

# Inhaltsverzeichnis

1	<b>Laras Welt</b> .....	19
1.1	Das Ziel dieses Buches .....	20
1.2	Die CompTIA Security+-Zertifizierung .....	20
1.3	Voraussetzungen für CompTIA Security+ .....	22
1.4	Persönliches .....	22
2	<b>Sind Sie bereit für CompTIA Security+?</b> .....	25
3	<b>Wo liegt denn das Problem?</b> .....	33
3.1	Fangen Sie bei sich selber an .....	33
3.2	Die Gefahrenlage .....	35
3.3	Die Analyse der Bedrohungslage .....	38
3.4	Kategorien der Informationssicherheit .....	38
3.5	Modelle und Lösungsansätze .....	41
	3.5.1 TCSEC oder ITSEC .....	41
	3.5.2 Common Criteria .....	42
	3.5.3 ISO 27000 .....	44
3.6	Die IT-Grundschutzkataloge des BSI .....	44
3.7	Lösungsansätze für die Praxis .....	46
	3.7.1 Das Information Security Management System .....	47
	3.7.2 Sicherheitsmanagement und Richtlinien .....	48
	3.7.3 Die Notfallvorsorge .....	49
	3.7.4 Die Cyber-Security-Strategie .....	49
3.8	Fragen zu diesem Kapitel .....	51
4	<b>Verschlüsselungstechnologie</b> .....	55
4.1	Grundlagen der Kryptografie .....	56
	4.1.1 One-Time-Pad .....	57
	4.1.2 Diffusion und Konfusion .....	58
	4.1.3 Blockverschlüsselung .....	58
	4.1.4 Stromverschlüsselung .....	59
4.2	Symmetrische Verschlüsselung .....	61
	4.2.1 DES .....	62
	4.2.2 3DES .....	62

4.2.3	AES .....	63
4.2.4	Blowfish.....	63
4.2.5	Twofish .....	64
4.2.6	RC4 .....	64
4.3	Asymmetrische Verschlüsselung .....	64
4.3.1	RSA .....	66
4.3.2	Diffie-Hellman .....	66
4.3.3	ECC .....	67
4.3.4	Perfect Forward Secrecy (PFS).....	68
4.3.5	Die Zukunft der Quanten .....	68
4.4	Hash-Verfahren .....	68
4.4.1	MD4 und MD5 .....	70
4.4.2	SHA.....	70
4.4.3	RIPEMD .....	71
4.4.4	HMAC .....	71
4.4.5	Hash-Verfahren mit symmetrischer Verschlüsselung .....	72
4.4.6	Digitale Signaturen.....	72
4.4.7	Hybride Verschlüsselung.....	73
4.5	Drei Status digitaler Daten .....	74
4.5.1	Data-in-transit .....	74
4.5.2	Data-at-rest .....	74
4.5.3	Data-in-use .....	75
4.6	Bekannte Angriffe gegen die Verschlüsselung .....	75
4.6.1	Cipher-text-only-Angriff.....	75
4.6.2	Known/Chosen-plain-text-Angriff.....	76
4.6.3	Schwache Verschlüsselung / Implementierung .....	76
4.6.4	Probleme mit Zertifikaten .....	76
4.7	PKI in Theorie und Praxis.....	77
4.7.1	Aufbau einer hierarchischen PKI .....	78
4.7.2	SSL-Zertifikate X.509 Version 3 .....	80
4.7.3	Zertifikatstypen.....	81
4.7.4	Zurückziehen von Zertifikaten .....	83
4.7.5	Hinterlegung von Schlüsseln .....	83
4.7.6	Aufsetzen einer hierarchischen PKI.....	84
4.8	Fragen zu diesem Kapitel .....	84
5	<b>Die Geschichte mit der Identität.....</b>	<b>87</b>
5.1	Identitäten und deren Rechte .....	87
5.1.1	Zuweisung von Rechten.....	87

5.1.2	Rollen .....	89
5.1.3	Single Sign On .....	89
5.2	Authentifizierungsmethoden .....	90
5.2.1	Benutzername und Kennwort .....	90
5.2.2	Token .....	91
5.2.3	Zertifikate .....	91
5.2.4	Biometrie .....	92
5.2.5	Benutzername, Kennwort und Smartcard .....	94
5.2.6	Wechselseitige Authentifizierung .....	95
5.3	Zugriffssteuerungsmodelle .....	95
5.3.1	Mandatory Access Control (MAC) .....	95
5.3.2	Discretionary Access Control (DAC) .....	97
5.3.3	Role Based Access Control (RBAC) .....	98
5.3.4	Principle of Least Privileges .....	99
5.4	Protokolle für die Authentifizierung .....	99
5.4.1	Kerberos .....	100
5.4.2	PAP .....	101
5.4.3	CHAP .....	101
5.4.4	NTLM .....	102
5.5	Die Non-Repudiation .....	102
5.6	Vom Umgang mit Passwörtern .....	103
5.7	Fragen zu diesem Kapitel .....	104
<b>6</b>	<b>Physische Sicherheit .....</b>	<b>107</b>
6.1	Zutrittsregelungen .....	108
6.1.1	Schlüsselsysteme .....	109
6.1.2	Badges und Keycards .....	110
6.1.3	Biometrische Erkennungssysteme .....	110
6.1.4	Zutrittsschleusen .....	111
6.1.5	Videouberwachung .....	113
6.1.6	Multiple Systeme .....	113
6.2	Bauschutz .....	114
6.2.1	Einbruchschutz .....	114
6.2.2	Hochwasserschutz .....	115
6.2.3	Brandschutz .....	115
6.2.4	Klimatisierung und Kühlung .....	117
6.3	Elektrostatische Entladung .....	119
6.4	Stromversorgung .....	119
6.4.1	USV .....	120

6.4.2	Notstromgruppen . . . . .	122
6.4.3	Einsatzszenarien . . . . .	123
6.4.4	Rotationsenergiestromversorgungen . . . . .	124
6.4.5	Ein Wort zu EMP . . . . .	124
6.5	Feuchtigkeit und Temperatur . . . . .	125
6.6	Fragen zu diesem Kapitel . . . . .	127
7	<b>Im Angesicht des Feindes</b> . . . . .	129
7.1	Malware ist tatsächlich böse . . . . .	129
7.1.1	Die Problematik von Malware . . . . .	133
7.1.2	Viren und ihre Unterarten . . . . .	134
7.1.3	Wie aus Trojanischen Pferden böse Trojaner wurden. . . . .	137
7.1.4	Backdoor . . . . .	141
7.1.5	Logische Bomben . . . . .	142
7.1.6	Würmer . . . . .	142
7.1.7	Ransomware . . . . .	143
7.1.8	Hoaxes . . . . .	145
7.2	Social Engineering . . . . .	145
7.2.1	Phishing . . . . .	148
7.2.2	Vishing . . . . .	152
7.2.3	Spear Phishing . . . . .	153
7.2.4	Pharming . . . . .	153
7.2.5	Drive-by-Pharming . . . . .	154
7.3	Angriffe gegen IT-Systeme . . . . .	155
7.3.1	Exploits und Exploit-Kits . . . . .	155
7.3.2	Darknet und Darkweb . . . . .	157
7.3.3	Malwaretising . . . . .	157
7.3.4	Watering-Hole-Attacke . . . . .	157
7.3.5	Malware Dropper . . . . .	158
7.3.6	RAT (Remote Access Tool) . . . . .	158
7.3.7	Keylogger . . . . .	159
7.3.8	Post Exploitation . . . . .	159
7.4	Gefahren für die Nutzung mobiler Geräte und Dienste . . . . .	161
7.5	APT – Advanced Persistent Threats . . . . .	162
7.5.1	Stuxnet . . . . .	163
7.5.2	Carbanak . . . . .	163
7.6	Advanced Threats . . . . .	164
7.6.1	Evasion-Techniken . . . . .	164
7.6.2	Pass-the-Hash-Angriffe (PtH) . . . . .	166

7.6.3	Kaltstartattacke (Cold Boot Attack) . . . . .	166
7.6.4	Physische RAM-Manipulation über DMA (FireWire-Hack) . . . . .	167
7.6.5	Human Interface Device Attack (Teensy USB HID Attack) . . . . .	167
7.6.6	BAD-USB-Angriff. . . . .	167
7.6.7	SSL-Stripping-Angriff . . . . .	168
7.6.8	Angriff über Wireless-Mäuse . . . . .	169
7.7	Angriffe in Wireless-Netzwerken. . . . .	169
7.7.1	Spoofing in Wireless-Netzwerken. . . . .	170
7.7.2	Sniffing in drahtlosen Netzwerken. . . . .	170
7.7.3	DNS-Tunneling in Public WLANs . . . . .	172
7.7.4	Rogue Access Point/Evil Twin. . . . .	172
7.7.5	Attacken auf die WLAN-Verschlüsselung . . . . .	173
7.7.6	Verschlüsselung brechen mit WPS-Attacken. . . . .	174
7.7.7	Denial-of-Service-Angriffe im WLAN . . . . .	175
7.7.8	Angriffe auf NFC-Technologien . . . . .	175
7.8	Das Internet of Angriff . . . . .	176
7.9	Fragen zu diesem Kapitel . . . . .	178
<b>8</b>	<b>Systemsicherheit realisieren . . . . .</b>	<b>181</b>
8.1	Konfigurationsmanagement. . . . .	182
8.2	Das Arbeiten mit Richtlinien . . . . .	184
8.3	Grundlagen der Systemhärtung. . . . .	186
8.3.1	Schutz von Gehäuse und BIOS. . . . .	188
8.3.2	Sicherheit durch TPM . . . . .	189
8.3.3	Full Disk Encryption . . . . .	190
8.3.4	Softwarebasierte Laufwerksverschlüsselung . . . . .	190
8.3.5	Hardware-Sicherheitsmodul . . . . .	190
8.3.6	Software-Firewall (Host-based Firewall). . . . .	191
8.3.7	Systemintegrität . . . . .	192
8.3.8	Überlegungen bei der Virtualisierung . . . . .	192
8.4	Embedded-Systeme und Industriesysteme . . . . .	193
8.5	Softwareaktualisierung ist kein Luxus . . . . .	198
8.5.1	Vom Hotfix zum Upgrade. . . . .	200
8.5.2	Problemkategorien . . . . .	201
8.5.3	Maintenance-Produkte. . . . .	201
8.5.4	Die Bedeutung des Patch- und Update-Managements . . . . .	203
8.5.5	Entfernen Sie, was Sie nicht brauchen. . . . .	204

8.6	Malware bekämpfen .....	205
8.6.1	Endpoint-Protection am Client .....	208
8.6.2	Reputationslösungen .....	208
8.6.3	Aktivitätsüberwachung HIPS/HIDS.....	209
8.6.4	Online-Virens Scanner – Webantivirus-NIPS .....	209
8.6.5	Sensibilisierung der Mitarbeitenden.....	210
8.6.6	Suchen und Entfernen von Viren .....	212
8.6.7	Virenschutzkonzept .....	213
8.6.8	Testen von Installationen.....	214
8.6.9	Sicher und vertrauenswürdig ist gut.....	214
8.7	Advanced Threat Protection .....	216
8.7.1	Explizites Applikations-Whitelisting versus -Blacklisting ...	216
8.7.2	Explizites Whitelisting auf Firewalls.....	217
8.7.3	Erweiterter Exploit-Schutz .....	218
8.7.4	Virtualisierung von Anwendungen.....	220
8.7.5	Schutz vor HID-Angriffen und BAD-USB .....	220
8.7.6	Geschlossene Systeme .....	222
8.7.7	Schutz vor SSL-Stripping-Angriffen .....	223
8.7.8	Schutz vor Angriffen über drahtlose Mäuse.....	225
8.7.9	Security Intelligence.....	225
8.8	Anwendungssicherheit .....	226
8.8.1	Lifecycle-Management/DevOps.....	226
8.8.2	Sichere Codierungskonzepte.....	227
8.8.3	Input Validation .....	227
8.8.4	Fehler- und Ausnahmebehandlung .....	227
8.8.5	NoSQL- versus SQL-Datenbanken .....	227
8.8.6	Serverseitige versus clientseitige Validierung .....	228
8.8.7	Session Token.....	228
8.8.8	Web-Application-Firewall (WAF).....	228
8.9	Fragen zu diesem Kapitel .....	229
<b>9</b>	<b>Sicherheit für mobile Systeme .....</b>	<b>231</b>
9.1	Die Risikolage mit mobilen Geräten und Diensten .....	232
9.2	Organisatorische Sicherheitsmaßnahmen .....	234
9.3	Technische Sicherheitsmaßnahmen .....	235
9.3.1	Vollständige Geräteverschlüsselung (Full Device Encryption) .....	237
9.3.2	Gerätesperren (Lockout).....	238
9.3.3	Bildschirm Sperre (Screenlocks).....	238

9.3.4	Remote Wipe/Sanitation .....	239
9.3.5	Standortdaten (GPS) und Asset Tracking.....	239
9.3.6	Sichere Installationsquellen und Anwendungs- steuerung .....	240
9.3.7	VPN-Lösungen auf mobilen Geräten .....	241
9.3.8	Public-Cloud-Dienste auf mobilen Geräten .....	241
9.4	Anwendungssicherheit bei mobilen Systemen.....	241
9.4.1	Schlüsselverwaltung (Key-Management) .....	242
9.4.2	Credential-Management .....	242
9.4.3	Authentifizierung.....	242
9.4.4	Geo-Tagging .....	242
9.4.5	Verschlüsselung.....	243
9.4.6	Whitelisting von Anwendungen .....	243
9.4.7	Transitive Trust/Authentifizierung.....	243
9.5	Fragen rund um BYOD.....	243
9.5.1	Dateneigentum (Data Ownership) .....	244
9.5.2	Zuständigkeit für den Unterhalt (Support Ownership) ....	245
9.5.3	Antivirus-Management .....	245
9.5.4	Patch-Management .....	245
9.5.5	Forensik .....	246
9.5.6	Privatsphäre und Sicherheit der geschäftlichen Daten .....	246
9.5.7	Akzeptanz der Benutzer und akzeptable Benutzung .....	247
9.5.8	Architektur-/Infrastrukturüberlegungen .....	247
9.5.9	On-Board-Kamera/Video.....	248
9.6	Fragen zu diesem Kapitel .....	248
<b>10</b>	<b>Den DAU gibt's wirklich – und Sie sind schuld .....</b>	<b>251</b>
10.1	Klassifizierung von Informationen .....	252
10.1.1	Die Klassifizierung nach Status .....	252
10.1.2	Die Klassifizierung nach Risiken .....	254
10.1.3	Data Loss Prevention .....	256
10.1.4	Was es zu beachten gilt .....	257
10.2	Der Datenschutz .....	257
10.3	Vom Umgang mit dem Personal .....	260
10.4	E-Mail-Sicherheit.....	262
10.4.1	Secure Multipurpose Internet Mail Extensions (S/MIME) .....	263
10.4.2	PGP (Pretty Good Privacy).....	264
10.4.3	Schwachstellen .....	267

10.4.4	Schutz durch einen Mail-Gateway	270
10.4.5	Social Media	271
10.5	Daten sichern	272
10.5.1	Datensicherung oder Datenarchivierung?	273
10.5.2	Die gesetzlichen Grundlagen	274
10.5.3	Das Datensicherungskonzept	276
10.5.4	Methoden der Datensicherung	281
10.5.5	Online-Backup	283
10.5.6	Daten vernichten	285
10.6	Sicherheit im Umgang mit Servicepartnern	286
10.7	Fragen zu diesem Kapitel	288
<b>11</b>	<b>Sicherheit für Netzwerke</b>	<b>291</b>
11.1	Trennung von IT-Systemen	291
11.1.1	Subnettierung von Netzen	292
11.1.2	NAT	294
11.1.3	Network Access Control	295
11.2	VLAN	296
11.2.1	Planung und Aufbau von VLANs	296
11.2.2	Vorgehen gegen Risiken bei Switch-Infrastrukturen	300
11.2.3	Port Security	301
11.2.4	Flood Guard	302
11.2.5	Spanning-Tree Protocol und Loop Protection	302
11.2.6	Maßnahmen gegen Gefahren in VLANs	303
11.3	TCP/IP-Kernprotokolle	304
11.3.1	Internet Protocol	304
11.3.2	Internet Control Message Protocol	304
11.3.3	Transmission Control Protocol	305
11.3.4	User Datagram Protocol	306
11.4	Weitere Transport- und Netzwerkprotokolle	307
11.4.1	Address Resolution Protocol	307
11.4.2	Internet Group Management Protocol	307
11.4.3	SLIP und PPP	307
11.4.4	IP-Version 6	308
11.4.5	Portnummern	308
11.5	Anwendungen	309
11.5.1	Telnet und SSH	309
11.5.2	FTP und TFTP	309
11.5.3	SCP, SFTP und FTPS	310



11.5.4	DNS	310
11.5.5	SNMP	311
11.5.6	E-Mail-Protokolle	311
11.5.7	HTTP	312
11.5.8	SSL und TLS	312
11.5.9	NetBIOS und CIFS	313
11.5.10	Lightweight Directory Access	314
11.6	Sicherheit in der Cloud	314
11.6.1	Cloud-Computing-Betriebsmodelle	315
11.6.2	Formen des Einsatzes	316
11.7	Fragen zu diesem Kapitel	318
<b>12</b>	<b>Schwachstellen und Attacken</b>	<b>321</b>
12.1	Welches Risiko darf es denn sein?	321
12.2	Angriffe gegen IT-Systeme	323
12.2.1	Denial of Service	323
12.2.2	Pufferüberlauf	324
12.2.3	Race-Condition	325
12.2.4	Password Guessing und Cracking	325
12.3	Angriffe gegen Anwendungen	327
12.3.1	Directory-Traversal	327
12.3.2	Cross Site Scripting	328
12.3.3	Cross-Site Request Forgery (XSRF)	329
12.3.4	Injection-Varianten	329
12.3.5	Parametermanipulation	330
12.3.6	Transitive Zugriffe	331
12.3.7	Phishing	331
12.3.8	Treibermanipulationen	332
12.4	Angriffe gegen Clients	332
12.4.1	Drive by Attack	333
12.4.2	Böswillige Add-ons und Applets	333
12.4.3	Local Shared Objects (LSOs)	333
12.4.4	Spam, Spim und Spit	334
12.4.5	Typosquatting/URL-Hijacking	334
12.4.6	Clickjacking	334
12.4.7	Domain Hijacking	334
12.4.8	Man-in-the-Browser	334
12.5	Netzwerkangriffe	335
12.5.1	Denial of Service (DoS)	335

12.5.2	Distributed Denial of Service (DDoS) . . . . .	336
12.5.3	Spoofing . . . . .	337
12.5.4	Man in the Middle . . . . .	338
12.5.5	Replay-Angriff. . . . .	340
12.5.6	SSL-Downgrading. . . . .	341
12.5.7	Session-Hijacking. . . . .	341
12.5.8	Brechen von Schlüsseln . . . . .	342
12.5.9	Backdoor . . . . .	343
12.6	Angriffe gegen die Public Cloud. . . . .	343
12.7	Steganografie . . . . .	344
12.8	Unterschiedliche Angriffertypen . . . . .	345
12.8.1	Von Hüten und Angreifern . . . . .	345
12.8.2	Eigenschaften der verschiedenen Angreifer . . . . .	347
12.9	Fragen zu diesem Kapitel . . . . .	348
<b>13</b>	<b>Der sichere Remotezugriff . . . . .</b>	<b>351</b>
13.1	Virtual Private Network. . . . .	351
13.1.1	Site-to-Site-VPN . . . . .	353
13.1.2	Remote-Access-VPN . . . . .	354
13.1.3	Soft- und Hardwarelösungen. . . . .	355
13.2	Remote Access Server . . . . .	356
13.3	Protokolle für den entfernten Zugriff . . . . .	356
13.3.1	802.1x. . . . .	356
13.3.2	RADIUS . . . . .	358
13.3.3	TACACS, XTACACS und TACACS+ . . . . .	359
13.3.4	L2TP und PPTP . . . . .	360
13.3.5	IPsec . . . . .	361
13.3.6	SSL/TLS. . . . .	367
13.3.7	SSH . . . . .	367
13.4	Schwachstellen. . . . .	368
13.5	Fragen zu diesem Kapitel . . . . .	370
<b>14</b>	<b>Drahtlose Netzwerke sicher gestalten . . . . .</b>	<b>373</b>
14.1	Aller WLAN-Standard beginnt mit IEEE 802.11 . . . . .	374
14.1.1	Die Standards IEEE 802.11a/b/g. . . . .	374
14.1.2	Die Gegenwart: IEEE 802.11n und 802.11ac. . . . .	375
14.1.3	Frequenzträger und Kanalbreite . . . . .	378
14.2	Die Verbindungsaufnahme im WLAN. . . . .	380
14.2.1	Das Ad-hoc-Netzwerk . . . . .	380
14.2.2	Das Infrastrukturnetzwerk. . . . .	380

14.3	Ein WLAN richtig aufbauen . . . . .	381
14.3.1	Aufbau der Hardware. . . . .	381
14.3.2	Konfiguration des drahtlosen Netzwerks . . . . .	383
14.4	Sicherheit in drahtlosen Verbindungen. . . . .	385
14.4.1	Wired Equivalent Privacy. . . . .	386
14.4.2	WPA und 802.11i . . . . .	388
14.4.3	Die Implementierung von 802.1x . . . . .	390
14.4.4	Das Extensible Authentication Protocol (EAP). . . . .	391
14.4.5	WAP (Wireless Application Protocol) . . . . .	392
14.4.6	Near Field Communication. . . . .	393
14.5	Grundlegende Sicherheitsmaßnahmen umsetzen. . . . .	393
14.6	Wireless Intrusion Prevention System . . . . .	396
14.7	Bluetooth – Risiken und Maßnahmen . . . . .	396
14.8	Fragen zu diesem Kapitel . . . . .	398
<b>15</b>	<b>System- und Netzwerküberwachung . . . . .</b>	<b>401</b>
15.1	Das OSI-Management-Framework . . . . .	401
15.2	SNMP-Protokolle. . . . .	404
15.3	Leistungsüberwachung. . . . .	407
15.4	Das Monitoring von Netzwerken . . . . .	408
15.5	Monitoring-Programme . . . . .	410
15.5.1	Der Windows-Netzwerkmonitor . . . . .	410
15.5.2	Wireshark . . . . .	412
15.5.3	inSSIDer . . . . .	414
15.5.4	MRTG bzw. RRDTools. . . . .	415
15.5.5	Nagios . . . . .	417
15.6	Zusammenführen der Logs in einem SIEM . . . . .	417
15.7	Kommandozeilenprogramme. . . . .	418
15.7.1	ipconfig/ip. . . . .	418
15.7.2	ping . . . . .	419
15.7.3	ARP . . . . .	420
15.7.4	tracert/traceroute . . . . .	421
15.7.5	nslookup . . . . .	421
15.7.6	netstat . . . . .	422
15.8	Fragen zu diesem Kapitel . . . . .	423
<b>16</b>	<b>Brandschutzmauer für das Netzwerk . . . . .</b>	<b>427</b>
16.1	Damit kein Feuer ausbricht . . . . .	427
16.2	Personal Firewalls und dedizierte Firewalls . . . . .	429

16.3	Das Regelwerk einer Firewall . . . . .	431
16.3.1	Positive Exceptions (Positive Rules) . . . . .	431
16.3.2	Negative Exceptions (Negative Rules) . . . . .	432
16.4	Das Konzept der DMZ. . . . .	433
16.4.1	Trennung Hostsystem von den virtuellen Maschinen. . . . .	434
16.4.2	Trennung bei WLAN-Infrastrukturen. . . . .	434
16.4.3	Extranet und Intranet . . . . .	435
16.5	Nicht jede Firewall leistet dasselbe. . . . .	435
16.5.1	Wenn einfach auch reicht: Die Paketfilter-Firewall . . . . .	435
16.5.2	Der nächste Level: Stateful Packet Inspection Firewall . . . . .	437
16.5.3	Jetzt wird's gründlich: Application Level Gateway. . . . .	437
16.5.4	Anwendungsbeispiele . . . . .	440
16.5.5	Unified Threat Management Firewall. . . . .	441
16.6	Die Angreifer kommen – aber Sie wissen's schon . . . . .	441
16.7	Unified Threat Management . . . . .	444
16.8	Fragen zu diesem Kapitel . . . . .	446
<b>17</b>	<b>Penetration Testing und Forensics. . . . .</b>	<b>449</b>
17.1	Penetration Testing . . . . .	449
17.1.1	Organisatorische Einbettung . . . . .	450
17.1.2	Prinzipielle Vorgehensweise . . . . .	451
17.1.3	Black Box und White Box. . . . .	454
17.1.4	Security-Scanner. . . . .	455
17.1.5	Datenbanken für Recherchen nach Sicherheitslücken . . . . .	457
17.1.6	Passwort-Guesser und -Cracker. . . . .	457
17.1.7	Paketgeneratoren und Netzwerk-Sniffer. . . . .	459
17.1.8	Fuzzing . . . . .	460
17.1.9	Metasploit Framework . . . . .	460
17.2	Forensics. . . . .	461
17.2.1	Vorbereitung . . . . .	461
17.2.2	Sichern von Beweismitteln . . . . .	462
17.2.3	Beweissicherung nach RFC 3227 . . . . .	463
17.2.4	Schutz und Analyse von Beweismitteln . . . . .	464
17.2.5	Timeline . . . . .	466
17.2.6	Data-Carving . . . . .	466
17.2.7	Suche nach Zeichenketten. . . . .	467
17.2.8	Nutzung von Hash-Datenbanken . . . . .	468
17.2.9	Programme und Toolkits . . . . .	468
17.3	Fragen zu diesem Kapitel . . . . .	470

<b>18</b>	<b>Wider den Notfall</b> .....	473
18.1	Fehlertoleranz .....	474
	18.1.1 RAID .....	474
	18.1.2 RAID Level .....	475
	18.1.3 Duplexing .....	480
	18.1.4 Übersicht RAID .....	481
18.2	Redundante Verbindungen und Systeme .....	481
	18.2.1 Network Loadbalancing .....	481
	18.2.2 Cluster .....	482
18.3	Notfallvorsorgeplanung .....	483
	18.3.1 Bedrohungsanalyse .....	483
	18.3.2 Von der Bedrohung bis zur Maßnahme .....	484
18.4	Analyse .....	485
	18.4.1 Ausfallszenarien .....	485
	18.4.2 Impact-Analyse .....	486
18.5	Umsetzung .....	487
	18.5.1 Strategie und Planung .....	488
	18.5.2 Verschiedene Implementierungsansätze .....	490
	18.5.3 Incident-Response-Prozesse .....	492
	18.5.4 Der Vorfallsreaktionsplan (Incident Response Plan) .....	492
18.6	Test und Wartung des Disaster-Recovery-Plans .....	493
	18.6.1 Wartung der Disaster Recovery .....	494
	18.6.2 Punktuelle Anpassungen .....	494
	18.6.3 Regelmäßige Überprüfung .....	494
18.7	Merkmale zur Disaster Recovery .....	495
18.8	Fragen zu diesem Kapitel .....	495
<b>19</b>	<b>Security-Audit</b> .....	499
19.1	Grundlagen von Security-Audits .....	500
	19.1.1 Fragestellungen .....	500
	19.1.2 Prinzipielle Vorgehensweise .....	500
	19.1.3 Bestandteile eines Security-Audits .....	501
19.2	Standards .....	501
	19.2.1 ISO 27001 .....	502
	19.2.2 IT-Grundschutzkataloge .....	502
	19.2.3 Kombination aus ISO 27000 und IT-Grundschutz .....	504
19.3	Beispiel-Audit Windows Server 2008 .....	504
	19.3.1 Nutzung von Sicherheitsvorlagen .....	505
	19.3.2 Einsatz von Kommandos und Scripts .....	505

19.3.3	Passwortschutz	505
19.3.4	Geräteschutz	506
19.3.5	Sichere Basiskonfiguration	506
19.3.6	Sichere Installation und Bereitstellung	506
19.3.7	Sichere Konfiguration der IIS-Basis-Komponente	506
19.3.8	Sichere Migration auf Windows Server 2003/2008	507
19.3.9	Umgang mit Diensten unter Windows Server	507
19.3.10	Deinstallation nicht benötigter Client-Funktionen	507
19.3.11	Verwendung der Softwareeinschränkungsrichtlinie	507
19.4	Berichtswesen	507
19.4.1	Titelseite	508
19.4.2	Einleitung	508
19.4.3	Management-Summary	508
19.4.4	Ergebnisse der Untersuchung	508
19.4.5	Erforderliche Maßnahmen	509
19.4.6	Anhang	509
19.5	Ergänzende Maßnahmen	510
19.5.1	Logfile-Analyse	510
19.5.2	Echtzeitanalyse von Netzwerkverkehr und Zugriffen	511
19.5.3	Risikoanalyse	511
19.6	Fragen zu diesem Kapitel	512
<b>20</b>	<b>Die CompTIA Security+-Prüfung</b>	<b>515</b>
20.1	Was von Ihnen verlangt wird	516
20.2	Wie Sie sich vorbereiten können	516
20.3	Wie eine Prüfung aussieht	517
20.4	Beispielprüfung zum Examen CompTIA Security+	521
<b>A</b>	<b>Anhänge</b>	<b>539</b>
A.1	Hier finden Sie die Prüfungsthemen	539
A.2	Antworten zu den Vorbereitungsfragen	541
A.3	Antworten zu den Kapitelnfragen	541
A.4	Antworten zu Fragen der Beispielprüfung	543
A.5	Weiterführende Literatur	544
A.5.1	Nützliche Literatur zum Thema	544
A.5.2	Weiterführende Links zum Thema	545
<b>B</b>	<b>Abkürzungsverzeichnis</b>	<b>547</b>
	<b>Stichwortverzeichnis</b>	<b>559</b>