

Inhaltsverzeichnis

1	Laras Welt.	23
1.1	Das Ziel dieses Buches	24
1.2	Die CompTIA Security+-Zertifizierung.	25
1.3	Voraussetzungen für CompTIA Security+	27
1.4	Persönliches.	27
2	Sind Sie bereit für CompTIA Security+?	31
3	Wo liegt denn das Problem?	39
3.1	Fangen Sie bei sich selbst an	39
3.2	Die Gefahrenlage.	41
3.3	Die Analyse der Bedrohungslage	44
3.4	Kategorien der Informationssicherheit	44
3.5	Modelle und Lösungsansätze	47
3.5.1	TCSEC oder ITSEC	47
3.5.2	Common Criteria	48
3.5.3	ISO 27000.	50
3.5.4	Das NIST Cybersecurity Framework	50
3.6	Der IT-Grundschutz nach BSI	52
3.7	Lösungsansätze für Ihr Unternehmen	55
3.7.1	Das Information Security Management System	57
3.7.2	Sicherheitsmanagement und Richtlinien.	57
3.7.3	Die Notfallvorsorge.	58
3.7.4	Risiken durch Dritte.	59
3.7.5	Die Cyber-Security-Strategie	60
3.8	Fragen zu diesem Kapitel	62
4	Rechtliche Grundlagen	65
4.1	Warum ist Datenschutz für Sie relevant?	66
4.1.1	Die Ursprünge des Datenschutzes	67
4.1.2	Datenschutz-Compliance für Unternehmen	68
4.1.3	Datenschutz als Beruf	69
4.2	Was sind Personendaten?	70
4.2.1	Relativer vs. absoluter Ansatz	70
4.2.2	Was sind Personendaten nach relativem Ansatz?	71

4.2.3	Anonymisierte und pseudonymisierte Daten.	71
4.2.4	Anwendungsbeispiele	71
4.2.5	Besonders sensible Daten	72
4.3	Was hat Datenschutz mit Datensicherheit zu tun?	73
4.3.1	Was bedeuten die gesetzlichen Vorgaben für die Praxis? ...	74
4.3.2	Data Breach Notifications.	76
4.3.3	Datenschutzfreundliches Design und ebensolche Konfiguration	76
4.3.4	Haftungsrisiko bei Missachtung der Datensicherheit	76
4.4	Inwiefern wird Missbrauch von Daten unter Strafe gestellt?	78
4.4.1	Unbefugte Datenbeschaffung (sog. Datendiebstahl)	78
4.4.2	Unbefugtes Eindringen in ein Datenverarbeitungs- system	78
4.4.3	Datenbeschädigung	79
4.4.4	Betrügerischer Missbrauch einer Datenverarbeitungs- anlage.	79
4.4.5	Erschleichen einer Leistung.	80
4.4.6	Unbefugte Entschlüsselung codierter Angebote	80
4.4.7	Unbefugtes Beschaffen von Personendaten.	80
4.4.8	Phishing und Skimming	81
4.4.9	Verletzung von Berufs-, Fabrikations- und Geschäfts- geheimnissen	81
4.4.10	Massenversand von Werbung (Spam)	82
4.5	Wann ist welches Gesetz anwendbar?	82
4.5.1	Sachlicher Anwendungsbereich	83
4.5.2	Räumlicher Anwendungsbereich	83
4.6	Welche Grundsätze müssen eingehalten werden?	86
4.7	Der Grundsatz der Datenminimierung	87
4.7.1	Unterschied zwischen Datensicherung und -archivierung.	88
4.7.2	Weshalb müssen Daten gesichert und archiviert werden?	88
4.7.3	Verwaltung der zu sichernden und zu archivierenden Daten	89
4.7.4	Wie werden nicht mehr benötigte Daten sicher vernichtet?	89
4.8	Welche Rechte haben die betroffenen Personen?	90
4.8.1	Recht auf Information	90

4.8.2	Recht auf Auskunft	91
4.8.3	Berichtigung, Einschränkung und Löschung	92
4.8.4	Recht auf Datenübertragbarkeit	92
4.8.5	Widerspruchsrecht	93
4.8.6	Beschwerderecht	94
4.9	Was ist bei der Zusammenarbeit mit Dritten zu beachten?	95
4.9.1	Auftragsbearbeiter	95
4.9.2	Gemeinsame Verantwortliche	96
4.9.3	Bearbeitung im Konzern	96
4.9.4	Datenexporte	96
4.10	Haftungsrisiken bei Datenschutzverletzungen	98
4.11	Fragen zu diesem Kapitel	101
5	Verschlüsselungstechnologie	103
5.1	Grundlagen der Kryptografie	104
5.1.1	Einige Grundbegriffe	105
5.1.2	One-Time-Pad	105
5.1.3	Diffusion und Konfusion	106
5.1.4	Blockverschlüsselung	107
5.1.5	Stromverschlüsselung	108
5.2	Symmetrische Verschlüsselung	109
5.2.1	DES	110
5.2.2	3DES	110
5.2.3	AES	111
5.2.4	Blowfish	111
5.2.5	Twofish	112
5.2.6	RC4	112
5.3	Asymmetrische Verschlüsselung	112
5.3.1	RSA	114
5.3.2	Diffie-Hellman	114
5.3.3	ECC	115
5.3.4	Perfect Forward Secrecy (PFS)	116
5.3.5	Die Zukunft der Quanten	116
5.4	Hash-Verfahren	116
5.4.1	MD4 und MD5	118
5.4.2	SHA	118
5.4.3	RIPEMD	119
5.4.4	HMAC	119
5.4.5	Hash-Verfahren mit symmetrischer Verschlüsselung	120

5.4.6	Digitale Signaturen	120
5.4.7	Hybride Verschlüsselung	120
5.5	Drei Status digitaler Daten	122
5.5.1	Data-in-transit	122
5.5.2	Data-at-rest	122
5.5.3	Data-in-use	123
5.6	Bekannte Angriffe gegen die Verschlüsselung	123
5.6.1	Cipher-text-only-Angriff	123
5.6.2	Known/Chosen-plain-text-Angriff	123
5.6.3	Schwache Verschlüsselung / Implementierung	124
5.6.4	Probleme mit Zertifikaten	124
5.7	PKI in Theorie und Praxis	124
5.7.1	Aufbau einer hierarchischen PKI	126
5.7.2	SSL-Zertifikate X.509 Version 3	127
5.7.3	Zertifikatstypen	128
5.7.4	Zurückziehen von Zertifikaten	131
5.7.5	Hinterlegung von Schlüsseln	131
5.7.6	Aufsetzen einer hierarchischen PKI	132
5.8	Fragen zu diesem Kapitel	132
6	Die Geschichte mit der Identität	135
6.1	Identitäten und deren Rechte	135
6.1.1	Zuweisung von Rechten	135
6.1.2	Rollen	137
6.1.3	Single Sign On	137
6.2	Authentifizierungsmethoden	137
6.2.1	Benutzername und Kennwort	138
6.2.2	Token	139
6.2.3	Zertifikate	139
6.2.4	Biometrie	140
6.2.5	Benutzername, Kennwort und Smartcard	142
6.2.6	Tokenization	143
6.2.7	Wechselseitige Authentifizierung	144
6.3	Zugriffssteuerungsmodelle	144
6.3.1	Mandatory Access Control (MAC)	144
6.3.2	Discretionary Access Control (DAC)	146
6.3.3	Role Based Access Control (RBAC)	146
6.3.4	ABAC – Attributbasiertes Zugriffssystem	148
6.3.5	Principle of Least Privileges	149

6.4	Protokolle für die Authentifizierung	149
6.4.1	Kerberos	149
6.4.2	PAP	150
6.4.3	CHAP	150
6.4.4	NTLM	151
6.4.5	Die Non-Repudiation	151
6.5	Vom Umgang mit Passwörtern	152
6.6	Fragen zu diesem Kapitel	153
7	Physische Sicherheit	157
7.1	Zutrittsregelungen.	158
7.1.1	Das Zonenkonzept.	159
7.1.2	Schlüsselsysteme	160
7.1.3	Badges und Keycards	160
7.1.4	Biometrische Erkennungssysteme	161
7.1.5	Zutrittsschleusen	162
7.1.6	Videoüberwachung.	163
7.1.7	Multiple Systeme	164
7.2	Bauschutz.	164
7.2.1	Einbruchsschutz.	164
7.2.2	Hochwasserschutz	165
7.2.3	Brandschutz	165
7.2.4	Klimatisierung und Kühlung	167
7.3	Elektrostatische Entladung	169
7.4	Stromversorgung.	170
7.4.1	USV	170
7.4.2	Notstromgruppen.	172
7.4.3	Einsatzszenarien.	173
7.4.4	Rotationsenergiestromversorgungen	174
7.4.5	Ein Wort zu EMP	175
7.5	Feuchtigkeit und Temperatur.	175
7.6	Fragen zu diesem Kapitel	177
8	Im Angesicht des Feindes.	179
8.1	Malware ist tatsächlich böse	180
8.1.1	Die Problematik von Malware	184
8.1.2	Viren und ihre Unterarten.	186
8.1.3	Wie aus Trojanischen Pferden böse Trojaner wurden	189
8.1.4	Backdoor	193

8.1.5	Logische Bomben	193
8.1.6	Würmer	194
8.1.7	Ransomware	195
8.1.8	Krypto-Malware (Cryptomalware)	197
8.1.9	Fileless Malware	198
8.1.10	Hoaxes	198
8.2	Angriffe mittels Social Engineering	199
8.2.1	Phishing	199
8.2.2	Vishing und Smishing	203
8.2.3	Spear Phishing	204
8.2.4	Pharming	205
8.2.5	Drive-by-Pharming	205
8.2.6	Doxing	206
8.3	Angriffe gegen IT-Systeme	206
8.3.1	Exploits und Exploit-Kits	207
8.3.2	Darknet und Darkweb	209
8.3.3	Malwaretising	210
8.3.4	Watering-Hole-Attacke	210
8.3.5	Malware Dropper und Malware-Scripts	210
8.3.6	RAT (Remote Access Tool/Remote Access Trojan)	211
8.3.7	Keylogger	211
8.3.8	Post Exploitation	213
8.4	Gefahren für die Nutzung mobiler Geräte und Dienste	214
8.5	APT – Advanced Persistent Threats	216
8.5.1	Carbanak	217
8.6	Advanced Threats	218
8.6.1	Evasion-Techniken	219
8.6.2	Pass-the-Hash-Angriffe (PtH)	220
8.6.3	Kaltstartattacke (Cold Boot Attack)	221
8.6.4	Physische RAM-Manipulation über DMA (FireWire-Hack)	221
8.6.5	Human Interface Device Attack (Teensy USB HID Attack)	221
8.6.6	BAD-USB-Angriff	222
8.6.7	Bösartiges USB-Kabel	222
8.6.8	SSL-Stripping-Angriff	223
8.6.9	Angriff über Wireless-Mäuse	223

8.7	Angriffe in Wireless-Netzwerken	224
8.7.1	Spoofing in Wireless-Netzwerken	225
8.7.2	Sniffing in drahtlosen Netzwerken	225
8.7.3	DNS-Tunneling in Public WLANs	227
8.7.4	Rogue Access Point/Evil Twin	228
8.7.5	Attacken auf die WLAN-Verschlüsselung	229
8.7.6	Verschlüsselung brechen mit WPS-Attacken	230
8.7.7	Denial-of-Service-Angriffe im WLAN	231
8.7.8	Angriffe auf NFC-Technologien	231
8.7.9	Angriffe auf Keycards	232
8.8	Moderne Angriffsformen	233
8.8.1	Angriffe mittels Drohnen	233
8.8.2	Verwundbare Anwendungen nachladen	234
8.8.3	Angriffe auf Application Programming Interface (API)	234
8.8.4	Gefahren durch künstliche Intelligenz (KI)	234
8.8.5	Das Internet of Things	235
8.9	Fragen zu diesem Kapitel	237
9	Systemsicherheit realisieren	241
9.1	Konfigurationsmanagement	242
9.2	Das Arbeiten mit Richtlinien	244
9.3	Grundlagen der Systemhärtung	246
9.3.1	Schutz von Gehäuse und BIOS	248
9.3.2	Sicherheit durch TPM	250
9.3.3	Full Disk Encryption	250
9.3.4	Softwarebasierte Laufwerksverschlüsselung	251
9.3.5	Hardware-Sicherheitsmodul	251
9.3.6	Software-Firewall (Host-based Firewall)	252
9.3.7	Systemintegrität	252
9.3.8	Überlegungen bei der Virtualisierung	253
9.4	Embedded-Systeme und Industriesysteme	254
9.5	Softwareaktualisierung ist kein Luxus	259
9.5.1	Vom Hotfix zum Upgrade	261
9.5.2	Problemkategorien	262
9.5.3	Maintenance-Produkte	262
9.5.4	Die Bedeutung des Patch- und Update-Managements	264
9.5.5	Entfernen Sie, was Sie nicht brauchen	265
9.6	Malware bekämpfen	266
9.6.1	Endpoint-Protection am Client	269

9.6.2	Reputationslösungen	270
9.6.3	Aktivitätsüberwachung HIPS/HIDS.	270
9.6.4	Online-Virens Scanner – Webantivirus-NIPS	271
9.6.5	Sensibilisierung der Mitarbeitenden.	271
9.6.6	Suchen und Entfernen von Viren	273
9.6.7	Virenschutzkonzept	274
9.6.8	Testen von Installationen.	276
9.6.9	Sicher und vertrauenswürdig ist gut.	276
9.7	Advanced Threat Protection	278
9.7.1	Explizites Applikations-Whitelisting versus -Blacklisting . . .	278
9.7.2	Explizites Whitelisting auf Firewalls	279
9.7.3	Erweiterter Exploit-Schutz	280
9.7.4	Virtualisierung von Anwendungen	282
9.7.5	Schutz vor HID-Angriffen und BAD-USB	282
9.7.6	Geschlossene Systeme	284
9.7.7	Schutz vor SSL-Stripping-Angriffen	285
9.7.8	Schutz vor Angriffen über drahtlose Mäuse.	287
9.7.9	Security- und Threat Intelligence	288
9.8	Anwendungssicherheit	289
9.8.1	Lifecycle-Management/DevOps.	289
9.8.2	Sichere Codierungskonzepte	290
9.8.3	Input Validation	290
9.8.4	Fehler- und Ausnahmebehandlung	290
9.8.5	Memory Leak.	290
9.8.6	NoSQL- versus SQL-Datenbanken	291
9.8.7	Serverseitige versus clientseitige Validierung	291
9.8.8	Session Token.	292
9.8.9	Web-Application-Firewall (WAF).	292
9.9	Fragen zu diesem Kapitel	292
10	Sicherheit für mobile Systeme	295
10.1	Die Risikolage mit mobilen Geräten und Diensten	296
10.2	Organisatorische Sicherheitsmaßnahmen	296
10.3	Technische Sicherheitsmaßnahmen	297
10.3.1	Vollständige Geräteverschlüsselung (Full Device Encryption)	299
10.3.2	Gerätesperren (Lockout).	300
10.3.3	Bildschirm Sperre (Screenlocks).	301
10.3.4	Remote Wipe/Sanitization.	301

10.3.5	Standortdaten (GPS) und Asset Tracking.....	301
10.3.6	Sichere Installationsquellen und Anwendungs- steuerung	302
10.3.7	VPN-Lösungen auf mobilen Geräten	303
10.3.8	Public-Cloud-Dienste auf mobilen Geräten	303
10.4	Anwendungssicherheit bei mobilen Systemen.....	303
10.4.1	Schlüsselverwaltung (Key-Management)	304
10.4.2	Credential-Management	304
10.4.3	Authentifizierung.....	304
10.4.4	Geo-Tagging	305
10.4.5	Verschlüsselung.....	305
10.4.6	Whitelisting von Anwendungen	305
10.4.7	Transitive Trust/Authentifizierung.....	305
10.5	Fragen rund um BYOD.....	306
10.5.1	Dateneigentum (Data Ownership)	306
10.5.2	Zuständigkeit für den Unterhalt (Support Ownership)	307
10.5.3	Antivirus-Management	307
10.5.4	Patch-Management	307
10.5.5	Forensik	308
10.5.6	Privatsphäre und Sicherheit der geschäftlichen Daten	308
10.5.7	Akzeptanz der Benutzer und akzeptable Benutzung	309
10.5.8	Architektur-/Infrastrukturüberlegungen	310
10.5.9	On-Board-Kamera/Video.....	310
10.6	Fragen zu diesem Kapitel	310
11	Den DAU gibt's wirklich – und Sie sind schuld	313
11.1	Klassifizierung von Informationen	314
11.1.1	Die Klassifizierung nach Status	314
11.1.2	Die Klassifizierung nach Risiken	316
11.1.3	Data Loss Prevention	318
11.1.4	Was es zu beachten gilt	319
11.2	Der Datenschutz im internationalen Umfeld	319
11.3	Vom Umgang mit dem Personal	323
11.4	Umgang mit Social Engineering	326
11.4.1	Praktiken, Ziele und Vorgehensweisen von Social Engineers	326
11.4.2	Informationsbeschaffung von OSINT bis Dumpster Diving	327
11.4.3	Pretexting und authentische Geschichten	328

11.4.4	Shoulder surfing.....	330
11.4.5	Tailgating.....	331
11.4.6	Gezielte Beeinflussung und Falschinformation (Influence campaigns)	332
11.4.7	CEO Fraud / Rechnungsbetrug.....	332
11.4.8	Prepending	332
11.4.9	Awareness-Schulungen und Reglements	333
11.5	E-Mail-Sicherheit	333
11.5.1	Secure Multipurpose Internet Mail Extensions (S/MIME)	334
11.5.2	PGP (Pretty Good Privacy).....	335
11.5.3	Schwachstellen	338
11.5.4	Schutz durch einen Mail-Gateway.....	342
11.5.5	Social Media	342
11.6	Daten sichern.....	343
11.6.1	Datensicherung oder Datenarchivierung?	345
11.6.2	Die gesetzlichen Grundlagen.....	346
11.6.3	Das Datensicherungskonzept	348
11.6.4	Methoden der Datensicherung	352
11.6.5	Online-Backup	355
11.6.6	Daten vernichten.....	357
11.7	Sicherheit im Umgang mit Servicepartnern	357
11.8	Fragen zu diesem Kapitel	359
12	Sicherheit für Netzwerke.....	363
12.1	Trennung von IT-Systemen	363
12.1.1	Subnettierung von Netzen.....	364
12.1.2	NAT	366
12.1.3	Network Access Control.....	367
12.2	VLAN	368
12.2.1	Planung und Aufbau von VLANs	368
12.2.2	Vorgehen gegen Risiken bei Switch-Infrastrukturen.....	372
12.2.3	Port Security	373
12.2.4	Flood Guard	373
12.2.5	Spanning-Tree Protocol und Loop Protection	374
12.2.6	Maßnahmen gegen Gefahren in VLANs	375
12.3	TCP/IP-Kernprotokolle	376
12.3.1	Internet Protocol.....	376
12.3.2	Internet Control Message Protocol	376

12.3.3	Transmission Control Protocol	377
12.3.4	User Datagram Protocol (UDP).	378
12.4	Weitere Transport- und Netzwerkprotokolle.	378
12.4.1	Address Resolution Protocol (ARP)	378
12.4.2	Internet Group Management Protocol (IGMP)	379
12.4.3	SLIP und PPP.	379
12.4.4	IP-Version 6	379
12.4.5	Portnummern.	380
12.5	Anwendungen	380
12.5.1	Telnet und SSH	381
12.5.2	FTP und TFTP	381
12.5.3	SCP, SFTP und FTPS.	381
12.5.4	DNS	382
12.5.5	SNMP	383
12.5.6	E-Mail-Protokolle	383
12.5.7	HTTP.	383
12.5.8	SSL und TLS	384
12.5.9	NetBIOS und CIFS.	387
12.5.10	Lightweight Directory Access (LDAP).	387
12.6	Sicherheit in der Cloud	388
12.6.1	Cloud-Computing-Betriebsmodelle	389
12.6.2	Sicherheit in der Wolke	390
12.6.3	Formen des Einsatzes	391
12.7	Fragen zu diesem Kapitel	393
13	Schwachstellen und Attacken	395
13.1	Welches Risiko darf es denn sein?	395
13.2	Angriffe gegen IT-Systeme	397
13.2.1	Denial of Service.	397
13.2.2	Pufferüberlauf	398
13.2.3	Race-Condition	399
13.2.4	Password Guessing und Cracking	399
13.3	Angriffe gegen Anwendungen	401
13.3.1	Directory-Traversal	401
13.3.2	Cross Site Scripting	403
13.3.3	Cross-Site Request Forgery (XSRF).	403
13.3.4	Injection-Varianten	404
13.3.5	Parametermanipulation	405
13.3.6	Transitive Zugriffe	406

13.3.7	Phishing	406
13.3.8	Treibermanipulationen	407
13.4	Angriffe gegen Clients.	407
13.4.1	Drive by Attack	408
13.4.2	Böswillige Add-ons und Applets	408
13.4.3	Local Shared Objects (LSOs)	408
13.4.4	Spam, Spim und Spit	409
13.4.5	Typo squatting bzw. URL-Hijacking	409
13.4.6	URL-Redirection	410
13.4.7	Clickjacking.	410
13.4.8	Domain Hijacking	410
13.4.9	Man in the Browser	410
13.5	Netzwerkangriffe	410
13.5.1	Denial of Service (DoS)	410
13.5.2	Distributed Denial of Service (DDoS)	412
13.5.3	Spoofing	413
13.5.4	Man in the Middle	414
13.5.5	Replay-Angriff.	416
13.5.6	SSL-Downgrading.	417
13.5.7	Session-Hijacking.	417
13.5.8	Brechen von Schlüsseln	418
13.5.9	Backdoor	419
13.6	Angriffe gegen die Public Cloud.	419
13.7	Steganografie	420
13.8	Akteure und ihre Motive	421
13.8.1	Generelle Eigenschaften der verschiedenen Angreifer	422
13.8.2	Von Hüten und Angreifern	423
13.8.3	Staatliche Akteure (State actors)	424
13.8.4	Organisierte Kriminalität (Criminal syndicates)	425
13.8.5	Wirtschaftsspionage (Competitors) und interne Täter	425
13.8.6	Hacktivisten (Hacktivists)	425
13.8.7	Script-Kiddies	426
13.8.8	Die Schatten-IT (Shadow IT)	426
13.8.9	Bug-Bounty	427
13.9	Fragen zu diesem Kapitel	427
14	Der sichere Remote-Zugriff	431
14.1	Virtual Private Network.	431
14.1.1	Site-to-Site-VPN	433

14.1.2	Remote-Access-VPN	434
14.1.3	Soft- und Hardwarelösungen	435
14.2	Remote Access Server	436
14.3	Protokolle für den entfernten Zugriff	436
14.3.1	802.1x	436
14.3.2	RADIUS	438
14.3.3	TACACS, XTACACS und TACACS+	439
14.3.4	L2TP und PPTP	440
14.3.5	IPsec	441
14.3.6	SSL/TLS	447
14.3.7	SSH	447
14.3.8	SRTP	449
14.4	Schwachstellen	449
14.5	Fragen zu diesem Kapitel	450
15	Drahtlose Netzwerke sicher gestalten	453
15.1	Aller WLAN-Standard beginnt mit IEEE 802.11	454
15.1.1	Die frühen IEEE-Standards von 802.11	454
15.1.2	Die Gegenwart heißt Wi-Fi 6	456
15.2	Die Verbindungsaufnahme im WLAN	459
15.2.1	Das Ad-hoc-Netzwerk	459
15.2.2	Das Infrastrukturnetzwerk	460
15.2.3	Erweitertes Infrastrukturnetz	460
15.3	Ein WLAN richtig aufbauen	461
15.3.1	Aufbau der Hardware	461
15.3.2	Konfiguration des drahtlosen Netzwerks	463
15.4	Sicherheit in drahtlosen Verbindungen	465
15.4.1	Wired Equivalent Privacy	466
15.4.2	Von WPA bis WPA3	468
15.4.3	Die Implementierung von 802.1x	470
15.4.4	Das Extensible Authentication Protocol (EAP)	471
15.4.5	WAP (Wireless Application Protocol)	472
15.4.6	Near Field Communication	473
15.5	Grundlegende Sicherheitsmaßnahmen umsetzen	474
15.6	Wireless Intrusion Prevention System	476
15.7	Bluetooth – Risiken und Maßnahmen	476
15.8	Fragen zu diesem Kapitel	478

16	System- und Netzwerküberwachung	481
16.1	Das OSI-Management-Framework	481
16.2	SNMP-Protokolle	484
16.3	Leistungsüberwachung	487
16.4	Das Monitoring von Netzwerken	489
16.5	Monitoring-Programme	490
16.5.1	Der Windows-Netzwerkmonitor	490
16.5.2	Wireshark	492
16.5.3	inSSIDer	495
16.5.4	MRTG bzw. RRDTools	495
16.5.5	Nagios	497
16.6	Proaktive Sicherheit dank SIEM	498
16.7	Kommandozeilenprogramme	500
16.7.1	ipconfig/ip	500
16.7.2	ping	502
16.7.3	ARP	503
16.7.4	tracert/traceroute	504
16.7.5	nslookup	505
16.7.6	netstat	506
16.8	Fragen zu diesem Kapitel	507
17	Brandschutzmauer für das Netzwerk	511
17.1	Damit kein Feuer ausbricht	511
17.2	Personal Firewalls und dedizierte Firewalls	513
17.3	Das Regelwerk einer Firewall	515
17.3.1	Positive Exceptions (Positive Rules)	515
17.3.2	Negative Exceptions (Negative Rules)	515
17.4	Das Konzept der DMZ	516
17.4.1	Trennung Hostsystem von den virtuellen Maschinen	518
17.4.2	Trennung bei WLAN-Infrastrukturen	518
17.4.3	Extranet und Intranet	519
17.5	Nicht jede Firewall leistet dasselbe	519
17.5.1	Wenn einfach auch reicht: Die Paketfilter-Firewall	519
17.5.2	Der nächste Level: Stateful Packet Inspection Firewall	520
17.5.3	Jetzt wird's gründlich: Application Level Gateway	521
17.5.4	Anwendungsbeispiele	523
17.5.5	Unified Threat Management Firewall	525
17.6	Die Angreifer kommen – aber Sie wissen's schon	525

17.7	Unified Threat Management	528
17.8	Fragen zu diesem Kapitel	530
18	Sicherheit überprüfen und analysieren	533
18.1	Informationsbeschaffung	534
18.1.1	Branchen- und Interessensverbände	534
18.1.2	Fachmedien	534
18.1.3	Schwachstelleninformationen	535
18.1.4	Sicherheitskonferenzen	535
18.1.5	Hersteller-Webseiten	535
18.2	Penetration Testing	535
18.2.1	Organisatorische Einbettung	537
18.2.2	Prinzipielle Vorgehensweise	539
18.2.3	Black Box und White Box	543
18.2.4	Security-Scanner	544
18.2.5	Datenbanken für Recherchen nach Sicherheitslücken	547
18.2.6	Passwort-Guesser und -Cracker	547
18.2.7	Paketgeneratoren und Netzwerk-Sniffer	549
18.2.8	Fuzzing	550
18.2.9	Metasploit Framework	550
18.3	Forensik	551
18.3.1	Vorbereitung	552
18.3.2	Sichern von Beweismitteln	553
18.3.3	Beweissicherung nach RFC 3227	554
18.3.4	Schutz und Analyse von Beweismitteln	555
18.3.5	Timeline	557
18.3.6	Data-Carving	557
18.3.7	Suche nach Zeichenketten	558
18.3.8	Nutzung von Hash-Datenbanken	558
18.3.9	Programme und Toolkits	559
18.4	Fragen zu diesem Kapitel	561
19	Wider den Notfall	563
19.1	Was ist denn ein Notfall?	564
19.2	Resilienz dank Fehlertoleranz	565
19.2.1	Aller Anfang ist RAID	566
19.2.2	RAID Level	567
19.2.3	Duplexing	572
19.2.4	Übersicht RAID	572

19.3	Redundante Verbindungen und Systeme	573
19.3.1	Network Loadbalancing	573
19.3.2	Cluster	574
19.4	Notfallvorsorgeplanung	575
19.4.1	Bedrohungsanalyse	575
19.4.2	Von der Bedrohung bis zur Maßnahme	576
19.5	Ein guter Plan beginnt mit einer guten Analyse	577
19.5.1	Ausfallszenarien	577
19.5.2	Impact-Analyse	577
19.6	Methoden der Umsetzung	579
19.6.1	Strategie und Planung	579
19.6.2	Die Rolle des Risiko-Managements	581
19.6.3	Verschiedene Implementierungsansätze	583
19.6.4	Incident-Response-Prozesse und Incident Response Plan	585
19.7	Test und Wartung des Notfallplans	587
19.7.1	Wartung der Disaster Recovery	587
19.7.2	Punktuelle Anpassungen	587
19.7.3	Regelmäßige Überprüfung	588
19.7.4	Merkmale zur Datenwiederherstellung	588
19.8	Fragen zu diesem Kapitel	589
20	Security-Audit.	593
20.1	Grundlagen von Security-Audits	594
20.1.1	Fragestellungen	594
20.1.2	Prinzipielle Vorgehensweise	594
20.1.3	Bestandteile eines Security-Audits	595
20.2	Standards	595
20.2.1	ISO 27001	596
20.2.2	IT-Grundschutz nach BSI	596
20.2.3	Kombination aus ISO 27000 und IT-Grundschutz	597
20.3	Beispiel-Audit Windows Server 2019	597
20.3.1	Nutzung von Sicherheitsvorlagen	598
20.3.2	Einsatz von Kommandos und Scripts	598
20.3.3	Passwortschutz	598
20.3.4	Geräteschutz	598
20.3.5	Sichere Basiskonfiguration	599
20.3.6	Sichere Installation und Bereitstellung	599
20.3.7	Sichere Konfiguration der IIS-Basis-Komponente	599

20.3.8	Sichere Migration auf Windows Server 2019	599
20.3.9	Umgang mit Diensten unter Windows Server	600
20.3.10	Deinstallation nicht benötigter Client-Funktionen	600
20.3.11	Verwendung der Softwareeinschränkungsrichtlinie	600
20.4	Berichtswesen	600
20.4.1	Titelseite	601
20.4.2	Einleitung	601
20.4.3	Management-Summary	601
20.4.4	Ergebnisse der Untersuchung	601
20.4.5	Erforderliche Maßnahmen	602
20.4.6	Anhang	602
20.5	Ergänzende Maßnahmen	603
20.5.1	Logfile-Analyse	603
20.5.2	Echtzeitanalyse von Netzwerkverkehr und Zugriffen	604
20.5.3	Risikoanalyse	604
20.6	Fragen zu diesem Kapitel	605
21	Die CompTIA Security+-Prüfung	607
21.1	Was von Ihnen verlangt wird	608
21.2	Wie Sie sich vorbereiten können	609
21.3	Wie eine Prüfung aussieht	609
21.4	Beispielprüfung zum Examen CompTIA Security+	614
A	Anhänge	633
A.1	Antworten zu den Vorbereitungsfragen	633
A.2	Antworten zu den Kapitelfragen	633
A.3	Antworten zu Fragen der Beispielprüfung	635
A.4	Weiterführende Literatur	636
A.4.1	Nützliche Literatur zum Thema	636
A.4.2	Weiterführende Links zum Thema	637
B	Abkürzungsverzeichnis	639
	Stichwortverzeichnis	653