

# Inhaltsverzeichnis

<b>1</b>	<b>Laras Welt</b> . . . . .	<b>19</b>
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
<b>2</b>	<b>Sind Sie bereit für CompTIA Security+?</b> . . . . .	<b>25</b>
<b>3</b>	<b>Wo liegt denn das Problem?</b> . . . . .	<b>33</b>
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 . . . . .	48
3.7.4	Die Cyber-Security-Strategie . . . . .	49
3.8	Fragen zu diesem Kapitel . . . . .	51
<b>4</b>	<b>Verschlüsselungstechnologie</b> . . . . .	<b>53</b>
4.1	Grundlagen der Kryptografie . . . . .	53
4.1.1	One-Time-Pad . . . . .	54
4.1.2	Blockverschlüsselung . . . . .	55
4.1.3	Stromverschlüsselung . . . . .	56
4.2	Symmetrische Verschlüsselung . . . . .	58
4.2.1	DES . . . . .	58
4.2.2	3DES . . . . .	59
4.2.3	AES . . . . .	59

4.2.4	Blowfish.....	60
4.2.5	Twofish .....	60
4.2.6	RC4 .....	60
4.3	Asymmetrische Verschlüsselung .....	61
4.3.1	RSA .....	62
4.3.2	Diffie-Hellman .....	62
4.3.3	ECC .....	63
4.3.4	Perfect Forward Secrecy (PFS).....	64
4.3.5	Die Zukunft der Quanten .....	64
4.4	Hash-Verfahren .....	64
4.4.1	MD4 und MD5 .....	66
4.4.2	SHA .....	66
4.4.3	RIPEMD .....	67
4.4.4	HMAC.....	67
4.4.5	Hash-Verfahren mit symmetrischer Verschlüsselung .....	67
4.4.6	Digitale Signaturen.....	68
4.4.7	Hybride Verschlüsselung.....	69
4.5	PKI in Theorie und Praxis.....	69
4.5.1	Aufbau einer hierarchischen PKI .....	71
4.5.2	Zurückziehen von Zertifikaten .....	72
4.5.3	Hinterlegung von Schlüsseln .....	73
4.5.4	Aufsetzen einer hierarchischen PKI .....	73
4.6	Fragen zu diesem Kapitel .....	74
5	<b>Die Geschichte mit der Identität.</b> .....	77
5.1	Identitäten und deren Rechte .....	77
5.1.1	Zuweisung von Rechten.....	77
5.1.2	Rollen.....	79
5.1.3	Single Sign On .....	79
5.2	Authentifizierungsmethoden .....	80
5.2.1	Benutzername und Kennwort .....	80
5.2.2	Token.....	81
5.2.3	Zertifikate .....	81
5.2.4	Biometrie.....	82
5.2.5	Benutzername, Kennwort und Smartcard .....	84
5.2.6	Wechselseitige Authentifizierung .....	85
5.3	Zugriffssteuerungsmodelle.....	85
5.3.1	Mandatory Access Control (MAC).....	85
5.3.2	Discretionary Access Control (DAC).....	87

5.3.3	Role Based Access Control (RBAC) . . . . .	88
5.3.4	Principle of Least Privileges . . . . .	89
5.4	Protokolle für die Authentifizierung . . . . .	89
5.4.1	Kerberos . . . . .	90
5.4.2	PAP . . . . .	91
5.4.3	CHAP . . . . .	91
5.4.4	NTLM . . . . .	92
5.5	Die Non-Repudiation. . . . .	92
5.6	Vom Umgang mit Passwörtern . . . . .	93
5.7	Fragen zu diesem Kapitel . . . . .	94
<b>6</b>	<b>Physische Sicherheit</b> . . . . .	<b>97</b>
6.1	Zutrittsregelungen. . . . .	98
6.1.1	Schlüsselsysteme . . . . .	99
6.1.2	Badges und Keycards . . . . .	100
6.1.3	Biometrische Erkennungssysteme . . . . .	100
6.1.4	Zutrittsschleusen . . . . .	101
6.1.5	Videouberwachung. . . . .	103
6.1.6	Multiple Systeme . . . . .	103
6.2	Bauschutz. . . . .	104
6.2.1	Einbruchschutz. . . . .	104
6.2.2	Hochwasserschutz . . . . .	105
6.2.3	Brandschutz . . . . .	105
6.2.4	Klimatisierung und Kühlung . . . . .	107
6.3	Elektrostatische Entladung . . . . .	108
6.4	Stromversorgung. . . . .	109
6.4.1	USV. . . . .	110
6.4.2	Notstromgruppen. . . . .	112
6.4.3	Einsatzszenarien. . . . .	112
6.4.4	Rotationsenergiestromversorgungen . . . . .	114
6.4.5	Ein Wort zu EMP . . . . .	114
6.5	Fragen zu diesem Kapitel . . . . .	114
<b>7</b>	<b>Im Angesicht des Feindes</b> . . . . .	<b>117</b>
7.1	Malware ist tatsächlich böse . . . . .	117
7.1.1	Die Problematik von Malware. . . . .	121
7.1.2	Viren und ihre Unterarten. . . . .	122
7.1.3	Wie aus Trojanischen Pferden böse Trojaner wurden . . . . .	125
7.1.4	Backdoor . . . . .	129

7.1.5	Logische Bomben .....	130
7.1.6	Würmer .....	130
7.1.7	Ransomware .....	131
7.1.8	Hoaxes .....	133
7.2	Social Engineering .....	133
7.2.1	Phishing .....	136
7.2.2	Vishing .....	139
7.2.3	Spear Phishing .....	140
7.2.4	Pharming .....	140
7.2.5	Drive-by-Pharming .....	141
7.3	Angriffe gegen IT-Systeme .....	142
7.3.1	Exploits und Exploit-Kits .....	142
7.3.2	Darknet und Darkweb .....	144
7.3.3	Malwaretising .....	144
7.3.4	Watering-Hole-Attacke .....	144
7.3.5	Malware Dropper .....	145
7.3.6	RAT (Remote Access Tool) .....	145
7.3.7	Keylogger .....	146
7.3.8	Post Exploitation .....	147
7.4	Gefahren für die Nutzung mobiler Geräte und Dienste .....	148
7.5	APT – Advanced Persistent Threats .....	149
7.5.1	Stuxnet .....	150
7.5.2	Carbanak .....	150
7.6	Advanced Threats .....	151
7.6.1	Evasion-Techniken .....	151
7.6.2	Pass-the-Hash-Angriffe (PtH) .....	153
7.6.3	Kaltstartattacke (Cold Boot Attack) .....	153
7.6.4	Physische RAM-Manipulation über DMA (FireWire-Hack) .....	154
7.6.5	Human Interface Device Attack (Teensy USB HID Attack) .....	154
7.6.6	BAD-USB-Angriff .....	154
7.6.7	SSL-Stripping-Angriff .....	155
7.6.8	Angriff über Wireless-Mäuse .....	156
7.7	Angriffe in Wireless-Netzwerken .....	156
7.7.1	Spoofing in Wireless-Netzwerken .....	156
7.7.2	Sniffing in drahtlosen Netzwerken .....	157
7.7.3	DNS-Tunneling in Public WLANs .....	158

7.7.4	Rogue Access Point/Evil Twin . . . . .	159
7.7.5	Attacken auf die WLAN-Verschlüsselung . . . . .	160
7.7.6	Verschlüsselung brechen mit WPS-Attacken. . . . .	161
7.7.7	Denial-of-Service-Angriffe im WLAN . . . . .	162
7.7.8	Angriffe auf NFC-Technologien . . . . .	162
7.8	Das Internet of Angriff . . . . .	163
7.9	Fragen zu diesem Kapitel . . . . .	164
<b>8</b>	<b>Systemsicherheit realisieren . . . . .</b>	<b>167</b>
8.1	Konfigurationsmanagement . . . . .	168
8.2	Das Arbeiten mit Richtlinien . . . . .	170
8.3	Grundlagen der Systemhärtung . . . . .	172
8.3.1	Schutz von Gehäuse und BIOS . . . . .	174
8.3.2	Sicherheit durch TPM . . . . .	175
8.3.3	Full Disk Encryption . . . . .	176
8.3.4	Softwarebasierte Laufwerksverschlüsselung . . . . .	176
8.3.5	Hardware-Sicherheitsmodul . . . . .	176
8.3.6	Software-Firewall (Host-based Firewall) . . . . .	177
8.4	Softwareaktualisierung ist kein Luxus . . . . .	178
8.4.1	Vom Hotfix zum Upgrade . . . . .	179
8.4.2	Problemkategorien . . . . .	180
8.4.3	Maintenance-Produkte . . . . .	180
8.4.4	Die Bedeutung des Patch- und Update-Managements . . . . .	182
8.4.5	Entfernen Sie, was Sie nicht brauchen . . . . .	183
8.5	Malware bekämpfen . . . . .	184
8.5.1	Endpoint-Protection am Client . . . . .	187
8.5.2	Reputationslösungen . . . . .	187
8.5.3	Aktivitätsüberwachung HIPS/HIDS . . . . .	188
8.5.4	Online-Virens Scanner – Webantivirus-NIPS . . . . .	188
8.5.5	Sensibilisierung der Mitarbeitenden . . . . .	189
8.5.6	Suchen und Entfernen von Viren . . . . .	190
8.5.7	Virenschutzkonzept . . . . .	191
8.5.8	Testen von Installationen . . . . .	192
8.5.9	Sicher und vertrauenswürdig ist gut . . . . .	193
8.6	Advanced Threat Protection . . . . .	194
8.6.1	Explizites Applikations-Whitelisting versus -Blacklisting . . . . .	195
8.6.2	Explizites Whitelisting auf Firewalls . . . . .	196
8.6.3	Erweiterter Exploit-Schutz . . . . .	196
8.6.4	Virtualisierung von Anwendungen . . . . .	198

8.6.5	Schutz vor HID-Angriffen und BAD-USB	198
8.6.6	Geschlossene Systeme	200
8.6.7	Schutz vor SSL-Stripping-Angriffen	201
8.6.8	Schutz vor Angriffen über drahtlose Mäuse	203
8.6.9	Security Intelligence	203
8.7	Anwendungssicherheit	203
8.7.1	Sichere Codierungskonzepte	203
8.7.2	Input Validation	203
8.7.3	Fehler- und Ausnahmebehandlung	204
8.7.4	NoSQL- versus SQL-Datenbanken	204
8.7.5	Serverseitige versus clientseitige Validierung	204
8.7.6	Session Token	205
8.8	Fragen zu diesem Kapitel	205
<b>9</b>	<b>Sicherheit für mobile Systeme</b>	<b>207</b>
9.1	Die Risikolage mit mobilen Geräten und Diensten	208
9.2	Organisatorische Sicherheitsmaßnahmen	210
9.3	Technische Sicherheitsmaßnahmen	211
9.3.1	Vollständige Geräteverschlüsselung (Full Device Encryption)	213
9.3.2	Gerätesperren (Lockout)	214
9.3.3	Bildschirm Sperre (Screenlocks)	214
9.3.4	Remote Wipe/Sanitation	215
9.3.5	Standortdaten (GPS) und Asset Tracking	215
9.3.6	Sichere Installationsquellen und Anwendungssteuerung	216
9.3.7	VPN-Lösungen auf mobilen Geräten	217
9.3.8	Public-Cloud-Dienste auf mobilen Geräten	217
9.4	Anwendungssicherheit bei mobilen Systemen	217
9.4.1	Schlüsselverwaltung (Key Management)	218
9.4.2	Credential-Management	218
9.4.3	Authentifizierung	218
9.4.4	Geo-Tagging	218
9.4.5	Verschlüsselung	219
9.4.6	Whitelisting von Anwendungen	219
9.4.7	Transitive Trust/Authentifizierung	219
9.5	Fragen rund um BYOD	219
9.5.1	Dateneigentum (Data Ownership)	220
9.5.2	Zuständigkeit für den Unterhalt (Support Ownership)	220
9.5.3	Antivirus-Management	221

9.5.4	Patch Management . . . . .	221
9.5.5	Forensik . . . . .	221
9.5.6	Privatsphäre und Sicherheit der geschäftlichen Daten . . . . .	222
9.5.7	Akzeptanz der Benutzer und akzeptable Benutzung . . . . .	222
9.5.8	Architektur-/Infrastrukturüberlegungen . . . . .	223
9.5.9	On-Board-Kamera/Video . . . . .	223
9.6	Fragen zu diesem Kapitel . . . . .	224
<b>10</b>	<b>Den DAU gibt's wirklich – und Sie sind schuld</b> . . . . .	<b>227</b>
10.1	Klassifizierung von Informationen . . . . .	228
10.1.1	Die Klassierung nach Status . . . . .	228
10.1.2	Die Klassierung nach Risiken . . . . .	230
10.1.3	Data Loss Prevention . . . . .	232
10.1.4	Was es zu beachten gilt . . . . .	233
10.2	Der Datenschutz . . . . .	233
10.3	Vom Umgang mit dem Personal . . . . .	235
10.4	E-Mail-Sicherheit . . . . .	236
10.4.1	Secure Multipurpose Internet Mail Extensions (S/MIME) . . . . .	237
10.4.2	PGP (Pretty Good Privacy) . . . . .	238
10.4.3	Schwachstellen . . . . .	241
10.5	Daten sichern . . . . .	244
10.5.1	Datensicherung oder Datenarchivierung? . . . . .	245
10.5.2	Die gesetzlichen Grundlagen . . . . .	246
10.5.3	Das Datensicherungskonzept . . . . .	248
10.5.4	Methoden der Datensicherung . . . . .	253
10.5.5	Online-Backup . . . . .	255
10.6	Sicherheit im Umgang mit Servicepartnern . . . . .	257
10.7	Fragen zu diesem Kapitel . . . . .	259
<b>II</b>	<b>Sicherheit für Netzwerke</b> . . . . .	<b>261</b>
II.1	Trennung von IT-Systemen . . . . .	261
II.1.1	Subnettierung von Netzen . . . . .	262
II.1.2	NAT . . . . .	264
II.1.3	Network Access Control . . . . .	265
II.2	VLAN . . . . .	266
II.2.1	Planung und Aufbau von VLANs . . . . .	266
II.2.2	Vorgehen gegen Risiken bei Switch Infrastrukturen . . . . .	270
II.2.3	Port Security . . . . .	271

II.2.4	Flood Guard . . . . .	271
II.2.5	Spanning Tree Protocol und Loop Protection . . . . .	272
II.2.6	Maßnahmen gegen Gefahren in VLANs . . . . .	273
II.3	TCP/IP-Kernprotokolle . . . . .	273
II.3.1	Internet Protocol . . . . .	274
II.3.2	Internet Control Message Protocol . . . . .	274
II.3.3	Transmission Control Protocol . . . . .	275
II.3.4	User Datagram Protocol . . . . .	276
II.4	Weitere Transport- und Netzwerkprotokolle . . . . .	276
II.4.1	Address Resolution Protocol . . . . .	276
II.4.2	Internet Group Management Protocol . . . . .	277
II.4.3	SLIP und PPP . . . . .	277
II.4.4	IP Version 6 . . . . .	277
II.4.5	Portnummern . . . . .	278
II.5	Anwendungen . . . . .	278
II.5.1	Telnet und SSH . . . . .	279
II.5.2	FTP und TFTP . . . . .	279
II.5.3	SCP, SFTP und FTPS . . . . .	279
II.5.4	DNS . . . . .	280
II.5.5	SNMP . . . . .	280
II.5.6	E-Mail-Protokolle . . . . .	281
II.5.7	HTTP . . . . .	281
II.5.8	SSL und TLS . . . . .	282
II.5.9	NetBIOS und CIFS . . . . .	283
II.5.10	Lightweight Directory Access . . . . .	283
II.6	Sicherheit in der Cloud . . . . .	284
II.6.1	Formen des Einsatzes . . . . .	285
II.7	Fragen zu diesem Kapitel . . . . .	287
<b>12</b>	<b>Schwachstellen und Attacken . . . . .</b>	<b>289</b>
12.1	Welches Risiko darf es denn sein? . . . . .	289
12.2	Angriffe gegen IT-Systeme . . . . .	291
12.2.1	Denial of Service . . . . .	291
12.2.2	Pufferüberlauf . . . . .	292
12.2.3	Race-Condition . . . . .	293
12.2.4	Password Guessing und Cracking . . . . .	293
12.3	Angriffe gegen Anwendungen . . . . .	295
12.3.1	Directory-Traversal . . . . .	295
12.3.2	Cross Site Scripting . . . . .	296



12.3.3	Cross-Site Request Forgery (XSRF).....	296
12.3.4	Injection-Varianten .....	297
12.3.5	Parametermanipulation.....	298
12.3.6	Transitive Zugriffe .....	298
12.3.7	Phishing .....	299
12.4	Angriffe gegen Clients .....	300
12.4.1	Drive by Attack .....	300
12.4.2	Böswillige Add-ons und Applets .....	300
12.4.3	Local Shared Objects (LSOs) .....	301
12.4.4	Spam, Spim und Spit .....	301
12.4.5	Typosquatting/URL-Hijacking .....	301
12.5	Netzwerkangriffe .....	301
12.5.1	Denial of Service (DoS) .....	301
12.5.2	Distributed Denial of Service (DDoS).....	302
12.5.3	Spoofing .....	303
12.5.4	Man in the Middle .....	304
12.5.5	Replay-Angriff.....	307
12.5.6	SSL-Downgrading .....	307
12.5.7	Session-Hijacking.....	308
12.5.8	Brechen von Schlüsseln.....	309
12.5.9	Backdoor .....	309
12.6	Angriffe gegen die Public Cloud .....	310
12.7	Steganografie .....	311
12.8	Von Hüten und Angreifern .....	312
12.9	Fragen zu diesem Kapitel .....	313
<b>13</b>	<b>Der sichere Remotezugriff .....</b>	<b>317</b>
13.1	Virtual Private Network .....	317
13.1.1	Site-to-Site-VPN .....	319
13.1.2	Remote-Access-VPN.....	320
13.1.3	Soft- und Hardwarelösungen .....	321
13.2	Remote Access Server .....	322
13.3	Protokolle für den entfernten Zugriff .....	322
13.3.1	802.1X .....	322
13.3.2	RADIUS .....	324
13.3.3	TACACS, XTACACS und TACACS+ .....	325
13.3.4	L2TP und PPTP .....	326
13.3.5	IPsec .....	327
13.3.6	SSL.....	332

	13.3.7	SSH .....	332
13.4		Schwachstellen .....	334
13.5		Fragen zu diesem Kapitel .....	335
<b>14</b>		<b>Drahtlose Netzwerke sicher gestalten .....</b>	<b>337</b>
14.1		Aller WLAN-Standard beginnt mit IEEE 802.11 .....	338
	14.1.1	Die Standards IEEE 802.11a/b/g .....	338
	14.1.2	Die Gegenwart: IEEE 802.11n und 802.11ac .....	339
	14.1.3	Frequenzträger und Kanalbreite .....	342
14.2		Die Verbindungsaufnahme im WLAN .....	344
	14.2.1	Das Ad-hoc-Netzwerk .....	344
	14.2.2	Das Infrastrukturnetzwerk .....	344
14.3		Ein WLAN richtig aufbauen .....	345
	14.3.1	Aufbau der Hardware .....	345
	14.3.2	Konfiguration des drahtlosen Netzwerks .....	347
14.4		Sicherheit in drahtlosen Verbindungen .....	349
	14.4.1	Wired Equivalent Privacy .....	350
	14.4.2	WPA und 802.11i .....	352
	14.4.3	Die Implementierung von 802.1x .....	354
	14.4.4	Das Extensible Authentication Protocol (EAP) .....	355
	14.4.5	WAP (Wireless Application Protocol) .....	356
	14.4.6	Near Field Communication .....	357
14.5		Grundlegende Sicherheitsmaßnahmen umsetzen .....	357
14.6		Wireless Intrusion Prevention System .....	359
14.7		Bluetooth – Risiken und Maßnahmen .....	360
14.8		Fragen zu diesem Kapitel .....	362
<b>15</b>		<b>System- und Netzwerküberwachung .....</b>	<b>365</b>
15.1		Das OSI Management Framework .....	365
15.2		SNMP-Protokolle .....	368
15.3		Leistungsüberwachung .....	371
15.4		Das Monitoring von Netzwerken .....	372
15.5		Monitoring-Programme .....	374
	15.5.1	Der Windows-Netzwerkmonitor .....	374
	15.5.2	Wireshark .....	376
	15.5.3	inSSIDer .....	379
	15.5.4	MRTG bzw. RRDTools .....	379
	15.5.5	Nagios .....	381
15.6		Fragen zu diesem Kapitel .....	382

<b>16</b>	<b>Brandschutzmauer für das Netzwerk</b> .....	<b>385</b>
16.1	Damit kein Feuer ausbricht .....	385
16.2	Personal Firewalls und dedizierte Firewalls .....	387
16.3	Das Regelwerk einer Firewall .....	389
	16.3.1 Positive Exceptions (Positive Rules) .....	389
	16.3.2 Negative Exceptions (Negative Rules) .....	389
16.4	Das Konzept der DMZ .....	390
	16.4.1 Trennung Hostsystem von den virtuellen Maschinen .....	392
	16.4.2 Trennung bei WLAN-Infrastrukturen .....	392
16.5	Nicht jede Firewall leistet dasselbe .....	393
	16.5.1 Wenn einfach auch reicht: Die Paketfilter-Firewall .....	393
	16.5.2 Der nächste Level: Stateful Packet Firewall .....	394
	16.5.3 Jetzt wird's gründlich: Application Level Gateway .....	394
	16.5.4 Anwendungsbeispiele .....	397
	16.5.5 Unified Threat Management Firewall .....	398
16.6	Die Angreifer kommen – aber Sie wissen's schon .....	398
16.7	Unified Threat Management .....	401
16.8	Fragen zu diesem Kapitel .....	403
<b>17</b>	<b>Penetration Testing und Forensics</b> .....	<b>405</b>
17.1	Penetration Testing .....	405
	17.1.1 Organisatorische Einbettung .....	406
	17.1.2 Prinzipielle Vorgehensweise .....	407
	17.1.3 Black Box und White Box .....	410
	17.1.4 Security-Scanner .....	411
	17.1.5 Datenbanken für Recherchen nach Sicherheitslücken .....	412
	17.1.6 Passwort-Guesser und -Cracker .....	413
	17.1.7 Paketgeneratoren und Netzwerk-Sniffer .....	414
	17.1.8 Fuzzing .....	415
	17.1.9 Metasploit Framework .....	415
17.2	Forensics .....	416
	17.2.1 Vorbereitung .....	417
	17.2.2 Sichern von Beweismitteln .....	418
	17.2.3 Beweissicherung nach RFC 3227 .....	418
	17.2.4 Schutz und Analyse von Beweismitteln .....	419
	17.2.5 Timeline .....	421
	17.2.6 Data-Carving .....	422
	17.2.7 Suche nach Zeichenketten .....	423

17.2.8	Nutzung von Hash-Datenbanken .....	423
17.2.9	Programme und Toolkits .....	424
17.3	Fragen zu diesem Kapitel .....	425
<b>18</b>	<b>Die Notfallplanung .....</b>	<b>429</b>
18.1	Fehlertoleranz .....	430
18.1.1	RAID .....	430
18.1.2	RAID Level .....	431
18.1.3	Duplexing .....	436
18.1.4	Übersicht RAID .....	437
18.2	Redundante Verbindungen und Systeme .....	437
18.2.1	Network Loadbalancing .....	438
18.2.2	Cluster .....	438
18.3	Notfallvorsorgeplanung .....	439
18.4	Analyse .....	440
18.4.1	Ausfallszenarien .....	440
18.4.2	Impact-Analyse .....	441
18.5	Umsetzung .....	442
18.5.1	Strategie und Planung .....	442
18.5.2	Verschiedene Implementierungsansätze .....	444
18.6	Test des Disaster-Recovery-Plans .....	446
18.7	Wartung der Disaster Recovery .....	446
18.7.1	Punktuelle Anpassungen .....	447
18.7.2	Regelmäßige Überprüfung .....	447
18.8	Merkmale zur Disaster Recovery .....	448
18.9	Fragen zum Kapitel .....	448
<b>19</b>	<b>Security-Audit .....</b>	<b>451</b>
19.1	Grundlagen von Security-Audits .....	452
19.1.1	Fragestellungen .....	452
19.1.2	Prinzipielle Vorgehensweise .....	452
19.1.3	Bestandteile eines Security-Audits .....	453
19.2	Standards .....	453
19.2.1	ISO 27001 .....	454
19.2.2	IT-Grundschutzkataloge .....	454
19.2.3	Kombination aus ISO 27000 und IT-Grundschutz .....	456
19.3	Beispiel-Audit Windows Server 2008 .....	456
19.3.1	Nutzung von Sicherheitsvorlagen .....	457
19.3.2	Einsatz von Kommandos und Skripten .....	457

19.3.3	Passwortschutz	457
19.3.4	Geräteschutz	458
19.3.5	Sichere Basiskonfiguration	458
19.3.6	Sichere Installation und Bereitstellung	458
19.3.7	Sichere Konfiguration der IIS-Basis-Komponente	458
19.3.8	Sichere Migration auf Windows Server 2003/2008	459
19.3.9	Umgang mit Diensten unter Windows Server	459
19.3.10	Deinstallation nicht benötigter Client-Funktionen	459
19.3.11	Verwendung der Softwareeinschränkungsrichtlinie	459
19.4	Berichtswesen	459
19.4.1	Titelseite	460
19.4.2	Einleitung	460
19.4.3	Management-Summary	460
19.4.4	Ergebnisse der Untersuchung	460
19.4.5	Erforderliche Maßnahmen	461
19.4.6	Anhang	461
19.5	Ergänzende Maßnahmen	462
19.5.1	Logfile-Analyse	462
19.5.2	Echtzeitanalyse von Netzwerkverkehr und Zugriffen	463
19.5.3	Risikoanalyse	463
19.6	Fragen zu diesem Kapitel	464
20	<b>Die CompTIA Security+-Prüfung</b>	467
20.1	Was von Ihnen verlangt wird	468
20.2	Wie Sie sich vorbereiten können	468
20.3	Wie eine Prüfung aussieht	469
20.4	Beispielprüfung zum Examen CompTIA Security+	473
<b>A</b>	<b>Anhänge</b>	491
A.1	Hier finden Sie die Prüfungsthemen	491
A.2	Antworten zu den Vorbereitungsfragen	512
A.3	Antworten zu den Kapitelfragen	513
A.4	Antworten zu Fragen der Beispielprüfung	515
A.5	Weiterführende Literatur	516
A.5.1	Nützliche Literatur zum Thema	516
A.5.2	Weiterführende Links zum Thema	516
<b>B</b>	<b>Abkürzungsverzeichnis</b>	517
	<b>Stichwortverzeichnis</b>	527