionise napad zasnovan na ljudskom kontaktu?	82
Uvod u nadzor procesa i datoteka	84
Zaključak	84
Teze za ispit	86
Kontrolna pitanja	88
Odgovori	92

3. Infrastruktura i povezivanje 95

Šta predstavlja zaštita infrastrukture	97
Rad sa hardverskim komponentama	98
Rad sa softverskim komponentama	99
Kako funkcionišu uređaji koji sačinjavaju mrežnu infrastrukturu?	100
Mrežne barijere	100
Čvorišta	104
Ruteri	105
Komutatori	107
Bežične pristupne tačke	108
Modemi	109
Servisi daljinskog pristupa	110
Telekom/PBX sistemi	110
Virtuelne privatne mreže	112
Praćenje saobraćaja na mreži i dijagnostika	114
Monitori mrežnog saobraćaja	114
Zaštita radnih stanica i servera	115
Kako funkcionišu mobilni uređaji?	117
Kako funkcionise udaljeni pristup?	118
Rad sa Serial Line Internet Protocolom	119
Rad sa Point-to-Point protokolom	119
Protokoli za tunelovanje	120
Bežični protokoli serije 802.1x	121
RADIUS	121
TACACS/+	122
Zaštita internet veza	122
Rad sa portovima i utičnicama	123
Kako funkcionise elektronska pošta?	124
Rad sa Webom	124
Rad sa File Transfer Protokolom	129
Kako funkcionišu SNMP i ostali TCP/IP protokoli?	130
Osnovni pojmovi o kabliranju, kablovima i vezi	132
Koaksijalni kabl	132
Neoklopljene i oklopljene upredene parice	135

Optički kablovi	137
Prenos u infracrvenom spektru	138
Radio frekvencije	138
Mikrotalasni sistemi	139
Upotreba izmenljivih medijuma	140
Magnetna traka	141
CD-R	142
Hard diskovi	142
Diskete	142
Fleš kartice	143
Smart kartice	143
Zaključak	144
Teze za ispit	145
Kontrolna pitanja	147
Odgovori	151

4. Praćenje saobraćaja na mreži 153

Praćenje rada mreže	155
Kako prepoznati različite vrste mrežnog saobraćaja?	156
TCP/IP	156
Praćenje rada mrežnih sistema	161
Kako funkcionišu sistemi za detekciju upada?	162
Rad sa IDS sistemom zasnovanim na mreži	165
Rad sa IDS sistemom zasnovanim na hostu	170
Primena lažnih "mamaca"	171
Reagovanje na incidente	172
Rad sa bežičnim sistemima	177
Wireless Transport Layer Security	177
IEEE 802.11x bežični protokoli	178
WEP/WAP	179
"Ranjiva" mesta bežičnih sistema koja morate poznavati	180
Kako funkcionišu instant poruke?	180
Osetljivost IM sistema	181
Kontrola privatnosti	181
Rad sa 8.3 standardom za nazive datoteka	182
Kako funkcionišu "prisluškivanje" paketa?	183
Kako funkcionišu elektronsko izviđanje?	184
Uzimanje "otisaka prstiju"	184
Skeniranje	185
Zaključak	185
Teze za ispit	186
Kontrolna pitanja	188
Odgovori	192

5. Implementacija i održavanje zaštićene mreže 195

Pretnje koje ugrožavaju mrežu	197
Propisivanje mera zaštite	199
Ojačanje OS-a i NOS-a	201
Konfiguracija mrežnih protokola	201
Microsoft Windows 9x	204
Ojačanje Microsoft Windowsa NT 4	204
Ojačanje Microsoft Windowsa 2000	205
Ojačanje Microsoft Windowsa XP	207
Ojačanje Windows 2003 Servera	208
Ojačanje Unix/Linux sistema	208
Ojačanje Novell NetWare operativnog sistema	209
Ojačanje Apple Macintosh sistema	211
Ojačanje datotečnih sistema	211
Ažuriranje operativnih sistema	213
Poboljšanje zaštite hard diskova	215
Ažuriranje mrežnih uređaja	215
Konfiguracija rutera i mrežnih barijera	216
Poboljšanje zaštite aplikacija	217
Poboljšanje zaštite web servera	217
Poboljšanje zaštite na e-mail serveru	218
Poboljšanje zaštite FTP servera	218
Poboljšanje zaštite DNS servera	219
Poboljšanje zaštite NNTP servera	220
Poboljšanje zaštite datotečnih servera i servera štampe	221
i njihovih servisa	
Poboljšanje zaštite DHCP servera	222
Rad sa skladištima podataka	222
Zaključak	226
Teze za ispit	228
Kontrolna pitanja	229
Odgovori	233

6. Zaštita mreže i radnog okruženja 235

Fizičke mere zaštite i bezbednost mreže	236
Kontrola pristupa	236
Kako funkcionišu socijalni napadi?	243
Procena šireg okruženja	245
Šta su planovi za hitne slučajeve?	253
Procena ključnih sistema u organizaciji	253
Procena rizika	255
Definisanje politike, standarda i uputstava	257
Definisanje politike	257
Definisanje standarda	258

Definisanje uputstava	259
Standardi u oblasti zaštite i ISO 17799	260
Određivanje stepena tajnosti podataka	261
Podaci javnog karaktera	262
Privatni podaci	263
Uloge u sistemu zaštite	265
Kontrola pristupa podacima	266
Zaključak	270
Teze za ispit	272
Kontrolna pitanja	274
Odgovori	278

7. Osnovi kriptografije i njeni metodi 281

Kratak uvod u kriptografiju	282
Kako funkcioniše fizička kriptografija?	282
Kako funkcioniše matematička kriptografija?	285
Kako funkcioniše kvantna kriptografija?	287
Razbijanje mita o neprobojnim šiframa	289
Kako funkcionišu kriptografski algoritmi?	291
Teorijske osnove heš funkcije	291
Rad sa simetričnim algoritmima	292
Rad sa asimetričnim algoritmima	294
Rad sa kriptografskim sistemima	295
Poverljivost	295
Integritet	296
Identifikacija	297
Neporičljivost	299
Kontrola pristupa	299
Rad sa sistemom Public Key Infrastructure	300
Institucije za izdavanje sertifikata	301
Rad sa registracionim institucijama (RA) i	302
lokalnim registracionim institucijama (LRA)	
Primena sertifikata	304
Poništavanje sertifikata	305
Povezivanje CA servera	306
Priprema kriptografskog napada	311
Zaključak	312
Teze za ispit	313
Kontrolna pitanja	315
Odgovori	319

8. Kriptografski standardi 321

Šta su kriptografski standardi i protokoli?	322
Poreklo kriptografskih standarda	323

PKIX/PKCS	326
X.509	327
SSL i TLS	328
CMP	330
S/MIME	330
SET	330
SSH	331
PGP	332
HTTPS	333
S-HTTP	334
IPSec	334
FIPS	335
Common Criteria	335
WLTS	335
WEP	335
ISO 17799	335
Kontrola ključeva i "životni ciklus" ključa	336
Poređenje centralizovanog i decentralizovanog	337
generisanja ključeva	339
Skladištenje i distribucija ključeva	339
Deponovanje ključeva	341
Prestanak važnosti ključa	341
Povlačenje ključa	341
Suspenzija ključeva	342
Obnavljanje i ahriviranje ključeva	342
Produženje važnosti ključeva	344
Uništavanje ključeva	344
Zaključak	345
Ispitne teze	347
Kontrolna pitanja	349
Odgovori	353

9. Pravilnici i procedure sistema zaštite 355

Neprekidnost poslovnog procesa	357
Komunalne usluge	357
Visoka dostupnost	359
Otklanjanje posledica	363
Obezbeđenje podrške dobavljača	376
Ugovor o dostupnosti servisa	376
Deponovanje izvornog koda	378
Izrada pravilnika i definisanje procedura	379
Pravilnik o ljudskim resursima	379
Poslovni pravilnik	382
Pravilnik o sertifikatima	384
Uputstvo o postupcima u slučaju incidenata	385

Kontrola privilegija	386
Upravljanje korisnicima i grupama	386
Proširenje ovlašćenja	388
Jedinstvena prijava na sistem	388
Donošenje odluka o dodeli privilegija	389
Kontrola	390
Kontrola pristupa	392
Zaključak	393
Ispitne teze	394
Kontrolna pitanja	396
Odgovori	400

10. Upravljanje poslovima zaštite 403

Računarska forenzika	404
Metodologija forenzične istrage	405
Evidencija prikupljenih dokaza	406
Obezbeđenje dokaza	408
Prikupljanje dokaza	408
Upravljanje poslovima zaštite	409
Formulisanje predloga i dokumentacije	410
Nivo svesti o sistemu zaštite i osposobljenost	416
Komunikacija i svest	416
Obuka	417
Održavanje visokog nivoa zaštite	419
Web lokacije	421
Časopisi	422
Normativno regulisanje tajnosti i zaštite	423
Health Insurance Portability and Accountability Act	423
Gramm-Leach Bliley Act iz 1999. godine	424
Computer Fraud and Abuse Act	424
Family Educational Rights and Privacy Act	425
Computer Security Act iz 1987. godine	425
Cyberspace Electronic Security Act	425
Cyber Security Enhancement Act	426
Patriot Act	426
Upoznajte međunarodne inicijative	426
Zaključak	427
Ispitne teze	428
Kontrolna pitanja	430
Odgovori	434

Rečnik 437

Indeks 475