Indice generale

L'autore ..... **xi**

Introduzione ..... **xiii**

A chi è rivolto questo libro xiii
Struttura del libro xiii
Convenzioni utilizzate xiv
Nota all'edizione italiana xv

Capitolo 1 Gli aspetti fondamentali della sicurezza **1**

La triade CIA 2
Identificazione dei controlli di sicurezza 3
Controlli amministrativi 3
Controlli tecnici 4
Controlli fisici 4
Controlli preventivi 6
Controlli deterrenti 6
Controlli successivi o investigativi (detective) 7
Controlli correttivi 7
Controlli compensativi 7
Controlli degli accessi 8
Hashing e integrità dei dati 12
Hashing in pratica 13
Modello di difesa in profondità (Defense in Depth) 14
Domande di ripasso 16
Risposte e spiegazioni 16

Capitolo 2 Conduzione di un'analisi dei rischi **19**

Gestione del rischio 20
Importanza di norme, piani e procedure 20
Procedure operative standard 20

Gestione del personale: norme e procedure 22
Role-based awareness training....23
Norme generali di sicurezza....23
Analisi dell'impatto di business....24
Valutazione di soglia della privacy/di impatto sulla privacy 25
Funzioni mission-essential/identificazione dei sistemi critici....25
Valutazione del rischio della supply chain....25
Concetti dell'analisi di impatto di business....26
Procedure e concetti per i rischi....27
Valutazione delle minacce....28
Attori delle minacce....28
Trattamento del rischio....29
Registro dei rischi....30
Analisi del rischio qualitativa/quantitativa....30
Domande di ripasso....31
Risposte e spiegazioni....31

Capitolo 3 Implementazione di policy e procedure di sicurezza....35

Framework e architettura di riferimento standard di settore....36
Il modello di riferimento OSI....36
Modello TCP/IP....37
Tipi di framework....37
Benchmark/guide per la configurazione sicura....38
Policy e guide per gli utenti....38
Guide di configurazione per la sicurezza – server web....40
Guide utente per dispositivi di infrastruttura di rete....40
Implementazione di pratiche per la sicurezza e la privacy dei dati ..41
Distruzione dei dati e dei supporti....42
Sensibilità dei dati: etichettatura e gestione....43
Conservazione dei dati: blocco legale e compliance....44
Ruoli per i dati....44
Attività pratica: creazione di una linea di base....44
Domande di ripasso....49
Risposte e spiegazioni....50

Capitolo 4 Identità e gestione degli accessi....53

Concetti fondamentali di gestione dell'identità e degli accessi....54
Password....54
Password di default/di amministratore....54
Password: policy di gruppo....54
Recupero della password....57
Fattori di autenticazione....57
Fiducia transitiva....58
Servizi di federazione....59

Shibboleth 61
Single sign-on (SSO) 61
Installazione e configurazione di servizi di identità e accesso 61
LDAP 61
Kerberos 63
Server AAA (autenticazione, autorizzazione e accounting) 65
Controlli di gestione dell'identità e dell'accesso 66
Biometria 67
Token e dispositivi di sicurezza 69
Autenticazione basata su certificazione 69
Pratiche comuni di gestione degli account 70
Tipi di account 70
Creazione di un account 72
Dipendenti che cambiano reparto 72
Ricertificazione degli account 73
Manutenzione degli account 73
Monitoraggio degli account 73
Security Information and Event Management 74
Controllo degli accessi basato sui gruppi 76
Gestione delle credenziali 76
Esercizio pratico: policy per le password 77
Domande di ripasso 77
Risposte e spiegazioni 79

Capitolo 5 Componenti delle reti 83

Modello di riferimento OSI 84
Installazione e configurazione di componenti di rete 86
Firewall 86
Router 88
Switch 90
Server proxy 92
Reverse proxy 93
Accesso remoto 93
VPN con L2TP/IPSec 94
IPSec 95
Concentratore VPN 96
VPN site-to-site 96
VPN always on o on-demand 96
SSL VPN 97
Split tunneling 97
Bilanciatore del carico 97
Clustering 99
Data-Loss Prevention 100
Informazioni di sicurezza e gestione degli eventi 100
Mail gateway 101
Email cloud-based 101

Media gateway....101
Hardware Security Module....101
Rete definita da software....101
Concetti di architettura di rete sicura....101
Network Address Translation (NAT)....102
Port Address Translation (PAT)....103
Network Access Control (NAC)....103
Honeypot....104
Acceleratori Secure Socket Layer....105
Decifratore SSL/TLS....105
Sensore/collettore....105
Tap/port mirror....105
Mitigatore DDoS....105
Segregazione/segmentazione/isolamento....106
Collocazione dei dispositivi e della tecnologia di sicurezza....107
Switch di aggregazione....108
Implementazione di segregazione/segmentazione/isolamento di protocolli sicuri....109
Caso d'uso (use case)....111
Implementazione di sicurezza per il wireless....122
Controller Wireless Access Point (WAP)....123
Rendere sicuro l'accesso al WAP....123
Ampiezza di banda wireless/selezione di banda....124
Canali wireless....125
Tipi di antenna wireless e intensità del segnale....125
Copertura wireless....126
Crittografia per il wireless....126
Open System Authentication....127
WPS....127
Captive portal....127
Attacchi wireless....127
Protocolli di autenticazione wireless....127
Domande di ripasso....128
Risposte e spiegazioni....131

Capitolo 6 Modelli cloud e virtualizzazione....135

Cloud computing....136
Implementazione di modelli di cloud deployment diversi....138
Modelli di servizio cloud....140
Resilienza e ridondanza dei dischi....143
Redundant Array of Independent Disks....143
Storage Area Network....146
Concetti di cloud storage....147
Reti virtuali....148
Virtual Desktop Infrastructure....150

VDE....151
HVAC: riscaldamento, ventilazione, condizionamento....151
Ambienti di rete....152
On-premises....152
Servizi hosted....152
Servizi di hosting nel cloud....152
Esercizio pratico: il cloud conviene?....152
Domande di ripasso....153
Risposte e spiegazioni....154

Capitolo 7 Gestione di host e deployment di applicazioni....157

Deployment sicuro di dispositivi mobili....158
Bring Your Own Device (BYOD)....158
Choose Your Own Device....159
Corporate-Owned Personally-Enabled....159
Virtual Desktop Infrastructure....160
Metodi di connessione per dispositivi mobili....160
Concetti della gestione dei dispositivi mobili....162
Accesso al dispositivo....162
Gestione dei dispositivi....163
Protezione dei dispositivi....163
Dati dei dispositivi....163
Messa in atto e monitoraggio di sicurezza per dispositivi mobili....164
Sistema di controllo industriale....166
Supervisory Control and Data Acquisition....166
Dispositivi mobili: problemi di sicurezza dei sistemi embedded....167
Dispositivi speciali....169
Sviluppo e deployment di applicazioni in modo sicuro....170
Modelli del ciclo di vita dello sviluppo: a cascata e Agile....170
Modello a cascata (waterfall)....170
Agile....171
Agile o cascata?....172
DevOps....172
Secure DevOps....172
Tecniche di codifica sicura....172
Qualità e testing del codice....175
Esecuzione e validazione lato server o lato client....176
Domande di ripasso....176
Risposte e spiegazioni....178

Capitolo 8 Protezione contro attacchi e vulnerabilità....181

Attacchi da parte di virus e malware....182
Attacchi di ingegneria sociale....184
Attacchi comuni....187
Attacchi ad applicazioni/servizi....188

Attacchi via programmazione 192
Esempio 1: JavaScript, creazione di una variabile money 193
Esempio 2: JavaScript, impostazione del giorno del mese 193
Attacchi di tipo "hijacking" 195
Manipolazione di driver 196
Attacchi crittografici 196
Attacchi alle password 197
Attacchi wireless 199
Penetration testing 201
Tecniche di penetration testing 201
Concetti della scansione di vulnerabilità 202
Scansioni con o senza credenziali 203
Penetration testing e scansione di vulnerabilità 203
Esercizio pratico: scanner di vulnerabilità con credenziali 203
Domande di ripasso 208
Risposte e spiegazioni 210

Capitolo 9 Implementazione dell'infrastruttura a chiave pubblica 213

Concetti della PKI 214
Gerarchia dei certificati 214
Certificate trust 216
Validità dei certificati 217
Gestione dei certificati 218
Tipi di certificati 219
Cifratura simmetrica e asimmetrica 221
Che cos'è la cifratura 221
Firme digitali 223
Algoritmi crittografici e loro caratteristiche 224
Algoritmi simmetrici 225
Algoritmi asimmetrici 225
Cifratura XOR 226
Algoritmi di key stretching 227
Modalità di cifratura 227
Hashing e integrità dei dati 228
Confronto fra i concetti fondamentali della crittografia 229
Crittografia asimmetrica: PKI 229
Algoritmi simmetrici: modalità di funzionamento 230
Algoritmi di hashing 231
Crypto service provider 231
Crypto module 231
Protezione dei dati 231
Terminologia crittografica di base 232
Offuscamento 232
Generatore di numeri pseudo-casuali 232
Nonce 232

Perfect forward secrecy 232
Security through obscurity 232
Collisione 233
Steganografia 233
Diffusione 233
Decisioni di implementazione 233
Casi d'uso comuni per la crittografia 233
Supporto della confidenzialità 233
Supporto dell'integrità 234
Supporto della non ripudiabilità 234
Supporto dell'offuscamento 234
Dispositivi a bassa potenza 234
Latenza ridotta 235
Resilienza elevata 235
Supporto dell'autenticazione 235
Vincoli di risorse e sicurezza 235
Esercizi pratici 235
Esercizio pratico 1: costruzione di un certificate server 236
Esercizio pratico 2: cifratura di dati con EFS e furto di certificati 236
Esercizio pratico 3: revoca del certificato EFS 237
Domande di ripasso 237
Risposte e spiegazioni 239

Capitolo 10 Risposta agli incidenti di sicurezza 243

Procedure di risposta agli incidenti 244
Processo di risposta agli incidenti 245
Concetti fondamentali dell'analisi forense 246
Strumenti software per valutare la sicurezza di un'organizzazione 251
Utility di backup 254
Tipi di backup 255
Strumenti da riga di comando 256
Analisi e interpretazione dell'output da tecnologie della sicurezza 261
Domande di ripasso 265
Risposte e spiegazioni 267

Capitolo 11 Gestione della continuità di business 271

Implementazione del progetto di sistemi sicuri 272
Sicurezza hardware/firmware 273
Sistemi operativi 274
Rendere sicuri i sistemi IT 274
Periferiche 275
L'importanza dei concetti di staging deployment sicuro 275
Risoluzione dei problemi di sicurezza comuni 277

Dispositivi malconfigurati 278
Problemi legati al personale....279
Problemi legati al software 280
Disaster recovery e continuità operativa....280
Domande di ripasso 282
Risposte e spiegazioni....284

Appendice A Preparazione all'esame CompTIA Security+ 501 287

Suggerimenti per l'esame 287
Preparazione all'esame 288
Lista di controllo per l'esame Security+ 289
Esercizio drag and drop 1: attacchi....290
Esercizio drag and drop 2: certificati....292
Esercizio drag and drop 3: porte/protocolli....293
Esercizio drag and drop 4: fattori di autenticazione....294
Esercizio drag and drop 5: generale....295
Drag and drop: risposte 296
Informazioni su Linux 301

Appendice B Simulazione d'esame 1 303

Appendice C Simulazione d'esame 2 317

Appendice D Risposte alle simulazioni d'esame 335

Simulazione d'esame 1 335
Simulazione d'esame 2....356

Appendice E Acronimi 383

Indice analitico....389