

Inhaltsverzeichnis

1	Laras Welt.	21
1.1	Das Ziel dieses Buches	22
1.2	Die CompTIA Security+-Zertifizierung	23
1.3	Das Weiterbildungsprogramm von CompTIA	25
1.4	Voraussetzungen für CompTIA Security+	26
1.5	Persönliches	26
2	Sind Sie bereit für CompTIA Security+?	29
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	58
	3.7.3 Die Notfallvorsorge	59
	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 personenbezogene Daten?	70
	4.2.1 Relativer vs. absoluter Ansatz	70
	4.2.2 Was sind personenbezogene Daten nach relativem Ansatz?	71

4.2.3	Anonymisierte und pseudonymisierte Daten.....	71
4.2.4	Anwendungsbeispiele	72
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 Datenverarbeitungssystem ...	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)	81
4.5	Wann ist welches Gesetz anwendbar?	82
4.5.1	Sachlicher Anwendungsbereich	82
4.5.2	Räumlicher Anwendungsbereich	83
4.6	Welche Grundsätze müssen eingehalten werden?	85
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.....	93
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	Auftragsverarbeiter.....	95
4.9.2	Gemeinsame Verantwortliche	96
4.9.3	Verarbeitung im Konzern	96
4.9.4	Datenexporte	97

4.10	Haftungsrisiken bei Datenschutzverletzungen.	98
4.11	Rechtliche Perspektiven von KI-Technologien	101
4.11.1	Anwendbarkeit der KI-Verordnung	102
4.11.2	Die KI-Verordnung der EU und die Risikopyramide	102
4.11.3	KI-Governance	103
4.12	Überblick über die NIS2-Richtlinie und das ISG	105
4.12.1	Warum ist NIS2 für Sie relevant?	106
4.12.2	Was ist in der NIS2 geregelt?	106
4.12.3	Regelung in der Schweiz	108
4.13	Fragen zu diesem Kapitel	109
5	Verschlüsselungstechnologie	113
5.1	Grundlagen der Kryptografie	114
5.1.1	Einige Grundbegriffe	115
5.1.2	One-Time-Pad.	116
5.1.3	Diffusion und Konfusion.	117
5.1.4	Blockverschlüsselung.	117
5.1.5	Stromverschlüsselung	118
5.2	Symmetrische Verschlüsselung	120
5.2.1	DES	120
5.2.2	3DES	121
5.2.3	AES	121
5.2.4	Blowfish	122
5.2.5	Twofish	122
5.2.6	RC4	122
5.3	Asymmetrische Verschlüsselung	123
5.3.1	RSA	124
5.3.2	Diffie-Hellman	124
5.3.3	ECC	125
5.3.4	Perfect Forward Secrecy (PFS)	126
5.3.5	Die Zukunft der Quanten	127
5.4	Hash-Verfahren	127
5.4.1	MD4 und MD5	128
5.4.2	SHA.	129
5.4.3	RIPEMD	130
5.4.4	HMAC.	130
5.4.5	Hash-Verfahren mit symmetrischer Verschlüsselung	130
5.4.6	Digitale Signaturen	131
5.4.7	Hybride Verschlüsselung.	132
5.5	Drei Status digitaler Daten	132
5.5.1	Data-in-transit.	133
5.5.2	Data-at-rest	133
5.5.3	Data-in-use	133

- 5.6 Bekannte Angriffe gegen die Verschlüsselung 134
 - 5.6.1 Cipher-text-only-Angriff 134
 - 5.6.2 Known/Chosen-plain-text-Angriff 134
 - 5.6.3 Schwache Verschlüsselung/Implementierung 135
 - 5.6.4 Probleme mit Zertifikaten 135
- 5.7 PKI in Theorie und Praxis 135
 - 5.7.1 Aufbau einer hierarchischen PKI 137
 - 5.7.2 TLS-Zertifikate X.509 Version 3 138
 - 5.7.3 Zertifikatstypen 139
 - 5.7.4 Zurückziehen von Zertifikaten 141
 - 5.7.5 Hinterlegung von Schlüsseln 142
 - 5.7.6 Schlüsselverwaltungssystem (Key Management System) ... 143
 - 5.7.7 Aufsetzen einer hierarchischen PKI 143
- 5.8 Fragen zu diesem Kapitel 144

- 6 Die Geschichte mit der Identität 147
 - 6.1 Identitäten und deren Rechte 147
 - 6.1.1 Zuweisung von Rechten 147
 - 6.1.2 Rollen 149
 - 6.1.3 Single Sign On 149
 - 6.2 Authentifizierungsmethoden 150
 - 6.2.1 Benutzername und Kennwort 150
 - 6.2.2 Passkeys 151
 - 6.2.3 Token 152
 - 6.2.4 Zertifikate 153
 - 6.2.5 Biometrie 154
 - 6.2.6 Benutzername, Kennwort und Smartcard 156
 - 6.2.7 Tokenization 156
 - 6.2.8 Wechselseitige Authentifizierung 157
 - 6.2.9 Das Zero-Trust-Konzept 158
 - 6.2.10 Privileged Access Management (PAM) 161
 - 6.3 Zugriffssteuerungsmodelle 162
 - 6.3.1 Mandatory Access Control (MAC) 162
 - 6.3.2 Discretionary Access Control (DAC) 163
 - 6.3.3 Role-Based Access Control (RBAC) 164
 - 6.3.4 ABAC – Attributbasiertes Zugriffssystem 166
 - 6.3.5 Principle of Least Privileges 166
 - 6.3.6 Need-to-know-Prinzip 167
 - 6.4 Protokolle für die Authentifizierung 167
 - 6.4.1 Kerberos 167
 - 6.4.2 PAP 168
 - 6.4.3 CHAP 169
 - 6.4.4 NTLM 169
 - 6.4.5 Die Non-Repudiation 170

6.5	Vom Umgang mit Passwörtern	170
6.6	Blockchain und Kryptogeld.....	171
6.7	Fragen zu diesem Kapitel	173
7	Physische Sicherheit	175
7.1	Zutrittsregelungen.....	176
7.1.1	Das Zonenkonzept.....	177
7.1.2	Schlüsselsysteme	178
7.1.3	Badges und Keycards	178
7.1.4	Biometrische Erkennungssysteme	179
7.1.5	Zutrittsschleusen	180
7.1.6	Videoüberwachung.....	181
7.1.7	Multiple Systeme	182
7.2	Bauschutz.....	182
7.2.1	Einbruchsschutz.....	182
7.2.2	Hochwasserschutz	183
7.2.3	Brandschutz	184
7.2.4	Klimatisierung und Kühlung	185
7.3	Elektrostatische Entladung	187
7.4	Stromversorgung.....	188
7.4.1	USV	188
7.4.2	Notstromgruppen.....	190
7.4.3	Einsatzszenarien.....	191
7.4.4	Rotationsenergiestromversorgungen	193
7.4.5	Ein Wort zu EMP	193
7.5	Feuchtigkeit und Temperatur.....	193
7.6	Fragen zu diesem Kapitel	195
8	Im Angesicht des Feindes	199
8.1	Malware ist tatsächlich böse	200
8.1.1	Die Problematik von Malware.....	205
8.1.2	Viren und ihre Unterarten.....	206
8.1.3	Wie aus Trojanischen Pferden böse Trojaner wurden	209
8.1.4	Backdoor	213
8.1.5	Logische Bomben.....	214
8.1.6	Würmer.....	214
8.1.7	Ransomware	215
8.1.8	Krypto-Malware (Cryptomalware)	218
8.1.9	Fileless Malware	218
8.1.10	Hoaxes.....	218
8.2	Angriffe mittels Social Engineering.....	219
8.2.1	Phishing	219
8.2.2	Vishing und Smishing	224

- 8.2.3 Spear Phishing 226
 - 8.2.4 Pharming..... 226
 - 8.2.5 Drive-by-Pharming..... 227
 - 8.2.6 Doxing..... 227
 - 8.3 Angriffe gegen IT-Systeme 227
 - 8.3.1 Drei Bedingungen für einen funktionierenden Angriff mit Schadcode..... 228
 - 8.3.2 Exploits und Exploit-Kits 228
 - 8.3.3 Darknet und Darkweb 231
 - 8.3.4 Malwaretising 231
 - 8.3.5 Watering-Hole-Attacke..... 231
 - 8.3.6 Malware Dropper und Malware-Scripts 232
 - 8.3.7 RAT (Remote Access Tool/Remote Access Trojan) 232
 - 8.3.8 Keylogger..... 233
 - 8.3.9 Post Exploitation..... 234
 - 8.4 Gefahren für die Nutzung mobiler Geräte und Dienste..... 236
 - 8.5 APT – Advanced Persistent Threats..... 238
 - 8.5.1 Stuxnet..... 238
 - 8.5.2 Carbanak 239
 - 8.6 Advanced Threats..... 240
 - 8.6.1 Evasion-Techniken 240
 - 8.6.2 Pass-the-Hash-Angriffe (PtH) 242
 - 8.6.3 Kaltstartattacke (Cold Boot Attack) 243
 - 8.6.4 Physische RAM-Manipulation über DMA (FireWire-Hack) 243
 - 8.6.5 Human Interface Device Attack (Teensy USB HID Attack) 244
 - 8.6.6 BAD-USB-Angriff..... 244
 - 8.6.7 Bösesartiges USB-Kabel..... 245
 - 8.6.8 SSL-Stripping-Angriff..... 245
 - 8.6.9 Angriff über Wireless-Mäuse..... 246
 - 8.7 Angriffe in Wireless-Netzwerken 247
 - 8.7.1 Spoofing in Wireless-Netzwerken..... 247
 - 8.7.2 Sniffing in drahtlosen Netzwerken..... 248
 - 8.7.3 DNS-Tunneling in Public WLANs 249
 - 8.7.4 Rogue Access Point/Evil Twin..... 250
 - 8.7.5 Attacken auf die WLAN-Verschlüsselung..... 251
 - 8.7.6 Verschlüsselung brechen mit WPS-Attacken..... 252
 - 8.7.7 Denial-of-Service-Angriffe im WLAN 253
 - 8.7.8 Angriffe auf NFC-Technologien 254
 - 8.7.9 Angriffe auf Keycards..... 254
 - 8.8 Moderne Angriffsformen 255
 - 8.8.1 Angriffe mittels Drohnen..... 256
 - 8.8.2 Angriffe mittels Living-off-the-Land 256

- 8.8.3 Verwundbare Anwendungen nachladen 257
 - 8.8.4 Angriffe auf Application Programming Interface (API) 257
 - 8.8.5 Gefahren durch künstliche Intelligenz (KI) 257
 - 8.8.6 Böswilliges Prompt Engineering/GPT-Jailbreaking 259
 - 8.8.7 Das Internet of Things..... 260
- 8.9 Fragen zu diesem Kapitel 262
- 9 **Systemsicherheit realisieren**..... 265
- 9.1 Konfigurationsmanagement..... 266
- 9.2 Das Arbeiten mit Richtlinien 268
- 9.3 Grundlagen der Systemhärtung..... 270
 - 9.3.1 Schutz von Gehäuse und BIOS..... 272
 - 9.3.2 Sicherheit durch TPM 274
 - 9.3.3 Secure Enclave 275
 - 9.3.4 Full Disk Encryption 275
 - 9.3.5 Softwarebasierte Laufwerksverschlüsselung 275
 - 9.3.6 Hardware-Sicherheitsmodul 276
 - 9.3.7 Software-Firewall (Host-based Firewall)..... 276
 - 9.3.8 Systemintegrität 277
 - 9.3.9 Überlegungen bei der Virtualisierung 278
- 9.4 Embedded-Systeme und Industriesysteme 280
- 9.5 Softwareaktualisierung ist kein Luxus 285
 - 9.5.1 Vom Hotfix zum Upgrade..... 287
 - 9.5.2 Problemkategorien..... 287
 - 9.5.3 Maintenance-Produkte..... 288
 - 9.5.4 Die Bedeutung des Patch- und Update-Managements 290
 - 9.5.5 Entfernen Sie, was Sie nicht brauchen..... 291
- 9.6 Malware bekämpfen 292
 - 9.6.1 End Point Protection am Client..... 294
 - 9.6.2 Reputationslösungen 296
 - 9.6.3 Aktivitätsüberwachung HIPS/HIDS 297
 - 9.6.4 Online-Virens Scanner – Webantivirus-NIPS..... 297
 - 9.6.5 Sensibilisierung der Mitarbeitenden 297
 - 9.6.6 Suchen und Entfernen von Viren 300
 - 9.6.7 Virenschutzkonzept..... 301
 - 9.6.8 Testen von Installationen..... 302
 - 9.6.9 Sicher und vertrauenswürdig ist gut..... 303
- 9.7 Advanced Threat Protection 304
 - 9.7.1 Explizites Applikations-Allowlisting versus -Denylisting ... 305
 - 9.7.2 Explizites Allowlisting auf Firewalls 306
 - 9.7.3 Erweiterter Exploit-Schutz 307
 - 9.7.4 Virtualisierung von Anwendungen..... 308
 - 9.7.5 Schutz vor HID-Angriffen und BAD-USB..... 309
 - 9.7.6 Geschlossene Systeme 311

9.7.7	Schutz vor SSL-Stripping-Angriffen	311
9.7.8	Schutz vor Angriffen über drahtlose Mäuse.	314
9.7.9	Security- und Threat Intelligence	314
9.8	Anwendungssicherheit	315
9.8.1	Lifecycle-Management/DevOps.	315
9.8.2	Sichere Codierungskonzepte	316
9.8.3	Anwendungsfälle von Automatisierung und Skripting.	316
9.8.4	Input Validation	317
9.8.5	Fehler- und Ausnahmebehandlung	317
9.8.6	Memory Leak.	318
9.8.7	NoSQL- versus SQL-Datenbanken	318
9.8.8	Serverseitige versus clientseitige Validierung	318
9.8.9	Session Token.	319
9.8.10	Web-Application-Firewall (WAF).	319
9.9	Fragen zu diesem Kapitel	320
10	Sicherheit für mobile Systeme	323
10.1	Die Risikolage mit mobilen Geräten und Diensten	324
10.2	Organisatorische Sicherheitsmaßnahmen	325
10.3	Technische Sicherheitsmaßnahmen	325
10.3.1	Vollständige Geräteverschlüsselung (Full Device Encryption)	328
10.3.2	Gerätesperren (Lockout).	328
10.3.3	Bildschirmsperre (Screenlocks).	329
10.3.4	Remote Wipe/Sanitization.	330
10.3.5	Standortdaten (GPS) und Asset Tracking.	330
10.3.6	Sichere Installationsquellen und Anwendungssteuerung.	331
10.3.7	VPN-Lösungen auf mobilen Geräten	331
10.3.8	Public-Cloud-Dienste auf mobilen Geräten	332
10.4	Anwendungssicherheit bei mobilen Systemen	332
10.4.1	Schlüsselverwaltung (Key-Management)	332
10.4.2	Credential-Management.	333
10.4.3	Geo-Tagging	333
10.4.4	Allowlisting von Anwendungen	333
10.4.5	Transitive Trust/Authentifizierung.	333
10.5	Fragen rund um BYOD.	334
10.5.1	Dateneigentum (Data Ownership)	334
10.5.2	Zuständigkeit für den Unterhalt (Support Ownership).	335
10.5.3	Antivirus-Management	335
10.5.4	Patch-Management.	335
10.5.5	Forensik.	336
10.5.6	Privatsphäre und Sicherheit der geschäftlichen Daten	336
10.5.7	Akzeptanz der Benutzer und akzeptable Benutzung	337
10.5.8	Architektur-/Infrastrukturüberlegungen	338

10.5.9	On-Board-Kamera/Video	338
10.6	Fragen zu diesem Kapitel	338
11	Den DAU gibt's wirklich – und Sie sind schuld	341
11.1	Klassifizierung von Informationen	342
11.1.1	Die Klassifizierung nach Status	343
11.1.2	Die Klassifizierung nach Risiken	344
11.1.3	Data Loss Prevention	346
11.1.4	Was es zu beachten gilt	347
11.2	Der Datenschutz im internationalen Umfeld	348
11.2.1	Compliance	349
11.2.2	Governance	350
11.3	Vom Umgang mit dem Personal	352
11.4	Umgang mit Social Engineering	354
11.4.1	Praktiken, Ziele und Vorgehensweisen von Social Engineers	355
11.4.2	Informationsbeschaffung von OSINT bis Dumpster Diving	356
11.4.3	Pretexting und authentische Geschichten	357
11.4.4	Shoulder Surfing	359
11.4.5	Tailgating	359
11.4.6	Gezielte Beeinflussung und Falschinformation (Influence Campaigns)	360
11.4.7	CEO Fraud/Rechnungsbetrug	360
11.4.8	Prepending	361
11.4.9	Awareness-Schulungen und Reglements	361
11.5	E-Mail-Sicherheit	362
11.5.1	Secure Multipurpose Internet Mail Extensions (S/MIME)	363
11.5.2	PGP (Pretty Good Privacy)	363
11.5.3	Schwachstellen	366
11.5.4	Schutz durch einen Mail-Gateway	370
11.5.5	Social Media	371
11.6	Daten sichern	372
11.6.1	Datensicherung oder Datenarchivierung?	373
11.6.2	Die gesetzlichen Grundlagen	374
11.6.3	Das Datensicherungskonzept	376
11.6.4	Methoden der Datensicherung	381
11.6.5	Online-Backup	384
11.6.6	Daten vernichten	385
11.7	Daten technisch schützen	386
11.7.1	Geografische Einschränkungen (Geographic restrictions)	386
11.7.2	Datenmaskierung und Tokenisierung	387
11.7.3	Verschleierung (Obfuscation)	387

11.8	Sicherheit im Umgang mit Servicepartnern	387
11.9	Fragen zu diesem Kapitel	390
12	Sicherheit für Netzwerke	393
12.1	Trennung von IT-Systemen	393
12.1.1	Subnettierung von Netzen	394
12.1.2	NAT	396
12.1.3	Network Access Control	397
12.2	VLAN	398
12.2.1	Planung und Aufbau von VLANs	398
12.2.2	Vorgehen gegen Risiken bei Switch-Infrastrukturen	402
12.2.3	Port Security	403
12.2.4	Flood Guard	404
12.2.5	Spanning-Tree Protocol und Loop Protection	404
12.2.6	Maßnahmen gegen Gefahren in VLANs	405
12.3	TCP/IP-Kernprotokolle	406
12.3.1	Internet Protocol	406
12.3.2	Internet Control Message Protocol	406
12.3.3	Transmission Control Protocol	407
12.3.4	User Datagram Protocol (UDP)	408
12.4	Weitere Transport- und Netzwerkprotokolle	409
12.4.1	Address Resolution Protocol (ARP)	409
12.4.2	Internet Group Management Protocol (IGMP)	409
12.4.3	SLIP und PPP	409
12.4.4	IP-Version 6	410
12.4.5	Portnummern	410
12.5	Anwendungen	411
12.5.1	Telnet und SSH	411
12.5.2	FTP und TFTP	411
12.5.3	SCP, SFTP und FTPS	412
12.5.4	DNS	412
12.5.5	SNMP	413
12.5.6	E-Mail-Protokolle	413
12.5.7	HTTP	414
12.5.8	SSL und TLS	415
12.5.9	NetBIOS und CIFS	418
12.5.10	Lightweight Directory Access (LDAP)	419
12.6	Sicherheit in der Cloud	419
12.6.1	Cloud-Computing-Betriebsmodelle	420
12.6.2	Sicherheit in der Wolke	421
12.6.3	Formen des Einsatzes	422
12.7	Fragen zu diesem Kapitel	424

13	Schwachstellen und Attacken	427
13.1	Welches Risiko darf es denn sein?	427
13.2	Angriffe gegen IT-Systeme	429
13.2.1	Dateibasierte Angriffe (file-based)	429
13.2.2	Bildbasierte Angriffe (image-based)	430
13.2.3	Memory Injection (Exploit)	430
13.2.4	Virtualisierung (Resource Reuse)	432
13.2.5	Denial of Service	432
13.2.6	Race Condition	434
13.2.7	Password Guessing und Cracking	434
13.3	Angriffe gegen Anwendungen	436
13.3.1	Directory-Traversal	436
13.3.2	Cross Site Scripting	438
13.3.3	Cross-Site Request Forgery (XSRF)	439
13.3.4	Injection-Varianten	439
13.3.5	Parametermanipulation	440
13.3.6	Transitive Zugriffe	441
13.3.7	Phishing	441
13.3.8	Treibermanipulationen	442
13.4	Angriffe gegen Clients	443
13.4.1	Drive-by Attack	443
13.4.2	Böswillige Add-ons und Applets	443
13.4.3	Local Shared Objects (LSOs)	444
13.4.4	Spam, Spim und Spit	444
13.4.5	Typo squatting bzw. URL-Hijacking	445
13.4.6	URL-Redirection	445
13.4.7	Clickjacking	445
13.4.8	Domain Hijacking	445
13.4.9	Man in the Browser	445
13.5	Netzwerkangriffe	446
13.5.1	Denial of Service (DoS)	446
13.5.2	Distributed Denial of Service (DDoS)	447
13.5.3	Spoofing	448
13.5.4	Man in the Middle	449
13.5.5	Replay-Angriff	452
13.5.6	SSL-Downgrading	452
13.5.7	Session-Hijacking	453
13.5.8	Brechen von Schlüsseln	454
13.5.9	Backdoor	454
13.6	Angriffe gegen die Public Cloud	455
13.7	Steganografie	456
13.8	Akteure und ihre Motive	457
13.8.1	Generelle Eigenschaften der verschiedenen Angreifer	457

13.8.2	Von Hüten und Angreifern	459
13.8.3	Staatliche Akteure (State actors)	460
13.8.4	Organisierte Kriminalität (Criminal syndicates)	460
13.8.5	Wirtschaftsspionage (Competitors) und interne Täter	461
13.8.6	Hacktivisten (Hacktivists)	461
13.8.7	Script-Kiddies	462
13.8.8	Die Schatten-IT (Shadow IT)	462
13.8.9	Lieferketten (Supply-Chain-Attacke)	463
13.8.10	Bug-Bounty	463
13.9	Fragen zu diesem Kapitel	464
14	Der sichere Remote-Zugriff	467
14.1	Virtual Private Network	467
14.1.1	Site-to-Site-VPN	469
14.1.2	Remote-Access-VPN	470
14.1.3	Soft- und Hardwarelösungen	471
14.2	Remote Access Server	472
14.3	Protokolle für den entfernten Zugriff	472
14.3.1	802.1x	472
14.3.2	RADIUS	474
14.3.3	TACACS, XTACACS und TACACS+	475
14.3.4	L2TP und PPTP	476
14.3.5	IPsec	477
14.3.6	SSL/TLS	483
14.3.7	SSH	484
14.3.8	SRTP	485
14.4	Schwachstellen	485
14.4.1	Man in the Middle	486
14.4.2	Identitäts-Spoofing	486
14.4.3	Botnetze (Botnet)	486
14.5	Fragen zu diesem Kapitel	487
15	Drahtlose Netzwerke sicher gestalten	489
15.1	Aller WLAN-Standard beginnt mit IEEE 802.11	490
15.1.1	Die frühen IEEE-Standards von 802.11	490
15.1.2	Die Gegenwart heißt Wi-Fi 6	492
15.2	Die Verbindungsaufnahme im WLAN	496
15.2.1	Das Ad-hoc-Netzwerk	496
15.2.2	Das Infrastrukturnetzwerk	496
15.2.3	Erweitertes Infrastrukturnetz	497
15.3	Ein WLAN richtig aufbauen	498
15.3.1	Aufbau der Hardware	498
15.3.2	Konfiguration des drahtlosen Netzwerks	500

15.4 Sicherheit in drahtlosen Verbindungen. 502

15.4.1 Wired Equivalent Privacy 502

15.4.2 Von WPA bis WPA3. 505

15.4.3 Die Implementierung von 802.1x 506

15.4.4 Das Extensible Authentication Protocol (EAP). 507

15.4.5 WAP (Wireless Application Protocol) 508

15.4.6 Near Field Communication 509

15.5 Grundlegende Sicherheitsmaßnahmen umsetzen. 510

15.6 Wireless Intrusion Prevention System 512

15.7 Bluetooth – Risiken und Maßnahmen 513

15.8 Fragen zu diesem Kapitel 515

16 System- und Netzwerküberwachung 519

16.1 Das OSI-Management-Framework 519

16.2 SNMP-Protokolle. 522

16.3 Leistungsüberwachung. 525

16.4 Das Monitoring von Netzwerken 527

16.5 Monitoring-Programme 528

16.5.1 Der Windows-Netzwerkmonitor 528

16.5.2 Wireshark 530

16.5.3 inSSIDer 533

16.5.4 MRTG bzw. RRDTools. 534

16.5.5 Nagios 535

16.6 Proaktive Sicherheit dank SIEM. 536

16.7 Kommandozeilenprogramme. 538

16.7.1 ipconfig/ip. 538

16.7.2 ping 540

16.7.3 ARP 541

16.7.4 tracert/traceroute 542

16.7.5 nslookup 543

16.7.6 netstat 544

16.8 Fragen zu diesem Kapitel 545

17 Brandschutzmauer für das Netzwerk 549

17.1 Damit kein Feuer ausbricht 549

17.2 Personal Firewalls und dedizierte Firewalls 551

17.3 Das Regelwerk einer Firewall 553

17.3.1 Positive Exceptions (Positive Rules) 553

17.3.2 Negative Exceptions (Negative Rules). 553

17.4 Das Konzept der DMZ 554

17.4.1 Trennung Hostsystem von den virtuellen Maschinen 556

17.4.2 Trennung bei WLAN-Infrastrukturen 556

17.4.3 Extranet und Intranet. 557

17.5	Nicht jede Firewall leistet dasselbe	557
17.5.1	Wenn einfach auch reicht: Die Paketfilter-Firewall	557
17.5.2	Der nächste Level: Stateful Packet Inspection Firewall	558
17.5.3	Jetzt wird's gründlich: Application Level Gateway	559
17.5.4	Das Konzept der Next-generation Firewalls	561
17.5.5	Anwendungsbeispiele	562
17.6	Die Angreifer kommen – aber Sie wissen's schon	563
17.7	Unified Threat Management	566
17.8	Fragen zu diesem Kapitel	568
18	Sicherheit überprüfen und analysieren	571
18.1	Informationsbeschaffung	572
18.1.1	Branchen- und Interessensverbände	572
18.1.2	Fachmedien	573
18.1.3	Schwachstelleninformationen	573
18.1.4	Sicherheitskonferenzen	574
18.1.5	Hersteller-Webseiten	574
18.2	Verschiedene Kontrollarten	574
18.2.1	Präventive Kontrollen	574
18.2.2	Abschreckende Maßnahmen	575
18.2.3	Aufdeckende Maßnahmen	575
18.2.4	Korrektive Maßnahmen	575
18.2.5	Kompensierende Maßnahmen	576
18.2.6	Richtlinien setzen	577
18.3	Die Bedeutung des Change-Managements	577
18.4	Auch Risiken wollen verwaltet werden	579
18.5	Penetration Testing	582
18.5.1	Organisatorische Einbettung	583
18.5.2	Prinzipielle Vorgehensweise	585
18.5.3	Black Box und White Box	589
18.5.4	Security-Scanner	589
18.5.5	Datenbanken für Recherchen nach Sicherheitslücken	593
18.5.6	Passwort-Guesser und -Cracker	593
18.5.7	Paketgeneratoren und Netzwerk-Sniffer	595
18.5.8	Fuzzing	596
18.5.9	Metasploit Framework	596
18.6	Forensik	597
18.6.1	Vorbereitung	598
18.6.2	Sichern von Beweismitteln	599
18.6.3	Beweissicherung nach RFC 3227	600
18.6.4	Schutz und Analyse von Beweismitteln	600
18.6.5	Timeline	603
18.6.6	Data-Carving	603

18.6.7	Suche nach Zeichenketten.	604
18.6.8	Nutzung von Hash-Datenbanken	604
18.6.9	Programme und Toolkits.	605
18.7	Fragen zu diesem Kapitel	606
19	Wider den Notfall	609
19.1	Was ist denn ein Notfall?	610
19.2	Resilienz dank Fehlertoleranz	611
19.2.1	Aller Anfang ist RAID	612
19.2.2	RAID Level	613
19.2.3	Duplexing	618
19.2.4	Übersicht RAID	618
19.2.5	Die Zukunft nach RAID	619
19.3	Redundante Verbindungen und Systeme	621
19.3.1	Network Loadbalancing	622
19.3.2	Cluster.	622
19.4	Notfallvorsorgeplanung.	623
19.4.1	Bedrohungsanalyse	623
19.4.2	Von der Bedrohung bis zur Maßnahme.	624
19.5	Ein guter Plan beginnt mit einer guten Analyse.	625
19.5.1	Ausfallszenarien.	625
19.5.2	Impact-Analyse.	626
19.6	Methoden der Umsetzung	628
19.6.1	Strategie und Planung	628
19.6.2	Die Rolle des Risiko-Managements	629
19.6.3	Verschiedene Implementierungsansätze.	629
19.6.4	Incident-Response-Prozesse und Incident Response Plan	632
19.7	Test und Wartung des Notfallplans	633
19.7.1	Wartung der Disaster Recovery.	634
19.7.2	Punktuelle Anpassungen.	634
19.7.3	Regelmäßige Überprüfung	634
19.7.4	Merkmale zur Datenwiederherstellung	635
19.8	Fragen zu diesem Kapitel	636
20	Security-Audit	639
20.1	Grundlagen von Security-Audits	640
20.1.1	Fragestellungen	640
20.1.2	Prinzipielle Vorgehensweise	640
20.1.3	Bestandteile eines Security-Audits	641
20.2	Standards	641
20.2.1	ISO 27001	642
20.2.2	IT-Grundschutz nach BSI	642

- 20.3 Beispiel-Audit Windows Server 2022. 643
 - 20.3.1 Nutzung von Sicherheitsvorlagen 644
 - 20.3.2 Einsatz von Kommandos und Scripts 644
 - 20.3.3 Passwortschutz 644
 - 20.3.4 Geräteschutz 644
 - 20.3.5 Sichere Basiskonfiguration 645
 - 20.3.6 Sichere Installation und Bereitstellung. 645
 - 20.3.7 Sichere Konfiguration der IIS-Basis-Komponente. 645
 - 20.3.8 Sichere Migration auf Windows Server 2022. 645
 - 20.3.9 Umgang mit Diensten unter Windows Server. 646
 - 20.3.10 Deinstallation nicht benötigter Client-Funktionen 646
 - 20.3.11 Verwendung der Softwareeinschränkungsrichtlinie 646
- 20.4 Berichtswesen 646
 - 20.4.1 Titelseite 647
 - 20.4.2 Einleitung 647
 - 20.4.3 Management-Summary 647
 - 20.4.4 Ergebnisse der Untersuchung. 647
 - 20.4.5 Erforderliche Maßnahmen. 648
 - 20.4.6 Anhang 649
- 20.5 Ergänzende Maßnahmen 649
 - 20.5.1 Logfile-Analyse 649
 - 20.5.2 Echtzeitanalyse von Netzwerkverkehr und Zugriffen 650
 - 20.5.3 Risikoanalyse. 651
- 20.6 Fragen zu diesem Kapitel 651

- 21 Die CompTIA Security+-Prüfung. 655
 - 21.1 Was von Ihnen verlangt wird 656
 - 21.2 Wie Sie sich vorbereiten können 657
 - 21.3 Wie eine Prüfung aussieht 657
 - 21.4 Beispielprüfung zum Examen CompTIA Security+ 662

- A Anhänge 685
 - A.1 Antworten zu den Vorbereitungsfragen. 685
 - A.2 Antworten zu den Kapitelfragen. 685
 - A.3 Antworten zu Fragen der Beispielprüfung 687
 - A.4 Weiterführende Literatur 688

- B Abkürzungsverzeichnis. 691

- Stichwortverzeichnis 705