

Mathias Gut | Markus Kammermann

# CompTIA Security+

IT-Sicherheit verständlich erläutert

Die umfassende Prüfungsvorbereitung  
zur CompTIA-Prüfung SY0-701

5. Auflage



mitp

# Inhaltsverzeichnis

1	<b>Laras Welt</b> . . . . .	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	<b>Sind Sie bereit für CompTIA Security+?</b> . . . . .	29
3	<b>Wo liegt denn das Problem?</b> . . . . .	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	<b>Rechtliche Grundlagen</b> . . . . .	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
<b>5</b>	<b>Verschlüsselungstechnologie . . . . .</b>	<b>113</b>
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
<b>6</b>	<b>Die Geschichte mit der Identität.</b> .....	<b>147</b>
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
<b>7</b>	<b>Physische Sicherheit</b> .....	<b>175</b>
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	Videüberwachung. ....	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
<b>8</b>	<b>Im Angesicht des Feindes</b> .....	<b>199</b>
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	Bösartiges 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
<b>9</b>	<b>Systemsicherheit realisieren . . . . .</b>	<b>265</b>
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
<b>10</b>	<b>Sicherheit für mobile Systeme . . . . .</b>	<b>323</b>
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	Bildschirm Sperre (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
<b>11</b>	<b>Den DAU gibt's wirklich – und Sie sind schuld . . . . .</b>	<b>341</b>
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
<b>12</b>	<b>Sicherheit für Netzwerke .....</b>	<b>393</b>
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

<b>13</b>	<b>Schwachstellen und Attacken</b> . . . . .	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
<b>14</b>	<b>Der sichere Remote-Zugriff</b> . . . . .	<b>467</b>
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
<b>15</b>	<b>Drahtlose Netzwerke sicher gestalten</b> . . . . .	<b>489</b>
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
<b>16</b>	<b>System- und Netzwerküberwachung</b> . . . . .	<b>519</b>
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
<b>17</b>	<b>Brandschutzmauer für das Netzwerk</b> . . . . .	<b>549</b>
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
<b>18</b>	<b>Sicherheit überprüfen und analysieren . . . . .</b>	<b>571</b>
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
<b>19</b>	<b>Wider den Notfall</b> . . . . .	<b>609</b>
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
<b>20</b>	<b>Security-Audit</b> . . . . .	<b>639</b>
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
<b>21</b>	<b>Die CompTIA Security+-Prüfung. . . . .</b>	<b>655</b>
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
<b>A</b>	<b>Anhänge . . . . .</b>	<b>685</b>
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>B</b>	<b>Abkürzungsverzeichnis. . . . .</b>	<b>691</b>
	<b>Stichwortverzeichnis . . . . .</b>	<b>705</b>

# Laras Welt

*Guten Tag, ich bin Lara aus Neustadt. Ich arbeite bei der lokalen Agentur der Nixsicura-Versicherungen und möchte euch einen Einblick in meinen beruflichen Alltag und den Umgang mit Informatik und Sicherheit geben.*

*Morgens bin ich jeweils die Erste, die anfängt, also schließe ich die Agentur und alle Büros auf und schalte über meine App die Kaffeemaschine ein. Anschließend gehe ich an meinen Computer und starte diesen, damit ich Zugriff auf die Daten und das Internet habe. Am Morgen genieße ich die Ruhe, da kann ich alle Mails lesen und noch ein wenig im Internet surfen und Videos schauen, was auf der Welt Interessantes geschieht. Allerdings muss ich in letzter Zeit oft darüber nachdenken, ob eine bestimmte Mail jetzt wirklich von einem Kunden oder einem Vertragspartner kommt oder nicht. Dann klicke ich zur Sicherheit jeweils auf den Anhang, dort steht ja, was ich wissen muss. Dabei hat mein Antivirenprogramm jetzt zweimal einen solchen Anhang gelöscht, dabei ich wollte doch nur nachsehen, was drin steht. Das fand ich dann doch unfair, zwei Mails waren doch sogar Bewerbungen für die neue Kundenberaterin, das muss ich doch lesen können!*

*So gegen acht Uhr kommen dann die beiden Kollegen und die Chefin, und der Arbeitstag beginnt: Kunden bedienen, Links mit den eingegangenen Verträgen anklicken und öffnen, Verträge zur Unterschrift weiterleiten, Policen in der Cloud am richtigen Ort ablegen oder auch mal Reklamationen bearbeiten – was alles so anfällt in einer Versicherungsagentur. Die Daten sind für mich zum Glück alle zugänglich, so kann ich auch der Chefin mal bei einem Vertrag unter die Arme greifen oder Arbeiten meiner Kollegen ordnen und korrekt ablegen, die gerne alles einfach irgendwo speichern. Zur Sicherheit haben wir auch alle unsere Kennwörter auf einer Liste notiert, dann können wir einander problemlos helfen.*

*Seit Kurzem kann ich für die Ausarbeitung von Texten auch das Programm Brainfree nutzen. Dieses arbeitet mit künstlicher Intelligenz und hilft mir sehr. So kann ich einen ausführlichen Schadensbericht mit allen Daten einfach hochladen und dem Programm sagen, es soll mir eine Zusammenfassung schreiben. Mit ein paar Kundenangaben dazu kann es mir sogar ein Antwortschreiben vorschlagen. Und das alles gratis und direkt im Internet, ich finde das super praktisch.*

*Über Mittag gehen wir meist alle zusammen essen. Wir kennen da ein kleines Restaurant in der Nähe, das ist über Mittag zwar gut gefüllt, aber für uns halten sie immer einen Tisch frei. Das Büro schließen wir natürlich ab, die Systeme lassen wir laufen, damit wir nach der Pause nicht so viel Zeit verlieren, bis wir wieder arbeiten können.*

*Am Mittagstisch kann man schon mal was Privates bereden, aber auch aktuelle Vorgänge vom Vormittag, interessante Schadensfälle oder die neuesten Ideen unserer Kunden können wir hier ebenso besprechen. Das kann auch mal laut werden, aber meistens ist es einfach interessant – der Mittag ist immer schnell vorbei.*

*Am Nachmittag geht's wieder zurück in die Agentur. Während die beiden Kollegen dann öfter draußen bei den Kunden sind, bleibe ich in der Agentur für die Administration zuständig und erledige Telefonate oder bediene Kunden, die sich bei mir an den Tisch setzen, um mit mir ihre Sorgen oder Anliegen zu besprechen. Erst letztlich hat mich ein potenzieller Kunde sehr genau über die Vorgänge in unserer Agentur ausgefragt, da konnte ich mal zeigen, was ich alles weiß. Ein anderer stellte sich via Teams-Telefon als Regional-Finanzverantwortlicher vor und bat mich, unseren Werbeetat-Anteil an ihn sofort zu überweisen, was mir zwar komisch vorkam, aber ich möchte ja freundlich sein und habe so viele Auskünfte erteilt, wie ich konnte. So gegen 17 Uhr verlasse ich dann das Büro – abschließen tut in der Regel die Chefin, da sie meistens länger bleibt.*

*So weit ist eigentlich alles wie immer, wir sind organisiert, und ich bin auf meiner Stelle zufrieden. Nur nächste Woche, da müssen wir die Agentur für einen Tag schließen, weil unsere Zentrale uns alle in so eine Awareness-Schulung schicken will. Ich weiß zwar nicht, wozu das gut sein soll, bei uns ist ja noch nie etwas passiert – aber wenn es angeordnet ist, gehen wir hin und sehen, was wird. Vielleicht lässt sich ja noch etwas lernen.*

## 1.1 Das Ziel dieses Buches

Laras Welt ist in Ordnung. Und für viele andere ist sie das auch, selbst wenn sie sich keine großen Gedanken über die Informatik machen, da sie diese als Instrument für ihre Arbeit nutzen und nicht als zentrales Thema um seinetwillen betrachten.

Oder denken Sie an IT, wenn Sie von einer Öl-Pipeline lesen? Und doch hat im Mai 2021 ein ebensolcher Angriff auf die IT-Systeme der größten amerikanischen Versorgungslinie dafür gesorgt, dass die Versorgungslinie selbst aus Sicherheitsgründen für mehrere Tage abgeschaltet werden musste. Und dies, obwohl durch diese Leitung mehr als 40 % der gesamten an der Ostküste verbrauchten Kraftstoffe laufen.

Oder denken Sie zuerst an IT, wenn Ihre Zeitung am Morgen nicht erscheint? So geschehen in Deutschland, als im April 2021 nach einem Hackerangriff zahlreiche Zeitung und Online-Portale der Madsack-Mediengruppe nicht mehr erreichbar waren oder Zeitungsteile über Tage nur in reduziertem Umfang produziert werden konnten.

Die Liste solcher und anderer Angriffe auf Unternehmen lässt sich mittlerweile täglich erweitern. Und die Folgen sind für die Unternehmen oft so gravierend, dass darüber nicht in den IT-Foren oder Security-Boards, sondern in der Tageschau oder den Zeitungen berichtet wird. Die Angriffe zeigen überdies, wie eng die Verzahnung der eigentlichen Wertschöpfung von Unternehmen mit der Informatik und ihren Systemen mittlerweile ist – und wie manche »Laras aus Neustadt« immer noch auf unbekannte Mails klicken, sich an Telefonen ausfragen lassen oder Systeme unbeachtet laufen lassen.

Die Welt wird wegen eines neuen Buches nicht sicherer, doch mit wachsendem Bewusstsein für die Gefahren, denen unsere Daten und Systeme heute ausgesetzt sind, lässt sich künftig wenigstens ein Teil solcher Angriffe erschweren oder verhindern.

Unser Buch soll dazu die notwendigen Anleitungen, Hilfestellungen, Erklärungen und praktischen Hinweise liefern, damit Ihnen das auch gelingen kann, – und Sie darüber hinaus auf die entsprechende Zertifizierung Ihrer Fähigkeiten als CompTIA-Security+-Techniker/-in gründlich vorbereiten.

Die folgenden Kapitel dieses Buches möchten Ihnen dazu das notwendige Wissen vermitteln und Ihnen eine Orientierung anbieten, damit Sie sich anschließend in den verschiedenen Themenbereichen der Netzwerk- und Systemsicherheit auskennen. So sind Sie auch in der Lage, sich von verschiedenen Seiten her mit der Thematik auseinanderzusetzen: von den Modellen wie IT-Grundschutz, ISO 27000 über die Bedrohungslage bis hin zur Implementation von Maßnahmen oder eines ganzen Security-Managementsystems!

Die Inhalte dieses Buches und eventuell auch ein dazugehöriges Seminar helfen Ihnen bei dem Verständnis der technischen Begriffe, der Funktionsweise von Sicherheitsmaßnahmen und den aktuellen Bedrohungen und einem praxistauglichen Vorgehen, um die Prüfung CompTIA Security+ bestehen zu können.

## 1.2 Die CompTIA Security+-Zertifizierung

CompTIA ist ein weltweiter Verband der Informationstechnologieindustrie. CompTIA hat Mitglieder in mehr als 100 Ländern und liefert Technologiestandards in den Bereichen internetfähige Dienstleistungen, E-Commerce, herstellerunabhängige Zertifizierung, Kundenzufriedenheit, Public Policy sowie Ausbildung. Die Arbeit von CompTIA beruht auf einem kooperierenden Mitgliedsmodell – das

heißt, Hersteller, Dienstleister und Beschäftigte der IT-Industrie arbeiten bei der Formulierung und Umsetzung konkreter Ziele zusammen.

Insbesondere im Bereich der IT-Zertifizierung hat sich CompTIA weltweit einen anerkannten Ruf erworben und ist heute der größte herstellerunabhängige Anbieter von Zertifizierungen im Bereich der Informationstechnologie. Die Basis für die anerkannte Güte der CompTIA-Zertifikate ist nicht zuletzt deren gemeinschaftliche Entwicklung durch IT-Fachkräfte und Mitgliedsunternehmen. Da ein großes Problem der IT-Branche der Wildwuchs zahlreicher Fort- und Weiterbildungsmaßnahmen ist, bietet CompTIA insbesondere im Rahmen der technischen Grundausbildung hochwertige Zertifikate an, die Privatpersonen wie Unternehmen die Orientierung auf dem unübersichtlichen Fortbildungsmarkt erleichtern sollen.

Das erklärte Ziel von CompTIA ist die Etablierung von technischen und fachlichen, aber auch ethischen und professionellen Qualitätsstandards in der IT-Industrie. Indem Unternehmen wie Cisco, Hewlett-Packard, IBM, Intel, Microsoft und Ricoh die Entwicklung der Zertifikate von CompTIA finanziell und mit ihrem Know-how unterstützen, gewinnen sie gleichzeitig Anhaltspunkte über die Fachkompetenz und ein sicheres Anforderungsprofil für die Auswahl von Mitarbeitenden.

Weltweit haben mehr als zwei Millionen Menschen CompTIA-Zertifikate in Systemtechnik, Netzwerktechnologie, Serverbetreuung und anderen Gebieten erworben.

Die CompTIA Security+-Zertifizierung wendet sich an Techniker und Technikerinnen mit eigener Berufserfahrung im Informatikbereich und bescheinigt Absolventen eine breite Kenntnis auf dem Gebiet der Sicherheitstechnologie. Das bestandene Examen bedeutet, dass Geprüfte über ausreichend Wissen verfügen, um die Bedrohungslage zu verstehen und eine Reihe von Maßnahmen zu konfigurieren bzw. in Betrieb zu nehmen. Im Rahmen der Zertifizierung werden zahlreiche herstellerunabhängige Technologien behandelt. Die CompTIA Security+-Prüfung eignet sich sehr gut als Vorbereitung auf die IT-Zertifikate diverser, im Security-Sektor aktiver Hersteller.

Damit die Zertifizierung am Markt erfolgreich bleibt, wird die Prüfung durch die CompTIA regelmäßig aktualisiert und an die aktuellen Anforderungen angepasst, und so liegt mittlerweile die 701er Version von CompTIA Security+ vor. Die Inhalte der Zertifizierung werden anschließend in Lernzieldokumenten auf der Website von CompTIA unter <http://www.comptia.org> veröffentlicht (sogenannte »Exam Objectives«).

Die CompTIA Security+-Zertifizierung teilt sich in mehrere Fachgebiete, im CompTIA-Sprachgebrauch »Domains« genannt. In der aktuellen Fassung der Prüfung (SY0-701) lauten diese Themen auf Englisch wie folgt:

- Domain 1 General Security Concepts (Generelle Sicherheitskonzepte)
- Domain 2 Threats, Vulnerabilities and Mitigation (Bedrohungen, Schwachstellen und Abwehrmaßnahmen)
- Domain 3 Security Architecture (Sicherheitsarchitektur)
- Domain 4 Security Operations (Sicherer Betrieb)
- Domain 5 Security Program Management and Oversight (Verwaltung und Überwachung von Sicherheitsprogrammen)

Entsprechend erhalten Sie in diesem Handbuch zur Sicherheit alle genannten Themen und ihre Zusammenhänge ausführlich erklärt und erlernen so zugleich das für die Zertifizierung notwendige Wissen. Im Zentrum steht dabei weniger die Auflistung aller möglichen und unmöglichen Abkürzungen aus diesem Bereich, sondern die Schaffung des Verständnisses für die Thematik Sicherheit. Für die Abkürzungen finden Sie zudem ein Abkürzungsverzeichnis im Anhang dieses Buches, ebenso wie eine Zuordnung der einzelnen Lernziele zu den Inhalten des Buches.

## 1.3 Das Weiterbildungsprogramm von CompTIA

Halten Sie Ihre Zertifizierung mit dem Weiterbildungsprogramm (CE) von CompTIA auf dem neuesten Stand. Es ist als kontinuierliche Bestätigung Ihrer Expertise und als Werkzeug zur Erweiterung Ihres Kompetenzspektrums konzipiert.

Durch die Teilnahme am Weiterbildungsprogramm von CompTIA bleiben Sie mit neuen und sich entwickelnden Technologien auf dem Laufenden und können Ihre einmal erworbene Prüfung rezertifizieren.

Ihre CompTIA-Security+-Zertifizierung ist ab dem Tag Ihrer Prüfung drei Jahre lang gültig. Das CE-Programm ermöglicht es Ihnen, Ihre Zertifizierung in dreijährigen Abständen durch Aktivitäten und Schulungen zu verlängern, die sich auf den Inhalt Ihrer Zertifizierung beziehen. Wie Security+ selbst verfügt auch CompTIA Security+ CE über einen weltweit anerkannten ISO/ANSI-Akkreditierungsstatus.

Sie können an unterschiedlichen Aktivitäten und Schulungsprogrammen teilnehmen, darunter auch an höherwertigen Zertifizierungen, um Ihre CompTIA-Security+-Zertifizierung zu erneuern. Schließen Sie CertMaster CE ab, einen Online-CE-Kurs im eigenen Tempo, oder sammeln Sie in drei Jahren mindestens 30 Continuing Education Units (CEUs), laden Sie diese auf Ihr Zertifizierungskonto hoch, und Network+ erneuert sich automatisch.

## Hinweis

Wenn Sie den an dieser Stelle von CompTIA zur Verfügung gestellten Code  nutzen, so erhalten Sie beim Kauf eines CompTIA-Prüfungs-Vouchers auf der Webseite von CompTIA 10 % Rabatt.

## 1.4 Voraussetzungen für CompTIA Security+

Gemäß der Website von CompTIA (<http://www.comptia.org>) sind die empfohlenen Voraussetzungen für das Bestehen der Security-Prüfung die CompTIA Network+-Zertifizierung sowie zwei Jahre Erfahrung im Netzwerkbereich mit Schwerpunkt Sicherheit oder einer Systemadministratorenrolle.

Diesen Empfehlungen stimmen die Autoren natürlich zu. Dieses Buch kann Ihnen nicht die praktische Erfahrung vermitteln, die im Bereich Netzwerktechnik nötig ist, um erfolgreich zu sein. Wenn Sie sich also auf die Zertifizierung vorbereiten möchten, lesen Sie dieses Buch, aber installieren Sie auch selbst ein Netzwerk, befassen Sie sich regelmäßig mit Sicherheitsthemen, gehen Sie in ein Training oder bauen Sie mit Kollegen eine Umgebung auf, die dafür geeignet ist, und üben Sie sich praktisch in der Erkennung von Bedrohungen, der Anwendung von Sicherheitsmaßnahmen und -konzepten.

Für weitere Informationen begeben Sie sich bitte auf die Website von CompTIA unter <http://www.comptia.org/de>. Details zur Prüfung finden Sie zudem in Kapitel 21, »Die CompTIA Security+-Prüfung«.

## 1.5 Persönliches

Wer sich zum ersten Mal mit der Thematik Informatiksicherheit befasst, wird vor allem eins feststellen: Es wimmelt nur so von Fremdwörtern und Fachbegriffen. Von Anti-Spam über Phishing bis zum Zombie ist alles vertreten, was das Alphabet zu bieten hat.

Als Autoren staunen wir manchmal selbst über die Vielfalt an Kreationen, die hier geschaffen werden – auch wir mussten nachdenken, als wir zum ersten Mal über »Whaling« gelesen haben ... und längst nicht alle Begriffe verfügen über den gleichen Tiefsinn oder fachlichen Rückhalt.

Ein Buch zur Informatiksicherheit zu verfassen, ist daher eine Gratwanderung zwischen der notwendigen Vermittlung von Fachwissen und der Zurückhaltung gegen ein Überborden von Pseudofachbegriffen und (vorwiegend) Anglizismen, die mehr vorgeben, als sie wirklich bedeuten.

Wir haben uns daher beim Schreiben bemüht, Ihnen einen Überblick zu ermöglichen, sich mit den zentralen Themen vertraut zu machen und vor allem die Thematik zu verstehen, aber nicht schlicht Begriffe auswendig zu lernen – obwohl sich das prüfungstechnisch nicht ganz vermeiden lässt.

Es ist unsere feste Hoffnung, dass wir Sie mit diesem Buch für die Thematik der Informationssicherheit über die reine Prüfung hinaus sensibilisieren können, Ihnen Hilfen an die Hand geben und Sie ausrüsten für einen sinnvollen und sicheren Umgang mit Informationen und Informatikmitteln in Ihrem Umfeld.

Zu den Autoren selbst:

Mathias Gut, Master of Advanced Studies ZFH in Business Analysis und Dipl. Informatiker, ist Information- und Cyber-Security-Experte. Er ist in verschiedenen Bereichen von Sicherheitsfragen ausgebildet und zertifiziert, unter anderem als zertifizierter OSSTMM Professional Security Tester (OPST), zertifizierter ICO ISMS Auditor nach ISO/IEC 27001:2022, CompTIA Advanced Security Practitioner (CASP), CompTIA Security+, CompTIA Network+, CompTIA Linux+ und hat zusätzlich ein abgeschlossenes Zertifikat CAS Information Security & Risk Management der Fachhochschule Nordwestschweiz. Er arbeitet täglich mit Fragen der Cybersicherheit und unterrichtet zudem als Dozent im Bereich der Informationstechnik mit Schwerpunkt Cyber-Sicherheit in der höheren beruflichen Bildung. Als impulsgebender Entwickler und Mitdozent des von der HWZ verliehenen CAS Cyber Security Expert übernimmt er eine aktive Rolle in der Weiterbildungslandschaft. In seiner Freizeit setzt er sich für quelloffene Software und freie Analysemethoden ein, forscht zu Themen des Living-off-the-Land Hackings und gibt Fachreferate dazu.

Markus Kammermann, ursprünglich Theologe, später weitere Berufsausbildungen zum IT-Projektleiter und Ausbilder, SCRUM Master, CompTIA Security+ und weitere Zertifizierungen, ist Autor mehrerer Fachbücher aus der CompTIA-Zertifizierungsreihe bei mitp. Allen voran das bereits in 9. Auflage erschienenen Grundlagenwerks »CompTIA Network+« sowie das in 6. Auflage verlegten Studienwerks »CompTIA A+«. Er arbeitet seit vielen Jahren als technischer Berater, Dozent und Referent in verschiedenen Ländern und ist in seiner Seele ein »Erklärer«, der nach wie vor selbst IT-Infrastruktur konzipiert, vernetzt und installiert und somit die Sicherheit in der IT tagtäglich mit seinen Kunden erlebt, auch und gerade, wenn sie nicht funktioniert. Als Dozent in der höheren beruflichen Bildung und Autor ist es ihm wichtig, nicht nur Sachverhalte darzulegen, sondern sie verständlich zu machen, denn Lernen lebt nicht vom Hören, sondern vom Verstehen und Befähigt werden.

Wir danken Herrn Rechtsanwalt Christian Mitscherlich (Partner), Herrn Rechtsanwalt Fokko Oldewurtel (Senior Associate) und Herrn Andreas Schäfer (Senior Associate) von der Kanzlei Domenig & Partner Rechtsanwälte AG für ihren wert-

vollen Beitrag zu den Themen Datenschutz, Cybercrime und KI-Recht. Ihre Kanzlei Domenig & Partner Rechtsanwälte AG aus Bern besteht aus führenden Datenschutzexperten der Schweiz, die an der Redaktion des neuen schweizerischen Datenschutzgesetzes mitgewirkt haben. Private Unternehmen und die öffentliche Hand zählen bei der Bewältigung ihrer datenschutzrechtlichen Herausforderungen auf die Hilfe des Datenschutzrechtsteams der Domenig & Partner Rechtsanwälte AG.

Anlässlich der anwaltlichen Beratung beschäftigen sich die Autoren täglich mit der Umsetzung von Vorgaben der DSGVO und des neuen schweizerischen Datenschutzgesetzes. Diese umfangreiche Praxiserfahrung ließen die Autoren bei der Redaktion des neuen Kapitels Kapitel 4, »Rechtliche Grundlagen«, der fünften Auflage dieser Publikation einfließen.

Bedanken möchten wir uns an der Stelle auch bei Markus a Campo, der an der ersten Auflage aktiv mitgearbeitet und damit etliche Vorarbeit vor allem zur 2. Auflage beigetragen hat. Er arbeitet als Berater, Autor und Schulungsreferent mit dem Schwerpunkt IT-Sicherheit. Er ist von der IHK Aachen öffentlich bestellter und vereidigter Experte im Bereich IT-Sicherheit.

Bedanken möchten wir uns an dieser Stelle zudem ausdrücklich bei den Herstellern und ihren Kommunikationsabteilungen, die uns mit Bildmaterial und Unterlagen unterstützt haben.

Ebenso möchten wir uns an dieser Stelle beim mitp-Verlag bedanken und persönlich bei Katja Völpel – ja, wir haben wieder einen Titel zusammen publiziert, und das ist erfreulich.

Und da dies heute ein aktuelles Thema ist: Dieses Buch wurde auch in der fünften Auflage nicht mit KI-basierten Tools erstellt oder revidiert, und wir haben die KI auch nicht um ihre Meinung zu unserem Buch befragt.

Wir wünschen Ihnen viele spannende Stunden, ob in einem E-Book am Tablet bzw. Computer oder mit einem gedruckten Exemplar, was übrigens, so als Randnotiz, immer noch mehr als 90 % aller Leser und Leserinnen vorziehen, und nein, diese Zahl stammt nicht von 2015 aus der ersten Auflage ...

# Sind Sie bereit für CompTIA Security+?

Bevor Sie sich an die eigentlichen Themen von CompTIA Security+ heranwagen, haben Sie an dieser Stelle die Gelegenheit, die Voraussetzungen für diese Zertifizierung in einem kleinen Test an sich selbst zu überprüfen.

Sie finden daher im Folgenden 25 Fragen, die sich, basierend auf den von CompTIA definierten Voraussetzungen, vorwiegend mit Netzwerkfragen befassen und Ihnen die Einschätzung erlauben sollen, ob Sie das für die folgenden Themen benötigte Verständnis und Fachwissen mitbringen.

### Frage 1

Sie verkaufen Ihrem Kunden eine Komponente mit der Aufschrift »IEEE 802.11ax«. Worum handelt es sich technisch gesehen bei diesem Produkt?

- A) VLAN-Technologie
- B) USB-3.0-Anschluss
- C) USB-1.n-Anschluss
- D) WLAN-Technologie
- E) FireWire-Anschluss
- F) FDDI-Anschluss

### Frage 2

Welches ist die maximale Segmentlänge eines Gigabit-Ethernet-Segments, wenn Sie dieses mit 1000BASE-LX verkabeln?

- A) 7500 Meter
- B) 5500 Meter
- C) 550 Meter
- D) 250 Meter
- E) 100 Meter

**Frage 3**

In einem Unternehmen sollen sich dessen Gäste mit dem Internet verbinden können, ohne dass sie irgendeinen Zugriff auf das Firmennetzwerk erhalten. Alle Verbindungen müssen über den gleichen Switch gemanagt werden können. Was werden Sie unternehmen, um diese Anforderungen zu erfüllen?

- A) RIPv2 implementieren
- B) OS-PF installieren
- C) Port Trunking implementieren
- D) VLAN-Funktionalität implementieren

**Frage 4**

Bei allen folgenden Anschlüssen handelt es sich um fiberoptische Anschlüsse mit Ausnahme von:

- A) BNC (British Naval Connector)
- B) MT-RJ (Mechanical Transfer-Registered Jack)
- C) ST (Straight Type)
- D) SC (Standard Connector)

**Frage 5**

Ein Netzwerk gemäß 802.11n-Standard kann auf Frequenzen im folgenden Frequenzband senden:

- A) 900 MHz
- B) 1,9 GHz
- C) 2,9 GHz
- D) 5,0 GHz
- E) 11,0 GHz

**Frage 6**

Nicht jedes Kabelmedium reagiert gleich auf elektromagnetische Störungen. Welches der folgenden Medien ist am anfälligsten für diese Störungen?

- A) UTP-Kategorie 5e
- B) MMF optisches Kabel
- C) RG-58 Koaxial
- D) F/STP-Kategorie 6a

**Frage 7**

Mit welchem der folgenden Geräte können Sie ein 802.3-Netzwerk mit einem 802.11-Netzwerk verbinden?

- A) Modem
- B) Repeater
- C) PVC (Permanent Virtual Circuit)
- D) Gateway
- E) WAP (Wireless Access Point)

**Frage 8**

Welche Netzwerkschnittstelle arbeitet auf den oberen drei OSI-Layern und verbindet Netzwerke unterschiedlicher Architekturen?

- A) Hub
- B) Modem
- C) Switch
- D) Router
- E) Gateway

**Frage 9**

Die Arbeitsstation, an der Sie gerade arbeiten, zeigt Ihnen eine Fehlermeldung. Diese besagt, dass die IP-Adresse Ihres Rechners doppelt im Netzwerk entdeckt worden ist. Nachdem Sie sich eine Ursache für dieses Problem überlegt haben, was ist Ihr nächster Schritt?

- A) Einen Aktionsplan zur Lösung umsetzen
- B) Zusätzliche Fakten zum Auftreten des Problems sammeln
- C) Die Lösung dokumentieren
- D) Den Aktionsplan testen und die Ergebnisse auswerten

**Frage 10**

Welcher Programmaufruf erzeugt das folgende Ergebnis auf dem Bildschirm:

Aktive Verbindungen

Proto	Lokale Adresse	Remoteadresse	Status
TCP	workstation:1135	192.168.2.68:microsoft	HERGESTELLT
TCP	workstation:3845	server05.mitp.de:HTTP	WARTEND

- A) arp
- B) ifconfig
- C) tracert
- D) netstat
- E) proto /a
- F) nslookup

**Frage 11**

Ein Benutzer meldet sich beim Administrator, dass er keinen Zugriff mehr auf das Netzwerk hat. Er kann keinen erfolgreichen *ping*-Befehl an die anderen Stationen in seinem Netz absetzen, und *ipconfig* zeigt ihm zwar eine gültige IP-Adresse an, die aber nicht das korrekte Subnetz anzeigt, in dem sich der Rechner eigentlich befindet. Welcher Ansatz beschreibt dieses Problem am ehesten richtig?

- A) Der DHCP-Server hat die Kommunikationsverbindung zum passenden DNS-Server verloren.
- B) Der WINS-Server ist offline.
- C) Der DHCP-Server ist offline.
- D) Jemand hat einen zweiten DHCP-Server aktiviert.
- E) Die Netzwerkkarte ist defekt.

### Frage 12

Ihr IT-Administrator hat kürzlich einen neuen DNS-Server ins Netzwerk integriert und den bisherigen DNS-Server vom Netz genommen. Der neue DNS-Server verfügt über eine neue IP-Adresse, und dieser Wechsel wurde im DHCP-Server auch eingetragen.

Dennoch können in der Folge einige Arbeitsstationen Webadressen wie z.B. `http://www.mitp.de` oder `http://www.educomp.eu` aufrufen, während andere dies nicht können. Welche Arbeitsstationen sind in der Lage, die Adresse `http://www.mitp.de` aufzurufen?

- A) Jede Arbeitsstation, die seit der Umstellung den DHCP-Lease nicht erneuert hat.
- B) Jede Arbeitsstation mit einer statischen IP-Adresse.
- C) Jede Arbeitsstation, die mindestens über Microsoft Edge verfügt.
- D) Jede Arbeitsstation, die den DHCP-Lease seit der Umstellung erneuert hat.

### Frage 13

Ein Webdesigner hat den Webaufttritt der Firma umgebaut und dabei so programmiert, dass ab jetzt HTTPS notwendig ist, um eine Verbindung zum Server herzustellen.

Nach dieser Umstellung ist der Webserver zwar für die Intranet-Benutzer nach wie vor zugänglich, aber vom Internet ist keine Verbindungsaufnahme mehr zu ihm möglich. Was verursacht dieses Problem am Ehesten?

- A) Die Firewall des Unternehmens verweigert den Zugang auf Port 389.
- B) Die Firewall des Unternehmens verweigert den Zugang auf Port 443.
- C) Der Webserver des Unternehmens verweigert den Zugang auf Port 8080.
- D) Der DNS-Server des Unternehmens ist deaktiviert.

### Frage 14

Welches der folgenden Kommandos resultiert in der Anzeige der MAC-Adresse eines bestimmten Computers?

- A) `nslookup`
- B) `ipconfig /all`
- C) `nbtstat -r`
- D) `netstat`

**Frage 15**

Eine Antivirensoftware bietet dann den besten Schutz, wenn sie ... (vervollständigen Sie bitte den Satz korrekt):

- A) auf den Arbeitsstationen installiert ist, die mit dem Internet verbunden sind.
- B) auf den Servern installiert ist.
- C) auf den Servern und allen Arbeitsstationen installiert ist.
- D) auf dem Internet-Gateway installiert ist.

**Frage 16**

Der Netzwerkadministrator muss das Notebook eines Außendienstmitarbeiters einrichten. Dabei muss er dem Verkäufer ermöglichen, im Außeneinsatz via Internet eine sichere Verbindung zum Firmennetzwerk aufbauen zu können. Was muss der Administrator bei der Einrichtung konfigurieren?

- A) Er installiert das IPX/SPX-Protokoll für sicheren Datenaustausch.
- B) Er installiert eine Firewall auf dem Laptop.
- C) Er richtet einen drahtlosen Zugang ein.
- D) Er erstellt eine PPTP-Verbindung.
- E) Er stellt sicher, dass die Antivirensoftware jederzeit auf dem neuesten Stand ist.

**Frage 17**

Ihr Netzwerkadministrator implementiert mehrere VLANs auf einem Switch. Welches Gerät bzw. welche Funktionalität benötigt er dabei, um den Datenverkehr zwischen den verschiedenen VLANs zu ermöglichen?

- A) Nichts
- B) Einen zweiten Switch
- C) Einen zusätzlichen Switch pro VLAN
- D) Einen Router

**Frage 18**

Beim Einsatz einer Routing-Tabelle wird welche der folgenden Routen am *ehesten* ausgewählt?

- A) Die niedrigste administrative Distanz
- B) Die höchste administrative Distanz
- C) Die BGP-Route
- D) Die Route mit dem höchsten Hop-Count

### Frage 19

Wenn ein Windows-Netzwerk auf eine Ressource zugreift, werden die »Credentials« (Zugriffsberechtigungen) durch den Gebrauch eines \_\_\_\_\_ (setzen Sie den korrekten Begriff ein) übertragen.

- A) Passworts
- B) Tokens
- C) Cookies
- D) Keys
- E) Usernames

### Frage 20

Sie installieren ein neues Netzwerk und setzen dazu zwei Domaincontroller auf. Der eine hat die Adresse 192.168.25.5 und der andere die Adresse 192.168.25.140. Beide fungieren als DHCP-Server im Range 192.168.25.1 – 192.168.25.254 mit dem Subnetz 255.255.255.0. Nach der Installation treten verschiedentlich DHCP-Fehler auf. Wie können Sie diese beheben?

- A) Ändern Sie das Subnetz auf 255.255.0.0, damit Sie mehr verfügbare Adressen erhalten.
- B) Die Server halten die IP-Adressen zu lange im Cache Memory fest. Booten Sie die beiden Server neu, und das Problem ist behoben.
- C) Teilen Sie den DHCP-IP-Bereich zwischen den beiden Servern auf, indem Sie den Bereich im DHCP-Server halbieren, sodass einer die Adressen von 192.168.25.1 bis 127 und der andere von 192.168.25.128 bis 254 vergibt.
- D) Teilen Sie den DHCP-IP-Bereich zwischen den beiden Servern auf, indem Sie das Subnetz auf 255.255.255.128 ändern und den IP-Bereich halbieren, sodass einer die Adressen von 192.168.25.1 bis 127 und der andere von 192.168.25.128 bis 254 vergeben kann.

### Frage 21

Sie arbeiten als Netzwerkadministrator in Ihrer Firma. Sie müssen den Bandbreitenbedarf für das Internet reduzieren. Wie können Sie dies erreichen?

- A) Sie installieren einen WINS-Server.
- B) Sie installieren einen Proxyserver.
- C) Sie installieren einen HTTP-Dienst.
- D) Sie installieren einen DHCP-Server.
- E) Sie installieren einen DNS-Server.
- F) Sie installieren eine Firewall.

**Frage 22**

Der Systemadministrator konfiguriert den MS-Exchange-Server für den Einsatz von E-Mail. Der Server muss dabei Mails an die Partnerfirma versenden können, die ihrerseits einen postfix-Server einsetzt. Welches Protokoll wird eingesetzt, um Mails zwischen diesen beiden Servern hin- und herzusenden?

- A) POP3 (Post Office Protocol Version 3)
- B) CSNW (Client Service for NetWare)
- C) SMTP (Simple Mail Transfer Protocol)
- D) TCP/IP
- E) WNMG (Windows NetWare Mail Gateway)

**Frage 23**

Der Administrator eines Netzwerks ist zuständig für ein kleines lokales Netzwerk, in dem zehn Stationen verkabelt durch einen Switch verbunden sind. Der Switch wiederum ist an einen Router angeschlossen, der die Verbindung ins Internet sicherstellt. Eines Tages wird er von einem Benutzer um Hilfe gebeten, weil dieser nicht mehr ins Internet kommt. Alle anderen Benutzer haben aber Zugriff auf das Internet. Was muss dieser Administrator prüfen, um dieses Problem anzugehen?

- A) Netzwerkkarte der betroffenen Maschine, Port des Switches, der zum Router verbunden ist
- B) Netzwerkkabel von der betroffenen Maschine zum Switch, Port am Switch, bei dem dieser Rechner eingesteckt ist, Zugangskabel vom Internet zum Router
- C) Netzwerkkarte der betroffenen Maschine, Netzwerkkabel von dieser Maschine zum Switch, Port am Switch, bei dem dieser Rechner eingesteckt ist
- D) Netzwerkkabel der betroffenen Maschine, Netzwerkkabel aller anderen Benutzer und deren Ports am Switch, Uplink-Port zum Router

**Frage 24**

Ihr Unternehmen möchte für das neue Verkaufssystem eine sichere Netzwerkumgebung einrichten. Daher muss der Netzwerkverkehr dieses Systems aus Sicherheitsgründen isoliert werden. Das aktuelle Adressschema lautet 10.22.33.x /24. Welche der folgenden Methoden hilft am besten, um den Verkehr zu separieren?

- A) Ein dediziertes Broadcast-Netzwerk für das neue System
- B) Ein dediziertes Multicast-Netzwerk für das neue System
- C) Der Wechsel der IP-Adressen in ein C-Klassenschema
- D) Die Einrichtung eines eigenen Subnetzes für das neue System

**Frage 25**

Welches Netzwerkgerät kann regelbasiert Pakete filtern?

- A) Firewall
- B) Layer-2-Switch
- C) Hub
- D) Bridge

Die Antworten zu diesen Fragen finden Sie in Abschnitt A.1, »Antworten zu den Vorbereitungsfragen«.

Das Ziel dieses Tests ist es, mindestens 72 % der Fragen richtig zu beantworten. Erreichen Sie dieses Ziel, sind Sie gut vorbereitet auf die folgenden Kapitel. Erreichen Sie dieses Ziel nicht, empfehlen wir Ihnen, sich vorab intensiver mit Netzwerktechnik auseinanderzusetzen, zum Beispiel anhand der CompTIA Network+-Zertifizierung, zu der von Markus Kammermann ebenfalls ein deutschsprachiges Buch aus dem mitp-Verlag vorliegt: »CompTIA Network+«.

# Stichwortverzeichnis

- 2,4-GHz-ISM-Band 493
- 3DES 121
- 5-GHz-ISM-Band 493
- 802.11ac 492
- 802.11b 490
- 802.11g 490
- 802.11i 505
- 802.11n 491
- 802.11p 496
- 802.11s. 496
- 802.1x 472, 506
- A**
- AAA-Protokoll 475
- ABAC
  - Zugriffsverfahren 166
- Absichtserklärung 389
- Access Control List 148, 163
- Access Point
  - Captive Portal 251
  - Evil Twin 251
  - Rogue 250
- Ad hoc 500
- Ad-hoc-Netzwerk 496
- Administrative Richtlinie 58
- Advanced Threat 304
- Adversary tactics, techniques and procedures (TTP) 240
- Adware 200, 201, 304
- AES 121
- AH 478
- AIRO 537
- Allowlisting 257, 305, 306, 333
- Amplification-Attack 447
- AMSI 298
- Änderung 578
- Angriffsvektoren 115
  - Dateibasierend 429
  - Image-basierend 430
- Annual Loss Expectancy 626
- Antivirus-Evasion-Methode 293
- API 257
- App 331
  - Whitelist 333
- Application-DDoS 447
- Application Gateway 559, 561
- Application Level Gateway 553
- AppLocker 305
- APT 211, 213, 238
- Arbitrary Code Execution 229
- Archivierung 344, 373
- ARP 541
  - NDP 541
- Artificial Intelligence (AI) 257, 298
- ASLR 230, 307, 308
- ASP 420
- Asset Tracking 330
- Asymmetrische Verschlüsselung 123, 132
- Attacke
  - Advanced Persistent Threat 213
  - Carbanak 239
  - DNS-Tunneling 249
  - HID-Angriff 244
  - Kaltstartattacke 243
  - MMS-Phishing 212
  - Pass-the-Hash 235, 242
  - Pharming 213
  - Phishing 213
  - Rootkit 212, 454
  - SMS-Phishing 212
  - Zero hour 212
- Attack Surface Reduction (ASR) 299
- Aufbewahrung 345
- Aufbewahrungspflicht 374
- Aufgabenteilung 353
- Aufnahmemöglichkeit mobiles Gerät 338
- Ausfallszenario 625
- Authentifizierung 150
- Authentifizierungsmethode 150
- Autorisierung 148
- Awareness 297, 353, 361
- B**
- BaaS 419
- Backdoor 213, 236, 244, 246, 454
- Badge 176, 178, 254
- BAD-USB-Angriff 244
- Baseline-Management 524
- Baseline-Messung 266
- BASH 232
- Bastion Host 559
- Bauliche Maßnahme 175
- BCM 610
- BCMS 610
- Bcrypt 131
- Bell La Padula 163
- Benutzerverwaltung 59
- Beweismittel 599
- Bildschirm Sperre 329
  - Notebook 327
- Biometrie 154
- Biometrisches Erkennungssystem 179
- Birthday-Attacke 584
- Bitcoin 172
- Black-Box-Test 589
- Black Hat 459
- Blockchain 171
- Blockverschlüsseler 117
- Blowfish 122
- Bluejacking 514
- Bluesnarfing 514
- Bogus Access Point 450
- Bogus DHCP-Server 450
- Bombe
  - logische 214
- Boot-Virus 207
- Bösartiges USB-Kabel 245
- Bot 486
- Botnet 262, 447, 486
- Brandklasse 184
- Brandschutz 184
- Bring Your Own Device 334
- Broadcast 395
- Brute Force 435
- BSI 51, 52, 53
  - Bausteine 53
  - Schichtenmodell 53
- Buffer Overflow 228, 229
- Bug-Bounty 463
- Business Continuity Management 376
- BYOD 334
- C**
- CA 132, 137, 138
- Cache-Poisoning 412
- CBC 118, 134
- CCMP 505
- CCPA 351

- CEO Fraud 360  
 CERT 428  
 Certificate Authority 132, 137, 138  
 CFB 119  
 Chain of Trust 139  
 Change-Management 577  
 Change-Protokoll 578  
 CHAP 169  
 Chassis Intrusion Detection 273  
 Choose Your Own Device 334  
 CIA 45, 113  
 CIFS 418  
 Cipher text only 134  
 Circuit Level-Firewall 560  
 Clean Desk Policy 348  
 Cleanup 589  
 Clickjacking 445  
 Cloud 455  
     Public-Cloud-Dienste 332  
     Sicherheit 419  
 Cloud Computing 280  
     IaaS 419  
     PaaS 419  
     SaaS 419  
 Cloud Security Alliance 423  
 Cluster 622  
 Clustering 621  
     HA-Cluster 621  
     NLB 622  
     SMP 621  
 CO2 185  
 Codesignierungs-Zertifikat 140  
 Cold Site 631  
 Command-and-Control 486, 568  
 Command-Injection 440  
 Command Shell (CMD) 232, 240  
 Common Criteria 276  
 Common Name 140  
 Community Cloud 421  
 Compliance 349  
 CompTIA Security+ 24  
 Container-Virtualisierung 279  
 Cookie-Diebstahl 453  
 Cookie-Manipulation 440  
 COOP 633  
 COPE 334  
 Corporate Owned Personally Enabled 334  
 Credential Guard 243  
 Credential harvesting 221  
 Credential-Management 333  
 Crimeware 203  
 CRL 142, 153  
 Cross Site Scripting 438  
 Cryptomalware 218  
 Cryptomining 218  
 CSA 423  
 CSAB 161  
 CSF 50  
 CSP 115, 438  
 CSR 137  
 CTR 119  
 cuckoo 584  
 curl 584  
 CVE 230, 573, 593, 597  
 CVSS 230, 593  
 Cyberkriminelle 199  
 CYOD 334  
**D**  
 DAC  
     Zugriffssteuerung 163  
 Darknet 231  
 Darkweb 231, 306  
 Data-at-rest 132  
 Data-Carving 603  
 Data Execution Prevention 308  
 Data-in-transit 132  
 Data-in-use 132  
 Data Loss Prevention 346  
 Data masking 387  
 Datenhaltung 344  
 Datenschutz 66  
 Datenschutzgesetz  
     Datensicherung 374  
 Datensicherung 301, 372, 373, 376, 381  
 Datensicherungskonzept 376  
 Datensicherungsmedium 373  
 DCS 281  
 DDoS 262  
 Deauthentication 252, 253  
 Dedizierte Firewall 551  
 Deep Fake 258  
 Deep Learning 258  
 Deep Packet Inspection 333  
 Degaussing 386  
 Denial of Service 215, 228, 253, 432, 446, 486  
 Denylisting 305  
 DEP 230, 307, 308, 431  
 DES 120  
 DevOps 315  
 DH 124  
 DH-Gruppen 125  
 Diebstahlsicherung 272  
 Dienstleistungsrahmenvertrag 389  
 Differenziell  
     Datensicherung 381  
 Diffie-Hellman 124  
 Diffusion 117  
 Digitale Signatur 131  
 Directory-Traversal 436  
 Disassoziation 253  
 Disaster Recovery 59, 380, 623  
 Disk  
     Full Disk Encryption 275  
     Opal 275  
     SED 275  
 Disposal-Management 89, 385  
 Distributed Denial of Service 447  
 DKIM 368  
 DLL-Injection 230  
 DLP 346  
 DMARC 299, 368  
 DMZ 550, 554  
 DNS 412, 554  
 dnsenum 584  
 DNS-Flooding 227  
 DNS-Poisoning 226  
 DNS-Spoofing 226  
 Domain 278  
 Domain Hijacking 445  
 Domänenrichtlinie 270  
 Doxing 227  
 Dragonblood 252  
 Drehschleuse 180  
 Drive-by-Angriff 443  
 Drive-by-Pharming 227  
 Drohnen 256  
 DSGVO 75, 82, 349  
 Dual-homed Firewall 552  
 Due Diligence 350  
 Dumpster Diving 357  
 Duplexing 618  
**E**  
 EAP 507  
 EAP-TLS 473  
 Eavesdropping 486  
 ECB 117  
 ECC 125  
 EDR 295  
 EICAR 302  
 Einbruchsschutz 182  
 EIP 229  
 Elektrostatische Entladung 187  
 ElGamal 125  
 E-Mail-Protokolle 413  
 E-Mail-Sicherheit 362  
 Embedded-System 318  
 EMP 193  
 End Point Protection 294  
 Energieversorgung 188  
 Enigma 114  
 Entladung  
     elektrostatische 187

- Erkennungssystem  
 biometrisches 179  
 Erpressung 216  
 Error Handling 317  
 SEH 318  
 ESD 187  
 ESD-Strip 187  
 ESP 479  
 Evil Maid 233  
 Evil Twin 247, 251  
 Exploit 228, 588  
 Extortion 216  
 Double 216  
 Triple 216  
 Extranet 557
- F**
- FaaS 279, 419  
 False Negative 592  
 False Positive 592  
 False-Positive 588  
 FCAPS 520  
 FDE 275, 328  
 Fehler  
 kritischer 287  
 sicherheitskritischer 287  
 FIDO2 150  
 File Inclusion  
 LFI 436  
 RFI 436  
 Fileless Malware 218  
 Fingerabdrucksensor 329  
 Fingerprint 154  
 Fingerprinting 587  
 FINMA 51  
 Firewall 555  
 Circuit Level 560  
 dedizierte 551  
 Dual-homed 552  
 Hardware- 552  
 Paketfilter 558  
 Personal 551, 555  
 Software-Firewall 276  
 Stateful Packet Inspection 558  
 Typen 553  
 FireWire-Hack 243  
 Firmware 237, 244, 253, 271,  
 272, 275, 283, 285, 511  
 FISMA 351  
 Fleeceware 201  
 Flood Guard 404  
 FOMO 203  
 Footprinting 585  
 Forensik 597  
 FORM-Field 440  
 FTP 411  
 Full Device Encryption 328  
 Fuzzing 596  
 FWaaS 161
- G**
- Gangerkennung 154  
 GCM 118  
 Generationenprinzip  
 Datensicherung 382  
 Geographic restrictions 386  
 Geo-Tagging 333  
 Geräteiname 514  
 Gerätesperre 328  
 Geschlossenes System 311  
 Gesichtserkennung 154  
 Google Dorks 356  
 Google-Hacking 356  
 Governance 350  
 GPDR 82  
 GPS-Tracker 327  
 GPT 259  
 GPT-Jailbreaking 260  
 Gray Hat 459  
 Grayware 200  
 Gruppenrichtlinie 269  
 Guard Rails 316
- H**
- H2M-Schnittstelle 281  
 Hackertatbestand 78  
 Hackeraktivist 461  
 Hardware-Firewall 552  
 Hardware-Sicherheitsmodul  
 276  
 Hardware-Virtualisierung  
 278  
 Hash 169  
 Hash-Wert 127  
 Header 603  
 Heap Spraying 432  
 Hierarchische PKI 137  
 HIPAA 351, 375  
 HIPS 294, 297  
 HMAC 130  
 Hoax 218  
 Hochwasserschutz 183  
 Höhere Gewalt 623  
 Honeynet 563  
 Honeypot 563  
 Hotfix 288, 437, 592  
 HOTP 153  
 Hot Site 59, 631  
 hping3 588  
 HSM 141, 276  
 HSTS 319  
 HTTP 414, 554  
 HTTP/2 415  
 HTTPS 414  
 Hybrid Cloud 421  
 Hybride Verschlüsselung 132  
 Hybrid-RAID 615  
 Hypervisor 278
- I**
- IaaS 419, 455  
 ICS-Server 281  
 Identifizierung 150  
 Identität 147  
 IDS 563, 565, 566  
 IEEE 802.11 490  
 IEEE 802.11ax 493  
 IEEE 802.11be 494  
 ifconfig 538  
 IGMP 409  
 IKE 481  
 Impersonation 357  
 Implementierung 406  
 Implicit Deny 148  
 Incident-Management 302  
 Incident Response 597  
 Incident-Response-Team 632  
 Industrie 4.0 280  
 Influence Campaigns 360  
 Information Gathering 235,  
 356  
 Informationsbeschaffung  
 572  
 Information Security  
 Management System 57  
 Informationsklasse 343  
 Informationsrichtlinie 58  
 Infrastrukturnetzwerk 496  
 Inkrementell  
 Datensicherung 381  
 Input Validation 317  
 Integer Overflow 230  
 Integrität 44  
 Internet of Things 260, 281  
 Intranet 557  
 Intrusion Detection 564  
 Intrusion Prevention 564  
 Intrusion Prevention System  
 566  
 Invoice scams 360  
 IoC 235, 314  
 IoT 260, 281, 286, 318  
 ipconfig 538  
 ip-Kommando 539  
 IP-Protokoll 406  
 IPS 566  
 IPsec 477, 480  
 IPv6 410  
 Iris-Scan 154  
 ISA 389  
 ISMS 57, 623  
 ISO/IEC 27001 50  
 IT-Grundschutz 55  
 ITSEC 47  
 IV-Attacke 503
- J**
- Jamming-Angriff 253  
 Job-Rotation 353

**K**

Kensington 273  
 Kerberos 167  
 Kerckhoff-Prinzip 134  
 Kernprotokoll 406  
 Keycard 177, 254  
 Keylogger 233, 443  
 Key-Stretching 115  
 Key stretching 131  
 Klassifizierung  
   Informationen 342  
   zur Datenhaltung 346  
 Klimaanlage 193  
 Known plain text 134  
 Kollision 436  
 Konfigurationsmanagement  
   266  
 Konfusion 117  
 Kontrollen 574  
 Kopplung  
   Bluetooth 515  
 KRACK-Attacke 251  
 Kriminalität  
   organisierte 460  
 Kriminelle Aktivitäten 624  
 Kritischer Fehler 287  
 Kryptografie 114  
 Krypto-Malware 218  
 Kryptoschlüssel 275  
 Kryptowährung 172  
 Künstliche Intelligenz (KI)  
   257, 298

**L**

L2TP 477  
 Länderfilter 306  
 Länderfilterungen 386  
 LANMAN 130  
 Lastwert 524  
 Lateral Movement 235, 242  
 LDAP 419  
 LDAP-Injection 439  
 Least Privileges 166, 167  
 Legacy 285  
 Leistungsbeschreibung 388  
 Leistungsüberwachung 525  
 Letter of Intent 389  
 Lifecycle-Management 315  
 Living-off-the-Land-Hacking  
   232, 240  
 LLM 258  
 Loadbalancing 622  
 Lockout 328  
 Logdaten 649  
 Logfile-Analyse 650  
 Logfiles 649  
 Logische Bombe 214  
 LoMAC 163  
 Löschen 385  
 LSASS 242

LSO 444  
 Luftfeuchtigkeit 194

**M**

M2M 281  
 MAC  
   Zugriffssteuerung 162  
 MAC-Cloning 449, 512  
 MAC-Flooding 451  
 MAC-Spoofing 448, 512  
 Mail-Gateway 370  
 Mail Spoofing 367  
 Makrovirus 207, 298  
 Malvertising 438  
 Malware 203  
   Adware 200  
   Antispyware 202  
   Arbeitsweise 206  
   Crimeware 203  
   Grayware 200  
   Spam 200  
   Spyware 200  
   Symptome einer Infek-  
   tion 205  
 Malware Dropper 212, 218,  
   232, 236, 241, 293  
 Malware Injector 232  
 Malwaretising 231  
 Managed Objects 519  
 Management Information  
   Base 520  
 Mandatory vacations 353  
 Man in the Browser 445  
 Man in the Middle 449, 452,  
   486  
 Mannschleuse 180  
 Man Trap 180  
 Maßnahme  
   bauliche 175  
 Maus 314  
 MD4 128  
 MD5 128  
 MDR 295  
 Memory Injection 430  
 Memory Leak 318  
 Memory of Understanding  
   389  
 Menschliches Versagen 624  
 Metasploit Framework 596  
 Mimikatz 235, 242  
 MIMO 491  
 Mining Rig 218  
 Mirror 613  
 MITRE ATLAS 259  
 MITRE ATT&CK® 240  
 Modus 1  
   Bluetooth 513  
 MOU 389  
 MouseJack 246  
 MRTG 534

MTO 383, 627  
 MTR 542  
 Multifaktorauthentifizie-  
   rung 156  
 Multi-Level-Security 162  
 MU-MIMO 493

**N**

NAC 397  
 Nagios 535  
 NAS 476  
 NAT 396  
   DNAT 396  
   NAPT 397  
   PAT 396, 397  
   SNAT 396  
   SUA 396  
 Need to know 167  
 Negative Rules 553  
 Nessus 584  
 NetBIOS 418  
 netcat 584  
 Netflow 650  
 netstat 544  
 Network Access Server 476,  
   507  
 Netzwerkmonitor 528, 529  
 Netzwerk-Sniffer 595  
 Netzwerküberwachung 528  
 NFC 254  
 NGFW 561  
 Nicht-Leugbarkeit 170  
 Nicht sichtbar  
   Bluetooth 514  
 NIDS 564  
 NIPS 294, 564  
 NIST 50  
 Non-Disclosure Agreement  
   584, 585  
 NOP 229  
 NoSQL-Datenbanksystem  
   318  
 Notebook  
   Bildschirm Sperre 327  
 Notfallplan 629  
 Notfallvorsorge 59, 611  
 Notstromaggregat 190  
 nslookup 543  
 NTLM 130, 131, 169

**O**

Obfuscation 387  
 OSCP 138  
 OFB 119  
 OFDMA 493  
 Offboarding 353  
 Öffentlicher Schlüssel 123  
 OID 139  
 OLA 388  
 Onboarding 353

- One-Time-Pad 116  
 Online-Backup 384  
 Open Framework Certificate  
   Transparency 313  
 Operational technology (OT)  
   261, 262  
 Organisierte Kriminalität  
   460  
 OSINT 227, 357, 361  
 OVAL 573  
 OWASP 316, 319
- P**
- PaaS 419  
 Paketfilter 553, 557  
 Paketfilter-Firewall 558  
 PAM 161  
 PAP 168  
 Passkeys 152  
 Pass-the-Hash 235, 242  
 Passwort  
   Regeln 151, 170  
 Passwort-Cracker 234, 595  
 Passwort-Guesser 594  
 Passwort Guessing 429, 430,  
   434  
 Passwort-Spraying 593  
 Patch 288  
 Patch-Management 290  
 PBKDF2 131  
 PCI DSS 576  
 PCI-DSS 351, 536  
 PEAP 474  
 PEAP-EAP-TLS 474  
 Penetrationstest 234, 582  
 Penetration Testing 582  
 PEP 160  
 Pepper 436  
 Perfect Forward Secrecy 126  
 Persistence 236  
 Personal Firewall 551, 555  
 Personendaten 70  
 PFS 126, 132  
 PGP 363  
 Pharming 226  
 Phishing 81, 219, 441  
 Phishing-Site 297  
 PII 349  
 PIN-Code 326  
 Ping 540  
 ping6 540  
 Ping of Death 446  
 Pivoting 235  
 Pixie Dust 253  
 PKI 135, 142  
   hierarchische 137, 143  
 Playbook 302, 632  
 PLC 281  
 Policy Administrator 159  
 Policy Enforcement Point 159
- Policy Engine 159  
 Polyglott-Angriff 429  
 Portnummer 410  
 Portscanner 587  
 Port Security 403  
 Positive Rules 553  
 Post Exploitation 234  
 Potentially unwanted pro-  
   grams 201  
 PowerShell 232, 240, 298  
 PPP 409  
 PPTP 476  
 Prepending 361  
 Pretexting 357  
 Privacy by default 77  
 Privacy by design 77  
 Private Cloud 420  
 Privater Schlüssel 123  
 Privilege Escalation 234, 235  
 Problemkategorie 287  
 Prompt Engineering 259  
 Proxy 560  
 PSK 482  
 Public Cloud 420  
 Public-Cloud-Dienst 332  
 Pufferüberlauf 431  
 Punkt-zu-Punkt-Verbindung  
   468  
 Python 232
- Q**
- Quantenkryptografie 127  
 Quarantänebereich  
   NAC 397  
 QUIC 414
- R**
- RA 137  
 Race Condition 434  
 RADIUS 474, 476, 507  
 RAID 612  
 RAID 0 613  
 RAID 1 613  
 RAID 10 615  
 RAID 5 614  
 RAID 50/51 616  
 RAID-Level 612  
 Rainbow-Tabelle 436, 595  
 Ransomware 208, 215, 306  
 Raspberry Pi 256  
 RAS-System 472  
 RAT 232, 234  
 RBAC  
   Zugriffssteuerung 164  
 RC4 122  
 RDR 295  
 Reconnaissance 356  
 Recovery-Agent 142  
 Redundanz 630  
 Refactoring 442
- Registration Authority 137  
 Registrierung 137  
 Release-Note 593  
 Remote-Access 467  
 Remote-Access-VPN  
   VPN 470  
 Remote Sanitation 327  
 Remote Wipe 327, 330  
 Remote-Zugriff 467  
 Replay-Angriff 118, 248, 414,  
   452  
   Session-Replay-Angriff  
   452  
 Reputationslösung 296  
 Resilienz 611  
 Resource Exhaustion Attack  
   228  
 Resource Reuse 432  
 Ressourcenbereitstellung  
   316  
 Retention Policy 634  
 Retina-Scan 154  
 RFC 573  
 RFID 254  
 Richtlinie  
   administrative 58  
   Informationsrichtlinien  
   58  
   Systemicherheitsricht-  
   linien 58  
 RIPEMD 130  
 Risikobewertung 579  
 RMON 522  
 Rogue Access Point 250, 513  
 Rollback 578  
 Rollen 149  
 Rollenbasierte Zugriffskon-  
   trolle 164  
 Rollups 289  
 Rootkit 212, 454  
 Root-Zertifikat 137  
 ROP 308, 431  
 RPO 383, 627  
 RSA 124  
 Rules of Engagement 585  
 Runbook 302
- S**
- S/MIME 363  
 SA 478, 481, 482  
 SaaS 420, 455  
 Safe 182  
 Safe Erase 89  
 Salt 118, 436  
 SAML 149  
 Sandbox 563  
 Sanitation 330  
 SAN-Zertifikat 140  
 SAO 537  
 SASE 160, 161, 562

- SCADA 281, 282  
 Scalper 202  
 scanless 584  
 SCAP 573, 574  
 Scarcity 203  
 Schadensausmaß 579  
 Schadssoftware 200  
 Schleuse 180  
 Schließsystem 176, 178  
 Schlüssel 176  
     öffentlicher 123  
     privater 123  
 Schlüsselbund 365  
 Schlüsselverwaltung 332  
 Schutzbedarf 348  
 Schutzbedarfsfeststellung 54  
 Schwache Verschlüsselung 135  
 Schwachstellen-Scanner 589  
 SCP 412  
 Scraping 202  
 Screenlock 329  
 Script-Kiddies 462  
 Secure Enclave 275  
 Secure Header 319  
 Security Operations Center 571, 592  
 Security-Scanner 589  
 Segregation of Duty 353  
 SEHOP 307, 308, 318  
 Sender Policy Framework 222  
 Serverless 279  
 Serverraum 195  
 Service Pack 289  
 Session-Hijacking 453  
 SHA 129  
 Shimming 442  
 Shoulder surfing 359  
 Sicherheit  
     organisatorische 46  
     physische 46  
     technische 46  
 Sicherheitskritischer Fehler 287  
 Sicherheitsprüfungen 574  
 Sicherheitsrichtlinie 268  
 Sicherheitsvorlage 270  
 Sicherungsverfahren  
     Datensicherung 381  
 Sideloadung 304, 333  
 SIEM 314, 536  
 Signatur  
     digitale 131  
 SIPS 485  
 Site-to-Site  
     VPN 469  
 Skimming 81, 255  
 SLA 388  
     Fehlerraten 388  
     Leistung 388  
 Reaktionsbereitschaft 388  
 Sanktionen 388  
 Verfügbarkeit 388  
 SLIP 409  
 Smishing 225  
 SMON 522  
 SMTP Relay 367  
 Smurf 446  
 SN1PER 585  
 Snapshot 382  
 Sniffing 248  
 SNMP 413, 522  
 SOAR 302, 537  
 SOC 537, 571, 592  
 Social Engineering 341, 354, 355, 361  
 Social Media 371  
 Software-Firewall 276  
 Software Maintenance 287  
 Something you know 150  
 SOX 375  
 Spam 200, 368, 444  
 Spear Phishing 226  
 SPF 222, 299, 368  
 Spim 225, 444  
 Spit 444  
 Spoofing 247, 448, 486  
 Spraying 308, 432  
 Spyware 200, 201, 232, 304  
 SQL-Injection 439  
 SRTP 485  
 SSE 161  
 SSH 411, 484, 554  
 SSID 500  
 SSL 415, 483  
 SSL Stripping 245, 311  
 SSL-Zertifikat 138  
 SSO 149  
 Stack 431  
 STAR-Zertifizierung 423  
 Stateful Packet Inspection Firewall 553, 558  
 Steganografie 456  
 Stimmenerkennung 154  
 Stripe 614  
 Stromverbrauch 194  
 Stromverschlüsseler 118  
 Stromverschlüsselung 119  
 Stromversorgung 188  
 Stuxnet 238  
 SUA 396, 397  
 Subnettierung 395  
 Subnetzmaske 394  
 Supply-Chain-Attacke 238, 463  
 Switch-Überlastung 451  
 SY0-301 656  
 Symmetrische Verschlüsselung 120, 132  
 SYN-Flooding 446  
 System  
     geschlossenes 311  
 Systemhärtung 270  
 Systemintegrität 277  
 Systemsicherheitsrichtlinie 58  
**T**  
 TACACS 475  
 TACACS+ 476  
 Tailgating 359  
 Tastatur 314  
 TCG 274  
 TCP 407  
 TCP-Hijacking 450  
 tcpreplay 564  
 TCSEC 47  
 Technisches Versagen 624  
 Telnet 411  
 Terminalverbindung 411  
 TFTP 411  
 TGT 168  
 The Harvester 585  
 Threat Hunting 295  
 Threat Intelligence 314  
 Ticketsystem 317  
 Timeline 603  
 Time-of-Check-to-Time-of-Use (TOCTTOU) 434  
 TKIP 505  
 TLS 415  
 Tokenisierung 387  
 Tokenization 352  
 TOM 75  
 TOR 216  
 TOTP 153  
 TPM 274, 301  
 Traceroute 542  
 tracert 542  
 tracert-6 542  
 Transitiver Zugriff 441  
 Transitive Trust 333  
 Transport-Modus 479  
 Transportverschlüsselung 411  
 Treibermanipulation 442  
 Triple-A 475  
 Trust-Center 132, 135, 138  
 Trusted Platform Module 274  
 Trust-Modell 135  
 Tunnel-Modus 479  
 Twofish 122  
 Typo squatting 445  
**U**  
 UAC 235  
 UAV 256  
 Überwachung 521  
 UDP 408

- UEFI-BIOS 301
- Unified Threat Management
  - 550, 566
- Update 289
- Upgrade 289
- UPS 188
- URL-Hijacking 445
- URL-Manipulation 441
- URL-Redirection 445
- USB-Kabel
  - bösartiges 245
- User Behaviour Analytics 536
- User-Provisionierung 316
- USV 188, 189
  - Leistung 190
- UTM 550, 566
- V**
- VBA 207, 232
- Venen-Scan 154
- Verfügbarkeit 44
- Verschlüsselung
  - asymmetrische 123, 132
  - hybride 132
  - schwache 135
  - symmetrische 120, 132
- Vertraulichkeit 44
- Videüberwachung 181
- Virenbekämpfung 292
- Virenschutzkonzept 301
- Virenverantwortlicher 301
- Virtualisierung 394
- Virtual Private Cloud 421
- Virus 205, 300
  - Botnet 209
  - Makroviren 207
  - Trojanisches Pferd 209
  - Unterarten 206
  - Würmer 214
- Vishing 224
- VLAN 398
- VLAN Sicherheitsbedenken 405
- VoIP 485
- Vollbackup
  - Datensicherung 381
- Voraussetzung
  - für Zertifizierungen 29
- VPN 467
- VPN-Konzentrator 471
- VPN-Lösung 331
- W**
- Wachpersonal 177
- WAF 319
- Wallets 172
- WAP 508
- War Chalking 489
- War Driving 489
- War Flying 256, 489
- Wartungsfenster 578
- Watering Hole 231
- Webantivirus 297
- Web-Spoofing 450
- WEP 502
- Whaling 226
- Whistleblowing 461
- White-Box-Test 589
- White Hat 459
- Whitelisting 295
- Widerstandsfähigkeit 612
- Wildcard-SSL-Zertifikat 140
- Wiping-Verfahren 328
- WIPS 512
- Wireshark 530
- WLAN
  - Analyse 533
  - Aufbau 498
  - CB 497
  - DFS 492
  - ESS 497
  - Heatmap 500
  - LWAPP 497
  - MAC-Filter 500
  - Outdoor 492
  - Stör- und Dämpfungsfelder 499
  - TPC 492
- Verschlüsselung 500
- Wörterbuch-Angriff 594
- WPA 505
- WPA2 505
  - Enterprise 506
  - PSK 506
- WPA3 506
- WPS 253
- Wrapper 304
- X**
- X.509 136, 138, 482
- XaaS 419
- XDR 243
- Xmas-Attacke 446
- XML-Injection 440
- XSRF 221, 319, 439, 452
- XSS 221, 319, 438
  - Reflective XSS 438
  - Stored XSS 438
- XTACACS 476
- Z**
- Zeitsteuerung
  - Rollen 149
- Zero-Day Exploit 229, 239, 371, 428, 460
- Zero Trust 158
- Zertifikat 137
  - Revocation 142
  - SSL 138
  - zurückziehen 141
- ZTA 158
- ZTNA 158
- Zugriff
  - transitiver 441
- Zugriffskontrolle
  - rollenbasierte 164
- Zugriffsliste 148
- Zugriffssteuerung 162
- Zutrittsregelung 176