



Markus
Kammermann

Markus
a Campo



CompTIA Security+

Vorbereitung auf die Prüfung SY0-301

Inhaltsverzeichnis

1	Laras Welt	15
1.1	Das Ziel dieses Buches	16
1.2	Die CompTIA Security+-Zertifizierung	16
1.3	Voraussetzungen für CompTIA Security+	18
1.4	Persönliches	18
2	Vorbereitungen	21
3	Wo liegt denn das Problem?	29
3.1	Die Risikolage	30
3.2	Kategorien der Informationssicherheit	31
3.3	Lösungsansätze im Überblick	32
3.4	TCSEC, ITSEC und Common Criteria	33
3.5	Die IT-Grundschutzkataloge des BSI	34
3.6	Lösungsansätze für die Praxis	36
3.7	Sicherheitsmanagement und Richtlinien	37
3.8	Fragen zu diesem Kapitel	39
4	Verschlüsselungstechnologie	41
4.1	Grundlagen der Kryptografie	41
4.1.1	One-Time-Pad	42
4.1.2	Blockverschlüsselung	43
4.1.3	Stromverschlüsselung	44
4.2	Symmetrische Verschlüsselung	45
4.2.1	DES	46
4.2.2	3DES	47
4.2.3	AES	47
4.2.4	Blowfish	47
4.2.5	Twofish	48
4.2.6	RC4	48
4.3	Asymmetrische Verschlüsselung	48
4.3.1	RSA	49
4.3.2	Diffie-Hellman	50
4.3.3	Hash-Verfahren	50

4.3.4	MD4 und MD5	51
4.3.5	SHA	52
4.3.6	RIPEMD	53
4.3.7	HMAC	53
4.3.8	Hash-Verfahren mit symmetrischer Verschlüsselung	53
4.3.9	ECC	54
4.3.10	Digitale Signaturen	55
4.4	Hybride Verschlüsselung	55
4.5	PKI in Theorie und Praxis	56
4.5.1	Aufbau einer hierarchischen PKI	57
4.5.2	Zurückziehen von Zertifikaten	59
4.5.3	Hinterlegung von Schlüsseln	59
4.5.4	Aufsetzen einer hierarchischen PKI	59
4.6	Fragen zu diesem Kapitel	60
5	Die Geschichte mit der Identität	63
5.1	Identitäten und deren Rechte	63
5.1.1	Zuweisung von Rechten	63
5.1.2	Rollen	64
5.1.3	Single Sign On	65
5.2	Authentifizierungsmethoden	65
5.2.1	Benutzername und Kennwort	65
5.2.2	Token	66
5.2.3	Zertifikate	67
5.2.4	Biometrie	67
5.2.5	Benutzername, Kennwort und SmartCard	69
5.2.6	Wechselseitige Authentifizierung	70
5.3	Protokolle für die Authentifizierung	70
5.3.1	Kerberos	70
5.3.2	PAP	72
5.3.3	CHAP	72
5.3.4	NTLM	72
5.4	Die Non-Repudiation	73
5.5	Vom Umgang mit Passwörtern	73
5.6	Fragen zu diesem Kapitel	74
6	Physische Sicherheit	75
6.1	Zutrittsregelungen	75
6.1.1	Schlüsselsysteme	77
6.1.2	Badges und Keycards	77

6.1.3	Biometrische Erkennungssysteme	78
6.1.4	Zutrittsschleusen	79
6.1.5	Videüberwachung.	80
6.1.6	Multiple Systeme	81
6.2	Bauschutz.	81
6.2.1	Einbruchschutz.	81
6.2.2	Hochwasserschutz	82
6.2.3	Brandschutz	82
6.2.4	Klimatisierung und Kühlung	84
6.3	Elektrostatische Entladung	85
6.4	Stromversorgung.	86
6.4.1	USV	87
6.4.2	Notstromgruppen.	89
6.4.3	Einsatzszenarien.	90
6.4.4	Rotationsenergiestromversorgungen	91
6.4.5	Ein Wort zu EMP	91
6.5	Fragen zu diesem Kapitel	91
7	Systemsicherheit realisieren	93
7.1	Welche Systeme sind gemeint?	93
7.2	Konfigurationsmanagement.	94
7.3	Das Arbeiten mit Richtlinien	94
7.4	Grundlagen der Systemhärtung.	96
7.4.1	Schutz von Gehäuse und BIOS	98
7.4.2	Sicherheit durch TPM	99
7.4.3	Full Disk Encryption	100
7.4.4	Hardware-Sicherheitsmodul	100
7.5	Ein Wort zu mobilen Geräten.	100
7.6	Softwareaktualisierung ist kein Luxus	102
7.6.1	Vom Hotfix zum Upgrade.	103
7.6.2	Problemkategorien.	104
7.6.3	Maintenance-Produkte.	105
7.6.4	Die Bedeutung des Patch- und Updatemanagements.	106
7.6.5	Entfernen Sie, was Sie nicht brauchen	107
7.7	Viren und Trojaner	108
7.7.1	Die Problematik von Viren	111
7.7.2	Verschiedene Unterarten von Viren	112
7.7.3	Trojanische Pferde	114
7.7.4	Logische Bomben.	116

7.7.5	Würmer	116
7.7.6	Hoaxes	117
7.8	Virenbekämpfung	117
7.8.1	Suchen und Entfernen von Viren	119
7.8.2	Virenschutzkonzept	120
7.8.3	Testen von Installationen	120
7.9	Fragen zu diesem Kapitel	121
8	Der Anwender ist die Schnittstelle	123
8.1	Klassifizierung von Informationen	123
8.2	Der Datenschutz	124
8.3	Vom Umgang mit dem Personal	126
8.4	Social Engineering	127
8.4.1	Phishing	130
8.4.2	Vishing	133
8.4.3	Spear Phishing	133
8.4.4	Pharming	133
8.4.5	Drive-By-Pharming	134
8.5	E-Mail-Sicherheit	134
8.5.1	Secure Multipurpose Internet Mail Extensions (S/MIME)	135
8.5.2	PGP (Pretty Good Privacy)	136
8.5.3	Schwachstellen	139
8.6	Daten sichern	142
8.6.1	Datensicherung oder Datenarchivierung?	143
8.6.2	Die gesetzlichen Grundlagen	144
8.6.3	Das Datensicherungskonzept	146
8.6.4	Methoden der Datensicherung	147
8.6.5	Online-Backup	149
8.7	Data Loss Prevention	151
8.8	Fragen zu diesem Kapitel	151
9	Sicherheit für Netzwerke	153
9.1	Zugriffssteuerungsmodelle	153
9.1.1	Mandatory Access Control (MAC)	153
9.1.2	Discretionary Access Control (DAC)	155
9.1.3	Role Based Access Control (RBAC)	155
9.1.4	Principle of Least Privileges	157
9.2	Trennung von IT-Systemen	157
9.2.1	Subnettierung von Netzen	158
9.2.2	NAT	160

9.2.3	VLAN	160
9.2.4	Network Access Control	161
9.3	TCP/IP-Kernprotokolle	161
9.3.1	Internet Protocol	162
9.3.2	Internet Control Message Protocol	162
9.3.3	Transmission Control Protocol	163
9.3.4	User Datagram Protocol	164
9.4	Weitere Transport- und Netzwerkprotokolle	164
9.4.1	Address Resolution Protocol	164
9.4.2	Internet Group Management Protocol	165
9.4.3	SLIP und PPP	165
9.4.4	IP Version 6	165
9.5	Anwendungen	166
9.5.1	Portnummern	166
9.5.2	Telnet	166
9.5.3	SSH	167
9.5.4	FTP	167
9.5.5	SCP, SFTP und FTPS	167
9.5.6	TFTP	167
9.5.7	DNS	168
9.5.8	SNMP	168
9.5.9	E-Mail-Protokolle	169
9.5.10	HTTP	169
9.5.11	SSL und TLS	170
9.5.12	NetBIOS und CIFS	171
9.5.13	Lightweight Directory Access	171
9.6	Fragen zu diesem Kapitel	172
10	Schwachstellen und Attacken	175
10.1	Angriffe gegen IT-Systeme	176
10.1.1	Denial of Service	176
10.1.2	Pufferüberlauf	178
10.1.3	Race-Condition	178
10.1.4	Password Guessing und Cracking	179
10.2	Input Validation	180
10.3	Angriffe gegen Anwendungen	181
10.3.1	Directory-Traversal	181
10.3.2	Cross Site Scripting	182
10.3.3	SQL-Injection	182

10.3.4	LDAP-Injection	183
10.3.5	XML-Injection	183
10.3.6	Command-Injection	183
10.3.7	Parameter-Manipulation	183
10.3.8	Transitive Zugriffe	184
10.3.9	Phishing	185
10.4	Angriffe gegen Clients	185
10.4.1	Attachments	186
10.4.2	Drive-By-Attack	186
10.4.3	Böswillige Add-ons	186
10.4.4	Spam, Spim und Spit	186
10.5	Netzwerkangriffe	186
10.5.1	Denial of Service (DoS)	187
10.5.2	Distributed Denial of Service (DDoS)	188
10.5.3	Spoofing	188
10.5.4	Man in the Middle	189
10.5.5	Replay-Angriff	192
10.5.6	SSL-Downgrading	192
10.5.7	Session-Hijacking	193
10.5.8	Brechen von Schlüsseln	194
10.5.9	Backdoor	194
10.6	Angriffe gegen die Cloud	195
10.7	Steganografie	195
10.8	Von Hüten und Angreifern	196
10.9	Fragen zu diesem Kapitel	197
II	Remotezugriff	199
II.1	Virtual Private Network	199
II.1.1	Site-to-Site-VPN	201
II.1.2	Remote-Access-VPN	201
II.1.3	Soft- und Hardwarelösungen	202
II.2	Remote Access Server	203
II.3	Protokolle für den entfernten Zugriff	204
II.3.1	802.1X	204
II.3.2	RADIUS	205
II.3.3	TACACS	206
II.3.4	L2TP und PPTP	207
II.3.5	IPsec	208

II.3.6	SSL	213
II.3.7	SSH	213
II.4	Schwachstellen	215
II.4.1	Man in the Middle	215
II.4.2	Identitäts-Spoofing	215
II.4.3	Botnets	215
II.5	Fragen zu diesem Kapitel	216
12	Drahtlostechnologien und -konzepte	219
12.1	Aller Standard beginnt mit IEEE 802.11	219
12.2	Der Netzaufbau	222
12.2.1	Das Ad-hoc-Netzwerk	222
12.2.2	Das Infrastrukturnetzwerk	222
12.2.3	Aufbau einer drahtlosen Verbindung	223
12.3	Sicherheit in drahtlosen Verbindungen	225
12.3.1	Wired Equivalent Privacy	226
12.3.2	WPA und 802.11i	228
12.3.3	Die Implementierung von 802.1X	230
12.3.4	Das Extensible Authentication Protocol (EAP)	231
12.3.5	WAP (Wireless Application Protocol)	232
12.4	Grundlegende Sicherheitsmaßnahmen	233
12.5	Bluetooth – Risiken und Maßnahmen	235
12.6	Fragen zu diesem Kapitel	237
13	System- und Netzwerküberwachung	241
13.1	SNMP-Protokolle	242
13.2	Leistungsüberwachung	246
13.3	Das Monitoring von Netzwerken	247
13.4	Monitoring-Programme	248
13.4.1	Der Windows-Netzwerkmonitor	248
13.4.2	Wireshark	251
13.4.3	MRTG	252
13.4.4	Nagios	254
13.5	Firewalls	254
13.5.1	Personal Firewalls und dedizierte Firewalls	256
13.5.2	Paketfilter-Firewall	258
13.5.3	Stateful Packet Firewall	259
13.5.4	Application Level Gateway	260
13.5.5	Anwendungsbeispiele	262

13.6	IDS und IPS	264
13.7	Unified Threat Management	266
13.8	Fragen zu diesem Kapitel	267
14	Penetration Testing und Forensics	269
14.1	Penetration Testing	269
14.1.1	Organisatorische Einbettung	269
14.1.2	Prinzipielle Vorgehensweise	270
14.1.3	Black Box und White Box.	272
14.1.4	Security-Scanner	273
14.1.5	Datenbanken für Recherchen nach Sicherheitslücken	274
14.1.6	Passwort-Guesser und -Cracker.	275
14.1.7	Paketgeneratoren	276
14.1.8	Netzwerk-Sniffer.	277
14.1.9	Fuzzing	277
14.1.10	Metasploit Framework	277
14.2	Forensics.	278
14.2.1	Aufgaben und Fragestellungen	278
14.2.2	Vorbereitung	279
14.2.3	Sichern von Beweismitteln	280
14.2.4	Beweissicherung nach RFC 3227	280
14.2.5	Schutz von Beweismitteln	281
14.2.6	Analyse von Beweismitteln	282
14.2.7	Timeline	283
14.2.8	Data-Carving	284
14.2.9	Suche nach Zeichenketten	285
14.2.10	Nutzung von Hash-Datenbanken	285
14.2.11	Programme und Toolkits	286
14.3	Fragen zu diesem Kapitel	287
15	Die Notfallplanung	289
15.1	Fehlertoleranz	289
15.1.1	RAID	290
15.1.2	RAID Level	290
15.1.3	Festplattenausfall	294
15.1.4	Duplexing	294
15.1.5	Übersicht RAID	295
15.2	Redundante Verbindungen und Systeme	295
15.2.1	Network Loadbalancing	295
15.2.2	Cluster	296

15.3	Notfallvorsorgeplanung	296
15.4	Analyse	298
15.4.1	Ausfallszenarien	298
15.4.2	Impact-Analyse	298
15.5	Umsetzung	299
15.5.1	Strategie und Planung	299
15.5.2	Verschiedene Implementierungsansätze	301
15.6	Test des Disaster-Recovery-Plans	303
15.7	Wartung der Disaster Recovery	303
15.7.1	Punktuelle Anpassungen	303
15.7.2	Regelmäßige Überprüfung	304
15.8	Merkmale zur Disaster Recovery	304
15.9	Fragen zum Kapitel	305
16	Security-Audit	309
16.1	Grundlagen von Security-Audits	309
16.1.1	Fragestellungen	309
16.1.2	Prinzipielle Vorgehensweise	310
16.1.3	Bestandteile eines Security-Audits	311
16.2	Standards	311
16.2.1	ISO 27001	311
16.2.2	IT-Grundschutzkataloge	312
16.2.3	Kombination aus ISO 27000 und IT-Grundschutz	313
16.3	Beispiel-Audit Windows Server 2008	314
16.3.1	Nutzung von Sicherheitsvorlagen	314
16.3.2	Einsatz von Kommandos und Skripten	315
16.3.3	Passwortschutz	315
16.3.4	Geräteschutz	315
16.3.5	Sichere Basiskonfiguration	315
16.3.6	Sichere Installation und Bereitstellung	316
16.3.7	Sichere Konfiguration der IIS-Basis-Komponente	316
16.3.8	Sichere Migration auf Windows Server 2003/2008	316
16.3.9	Umgang mit Diensten unter Windows Server	316
16.3.10	Deinstallation nicht benötigter Client-Funktionen	317
16.3.11	Verwendung der Softwareeinschränkungsrichtlinie	317
16.4	Berichtswesen	317
16.4.1	Titelseite	317
16.4.2	Einleitung	317
16.4.3	Management-Summary	318

16.4.4	Ergebnisse der Untersuchung	318
16.4.5	Erforderliche Maßnahmen	318
16.4.6	Anhang	319
16.5	Ergänzende Maßnahmen	319
16.5.1	Logfile-Analyse	320
16.5.2	Echtzeit-Analyse von Netzwerkverkehr und Zugriffen	321
16.5.3	Risikoanalyse	321
16.6	Fragen zu diesem Kapitel	321
17	Die CompTIA Security+-Prüfung	323
17.1	Was von Ihnen verlangt wird	324
17.2	Wie Sie sich vorbereiten können	325
17.3	Wie eine Prüfung aussieht	325
17.4	Beispielfragen zur Prüfung CompTIA Security+	330
A	Antworten zu den Fragen	343
A.1	Antworten zu den Vorbereitungsfragen	343
A.2	Antworten zu den Kapitelfragen	343
A.3	Antworten zu den Beispielfragen	345
B	Glossar	347
	Stichwortverzeichnis	357