



Mathias  
Gut

Markus  
Kammermann

4. Auflage



# CompTIA Security+

IT-Sicherheit verständlich erklärt

Die umfassende Prüfungsvorbereitung  
zur CompTIA-Prüfung SY0-601



## **Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)**

Liebe Leserinnen und Leser,

dieses E-Book, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Mit dem Kauf räumen wir Ihnen das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Jede Verwertung außerhalb dieser Grenzen ist ohne unsere Zustimmung unzulässig und strafbar. Das gilt besonders für Vervielfältigungen, Übersetzungen sowie Einspeicherung und Verarbeitung in elektronischen Systemen.

Je nachdem wo Sie Ihr E-Book gekauft haben, kann dieser Shop das E-Book vor Missbrauch durch ein digitales Rechtemanagement schützen. Häufig erfolgt dies in Form eines nicht sichtbaren digitalen Wasserzeichens, das dann individuell pro Nutzer signiert ist. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Beim Kauf des E-Books in unserem Verlagsshop ist Ihr E-Book DRM-frei.

Viele Grüße und viel Spaß beim Lesen,

*Ihr mitp-Verlagsteam*



Neuerscheinungen, Praxistipps, Gratiskapitel,  
Einblicke in den Verlagsalltag –  
gibt es alles bei uns auf Instagram und Facebook



[instagram.com/mitp\\_verlag](https://www.instagram.com/mitp_verlag)



[facebook.com/mitp.verlag](https://www.facebook.com/mitp.verlag)

# Inhaltsverzeichnis

## Impressum

### **Kapitel 1: Laras Welt**

- 1.1 Das Ziel dieses Buches
- 1.2 Die CompTIA Security+-Zertifizierung
- 1.3 Voraussetzungen für CompTIA Security+
- 1.4 Persönliches

### **Kapitel 2: Sind Sie bereit für CompTIA Security+?**

### **Kapitel 3: Wo liegt denn das Problem?**

- 3.1 Fangen Sie bei sich selbst an
- 3.2 Die Gefahrenlage
- 3.3 Die Analyse der Bedrohungslage
- 3.4 Kategorien der Informationssicherheit
- 3.5 Modelle und Lösungsansätze
  - 3.5.1 TCSEC oder ITSEC
  - 3.5.2 Common Criteria
  - 3.5.3 ISO 27000
  - 3.5.4 Das NIST Cybersecurity Framework
- 3.6 Der IT-Grundschutz nach BSI
- 3.7 Lösungsansätze für Ihr Unternehmen
  - 3.7.1 Das Information Security Management System
  - 3.7.2 Sicherheitsmanagement und Richtlinien
  - 3.7.3 Die Notfallvorsorge

3.7.4 Risiken durch Dritte

3.7.5 Die Cyber-Security-Strategie

3.8 Fragen zu diesem Kapitel

## **Kapitel 4: Rechtliche Grundlagen**

4.1 Warum ist Datenschutz für Sie relevant?

4.1.1 Die Ursprünge des Datenschutzes

4.1.2 Datenschutz-Compliance für Unternehmen

4.1.3 Datenschutz als Beruf

4.2 Was sind Personendaten?

4.2.1 Relativer vs. absoluter Ansatz

4.2.2 Was sind Personendaten nach relativem Ansatz?

4.2.3 Anonymisierte und pseudonymisierte Daten

4.2.4 Anwendungsbeispiele

4.2.5 Besonders sensible Daten

4.3 Was hat Datenschutz mit Datensicherheit zu tun?

4.3.1 Was bedeuten die gesetzlichen Vorgaben für die Praxis?

4.3.2 Data Breach Notifications

4.3.3 Datenschutzfreundliches Design und ebensolche Konfiguration

4.3.4 Haftungsrisiko bei Missachtung der Datensicherheit

4.4 Inwiefern wird Missbrauch von Daten unter Strafe gestellt?

4.4.1 Unbefugte Datenbeschaffung (sog. Datendiebstahl)

4.4.2 Unbefugtes Eindringen in ein Datenverarbeitungssystem

- 4.4.3 Datenbeschädigung
- 4.4.4 Betrügerischer Missbrauch einer Datenverarbeitungsanlage
- 4.4.5 Erschleichen einer Leistung
- 4.4.6 Unbefugte Entschlüsselung codierter Angebote
- 4.4.7 Unbefugtes Beschaffen von Personendaten
- 4.4.8 Phishing und Skimming
- 4.4.9 Verletzung von Berufs-, Fabrikations- und Geschäftsgeheimnissen
- 4.4.10 Massenversand von Werbung (Spam)
- 4.5 Wann ist welches Gesetz anwendbar?
  - 4.5.1 Sachlicher Anwendungsbereich
  - 4.5.2 Räumlicher Anwendungsbereich
- 4.6 Welche Grundsätze müssen eingehalten werden?
- 4.7 Der Grundsatz der Datenminimierung
  - 4.7.1 Unterschied zwischen Datensicherung und -archivierung
  - 4.7.2 Weshalb müssen Daten gesichert und archiviert werden?
  - 4.7.3 Verwaltung der zu sichernden und zu archivierenden Daten
  - 4.7.4 Wie werden nicht mehr benötigte Daten sicher vernichtet?
- 4.8 Welche Rechte haben die betroffenen Personen?
  - 4.8.1 Recht auf Information
  - 4.8.2 Recht auf Auskunft
  - 4.8.3 Berichtigung, Einschränkung und Löschung
  - 4.8.4 Recht auf Datenübertragbarkeit
  - 4.8.5 Widerspruchsrecht
  - 4.8.6 Beschwerderecht

4.9 Was ist bei der Zusammenarbeit mit Dritten zu beachten?

4.9.1 Auftragsbearbeiter

4.9.2 Gemeinsame Verantwortliche

4.9.3 Bearbeitung im Konzern

4.9.4 Datenexporte

4.10 Haftungsrisiken bei Datenschutzverletzungen

4.11 Fragen zu diesem Kapitel

## **Kapitel 5: Verschlüsselungstechnologie**

5.1 Grundlagen der Kryptografie

5.1.1 Einige Grundbegriffe

5.1.2 One-Time-Pad

5.1.3 Diffusion und Konfusion

5.1.4 Blockverschlüsselung

5.1.5 Stromverschlüsselung

5.2 Symmetrische Verschlüsselung

5.2.1 DES

5.2.2 3DES

5.2.3 AES

5.2.4 Blowfish

5.2.5 Twofish

5.2.6 RC4

5.3 Asymmetrische Verschlüsselung

5.3.1 RSA

5.3.2 Diffie-Hellman

5.3.3 ECC

5.3.4 Perfect Forward Secrecy (PFS)

5.3.5 Die Zukunft der Quanten



## 5.4 Hash-Verfahren

### 5.4.1 MD4 und MD5

### 5.4.2 SHA

### 5.4.3 RIPEMD

### 5.4.4 HMAC

### 5.4.5 Hash-Verfahren mit symmetrischer Verschlüsselung

### 5.4.6 Digitale Signaturen

### 5.4.7 Hybride Verschlüsselung

## 5.5 Drei Status digitaler Daten

### 5.5.1 Data-in-transit

### 5.5.2 Data-at-rest

### 5.5.3 Data-in-use

## 5.6 Bekannte Angriffe gegen die Verschlüsselung

### 5.6.1 Cipher-text-only-Angriff

### 5.6.2 Known/Chosen-plain-text-Angriff

### 5.6.3 Schwache Verschlüsselung / Implementierung

### 5.6.4 Probleme mit Zertifikaten

## 5.7 PKI in Theorie und Praxis

### 5.7.1 Aufbau einer hierarchischen PKI

### 5.7.2 SSL-Zertifikate X.509 Version 3

### 5.7.3 Zertifikatstypen

### 5.7.4 Zurückziehen von Zertifikaten

### 5.7.5 Hinterlegung von Schlüsseln

### 5.7.6 Aufsetzen einer hierarchischen PKI

## 5.8 Fragen zu diesem Kapitel

# **Kapitel 6: Die Geschichte mit der Identität**

## 6.1 Identitäten und deren Rechte

- 6.1.1 Zuweisung von Rechten
- 6.1.2 Rollen
- 6.1.3 Single Sign On
- 6.2 Authentifizierungsmethoden
  - 6.2.1 Benutzername und Kennwort
  - 6.2.2 Token
  - 6.2.3 Zertifikate
  - 6.2.4 Biometrie
  - 6.2.5 Benutzername, Kennwort und Smartcard
  - 6.2.6 Tokenization
  - 6.2.7 Wechselseitige Authentifizierung
- 6.3 Zugriffssteuerungsmodelle
  - 6.3.1 Mandatory Access Control (MAC)
  - 6.3.2 Discretionary Access Control (DAC)
  - 6.3.3 Role Based Access Control (RBAC)
  - 6.3.4 ABAC - Attributbasiertes Zugriffssystem
  - 6.3.5 Principle of Least Privileges
- 6.4 Protokolle für die Authentifizierung
  - 6.4.1 Kerberos
  - 6.4.2 PAP
  - 6.4.3 CHAP
  - 6.4.4 NTLM
  - 6.4.5 Die Non-Repudiation
- 6.5 Vom Umgang mit Passwörtern
- 6.6 Fragen zu diesem Kapitel

## **Kapitel 7: Physische Sicherheit**

- 7.1 Zutrittsregelungen
  - 7.1.1 Das Zonenkonzept

- 7.1.2 Schlüsselsysteme
- 7.1.3 Badges und Keycards
- 7.1.4 Biometrische Erkennungssysteme
- 7.1.5 Zutrittsschleusen
- 7.1.6 Videoüberwachung
- 7.1.7 Multiple Systeme
- 7.2 Bauschutz
  - 7.2.1 Einbruchsschutz
  - 7.2.2 Hochwasserschutz
  - 7.2.3 Brandschutz
  - 7.2.4 Klimatisierung und Kühlung
- 7.3 Elektrostatische Entladung
- 7.4 Stromversorgung
  - 7.4.1 USV
  - 7.4.2 Notstromgruppen
  - 7.4.3 Einsatzszenarien
  - 7.4.4 Rotationsenergiestromversorgungen
  - 7.4.5 Ein Wort zu EMP
- 7.5 Feuchtigkeit und Temperatur
- 7.6 Fragen zu diesem Kapitel

## **Kapitel 8: Im Angesicht des Feindes**

- 8.1 Malware ist tatsächlich böse
  - 8.1.1 Die Problematik von Malware
  - 8.1.2 Viren und ihre Unterarten
  - 8.1.3 Wie aus Trojanischen Pferden böse Trojaner wurden
  - 8.1.4 Backdoor
  - 8.1.5 Logische Bomben

- 8.1.6 Würmer
- 8.1.7 Ransomware
- 8.1.8 Krypto-Malware (Cryptomalware)
- 8.1.9 Fileless Malware
- 8.1.10 Hoaxes
- 8.2 Angriffe mittels Social Engineering
  - 8.2.1 Phishing
  - 8.2.2 Vishing und Smishing
  - 8.2.3 Spear Phishing
  - 8.2.4 Pharming
  - 8.2.5 Drive-by-Pharming
  - 8.2.6 Doxing
- 8.3 Angriffe gegen IT-Systeme
  - 8.3.1 Exploits und Exploit-Kits
  - 8.3.2 Darknet und Darkweb
  - 8.3.3 Malwaretising
  - 8.3.4 Watering-Hole-Attacke
  - 8.3.5 Malware Dropper und Malware-Scripts
  - 8.3.6 RAT (Remote Access Tool/Remote Access Trojan)
  - 8.3.7 Keylogger
  - 8.3.8 Post Exploitation
- 8.4 Gefahren für die Nutzung mobiler Geräte und Dienste
- 8.5 APT – Advanced Persistent Threats
  - Stuxnet
  - 8.5.1 Carbanak
- 8.6 Advanced Threats
  - 8.6.1 Evasion-Techniken

- 8.6.2 Pass-the-Hash-Angriffe (PtH)
- 8.6.3 Kaltstartattacke (Cold Boot Attack)
- 8.6.4 Physische RAM-Manipulation über DMA (FireWire-Hack)
- 8.6.5 Human Interface Device Attack (Teensy USB HID Attack)
- 8.6.6 BAD-USB-Angriff
- 8.6.7 Böses USB-Kabel
- 8.6.8 SSL-Stripping-Angriff
- 8.6.9 Angriff über Wireless-Mäuse
- 8.7 Angriffe in Wireless-Netzwerken
  - 8.7.1 Spoofing in Wireless-Netzwerken
  - 8.7.2 Sniffing in drahtlosen Netzwerken
  - 8.7.3 DNS-Tunneling in Public WLANs
  - 8.7.4 Rogue Access Point/Evil Twin
  - 8.7.5 Attacken auf die WLAN-Verschlüsselung
  - 8.7.6 Verschlüsselung brechen mit WPS-Attacken
  - 8.7.7 Denial-of-Service-Angriffe im WLAN
  - 8.7.8 Angriffe auf NFC-Technologien
  - 8.7.9 Angriffe auf Keycards
- 8.8 Moderne Angriffsformen
  - 8.8.1 Angriffe mittels Drohnen
  - 8.8.2 Verwundbare Anwendungen nachladen
  - 8.8.3 Angriffe auf Application Programming Interface (API)
  - 8.8.4 Gefahren durch künstliche Intelligenz (KI)
  - 8.8.5 Das Internet of Things
- 8.9 Fragen zu diesem Kapitel

## **Kapitel 9: Systemsicherheit realisieren**

- 9.1 Konfigurationsmanagement
- 9.2 Das Arbeiten mit Richtlinien
- 9.3 Grundlagen der Systemhärtung
  - 9.3.1 Schutz von Gehäuse und BIOS
  - 9.3.2 Sicherheit durch TPM
  - 9.3.3 Full Disk Encryption
  - 9.3.4 Softwarebasierte Laufwerksverschlüsselung
  - 9.3.5 Hardware-Sicherheitsmodul
  - 9.3.6 Software-Firewall (Host-based Firewall)
  - 9.3.7 Systemintegrität
  - 9.3.8 Überlegungen bei der Virtualisierung
- 9.4 Embedded-Systeme und Industriesysteme
- 9.5 Softwareaktualisierung ist kein Luxus
  - 9.5.1 Vom Hotfix zum Upgrade
  - 9.5.2 Problemkategorien
  - 9.5.3 Maintenance-Produkte
  - 9.5.4 Die Bedeutung des Patch- und Update-Managements
  - 9.5.5 Entfernen Sie, was Sie nicht brauchen
- 9.6 Malware bekämpfen
  - 9.6.1 Endpoint-Protection am Client
  - 9.6.2 Reputationslösungen
  - 9.6.3 Aktivitätsüberwachung HIPS/HIDS
  - 9.6.4 Online-Virens Scanner – Webantivirus-NIPS
  - 9.6.5 Sensibilisierung der Mitarbeitenden
  - 9.6.6 Suchen und Entfernen von Viren
  - 9.6.7 Virenschutzkonzept
  - 9.6.8 Testen von Installationen
  - 9.6.9 Sicher und vertrauenswürdig ist gut

## 9.7 Advanced Threat Protection

9.7.1 Explizites Applikations-Whitelisting versus -  
Blacklisting

9.7.2 Explizites Whitelisting auf Firewalls

9.7.3 Erweiterter Exploit-Schutz

9.7.4 Virtualisierung von Anwendungen

9.7.5 Schutz vor HID-Angriffen und BAD-USB

9.7.6 Geschlossene Systeme

9.7.7 Schutz vor SSL-Stripping-Angriffen

9.7.8 Schutz vor Angriffen über drahtlose Mäuse

9.7.9 Security- und Threat Intelligence

## 9.8 Anwendungssicherheit

9.8.1 Lifecycle-Management/DevOps

9.8.2 Sichere Codierungskonzepte

9.8.3 Input Validation

9.8.4 Fehler- und Ausnahmebehandlung

9.8.5 Memory Leak

9.8.6 NoSQL- versus SQL-Datenbanken

9.8.7 Serverseitige versus clientseitige Validierung

9.8.8 Session Token

9.8.9 Web-Application-Firewall (WAF)

## 9.9 Fragen zu diesem Kapitel

# **Kapitel 10: Sicherheit für mobile Systeme**

10.1 Die Risikolage mit mobilen Geräten und Diensten

10.2 Organisatorische Sicherheitsmaßnahmen

10.3 Technische Sicherheitsmaßnahmen

10.3.1 Vollständige Geräteverschlüsselung (Full  
Device Encryption)

- 10.3.2 Gerätesperren (Lockout)
- 10.3.3 Bildschirmsperre (Screenlocks)
- 10.3.4 Remote Wipe/Sanitization
- 10.3.5 Standortdaten (GPS) und Asset Tracking
- 10.3.6 Sichere Installationsquellen und Anwendungssteuerung
- 10.3.7 VPN-Lösungen auf mobilen Geräten
- 10.3.8 Public-Cloud-Dienste auf mobilen Geräten
- 10.4 Anwendungssicherheit bei mobilen Systemen
  - 10.4.1 Schlüsselmanagement (Key-Management)
  - 10.4.2 Credential-Management
  - 10.4.3 Authentifizierung
  - 10.4.4 Geo-Tagging
  - 10.4.5 Verschlüsselung
  - 10.4.6 Whitelisting von Anwendungen
  - 10.4.7 Transitive Trust/Authentifizierung
- 10.5 Fragen rund um BYOD
  - 10.5.1 Dateneigentum (Data Ownership)
  - 10.5.2 Zuständigkeit für den Unterhalt (Support Ownership)
  - 10.5.3 Antivirus-Management
  - 10.5.4 Patch-Management
  - 10.5.5 Forensik
  - 10.5.6 Privatsphäre und Sicherheit der geschäftlichen Daten
  - 10.5.7 Akzeptanz der Benutzer und akzeptable Benutzung ...
  - 10.5.8 Architektur-/Infrastrukturüberlegungen
  - 10.5.9 On-Board-Kamera/Video
- 10.6 Fragen zu diesem Kapitel



# **Kapitel 11: Den DAU gibt's wirklich - und Sie sind schuld**

## 11.1 Klassifizierung von Informationen

11.1.1 Die Klassifizierung nach Status

11.1.2 Die Klassifizierung nach Risiken

11.1.3 Data Loss Prevention

11.1.4 Was es zu beachten gilt

## 11.2 Der Datenschutz im internationalen Umfeld

## 11.3 Vom Umgang mit dem Personal

## 11.4 Umgang mit Social Engineering

11.4.1 Praktiken, Ziele und Vorgehensweisen von Social Engineers

11.4.2 Informationsbeschaffung von OSINT bis Dumpster Diving

11.4.3 Pretexting und authentische Geschichten

11.4.4 Shoulder surfing

11.4.5 Tailgating

11.4.6 Gezielte Beeinflussung und Falschinformation (Influence campaigns)

11.4.7 CEO Fraud / Rechnungsbetrug

11.4.8 Prepending

11.4.9 Awareness-Schulungen und Reglements

## 11.5 E-Mail-Sicherheit

11.5.1 Secure Multipurpose Internet Mail Extensions (S/MIME)

11.5.2 PGP (Pretty Good Privacy)

11.5.3 Schwachstellen

11.5.4 Schutz durch einen Mail-Gateway

11.5.5 Social Media

## 11.6 Daten sichern

11.6.1 Datensicherung oder Datenarchivierung?

11.6.2 Die gesetzlichen Grundlagen

11.6.3 Das Datensicherungskonzept

11.6.4 Methoden der Datensicherung

11.6.5 Online-Backup

11.6.6 Daten vernichten

## 11.7 Sicherheit im Umgang mit Servicepartnern

## 11.8 Fragen zu diesem Kapitel

# **Kapitel 12: Sicherheit für Netzwerke**

## 12.1 Trennung von IT-Systemen

12.1.1 Subnettierung von Netzen

12.1.2 NAT

12.1.3 Network Access Control

## 12.2 VLAN

12.2.1 Planung und Aufbau von VLANs

12.2.2 Vorgehen gegen Risiken bei Switch-Infrastrukturen

12.2.3 Port Security

12.2.4 Flood Guard

12.2.5 Spanning-Tree Protocol und Loop Protection

12.2.6 Maßnahmen gegen Gefahren in VLANs

## 12.3 TCP/IP-Kernprotokolle

12.3.1 Internet Protocol

12.3.2 Internet Control Message Protocol

12.3.3 Transmission Control Protocol

12.3.4 User Datagram Protocol (UDP)

## 12.4 Weitere Transport- und Netzwerkprotokolle

- 12.4.1 Address Resolution Protocol (ARP)
- 12.4.2 Internet Group Management Protocol (IGMP)
- 12.4.3 SLIP und PPP
- 12.4.4 IP-Version 6
- 12.4.5 Portnummern
- 12.5 Anwendungen
  - 12.5.1 Telnet und SSH
  - 12.5.2 FTP und TFTP
  - 12.5.3 SCP, SFTP und FTPS
  - 12.5.4 DNS
  - 12.5.5 SNMP
  - 12.5.6 E-Mail-Protokolle
  - 12.5.7 HTTP
  - 12.5.8 SSL und TLS
  - 12.5.9 NetBIOS und CIFS
  - 12.5.10 Lightweight Directory Access (LDAP)
- 12.6 Sicherheit in der Cloud
  - 12.6.1 Cloud-Computing-Betriebsmodelle
  - 12.6.2 Sicherheit in der Wolke
  - 12.6.3 Formen des Einsatzes
- 12.7 Fragen zu diesem Kapitel

## **Kapitel 13: Schwachstellen und Attacken**

- 13.1 Welches Risiko darf es denn sein?
- 13.2 Angriffe gegen IT-Systeme
  - 13.2.1 Denial of Service
  - 13.2.2 Pufferüberlauf
  - 13.2.3 Race-Condition
  - 13.2.4 Password Guessing und Cracking

## 13.3 Angriffe gegen Anwendungen

13.3.1 Directory-Traversal

13.3.2 Cross Site Scripting

13.3.3 Cross-Site Request Forgery (XSRF)

13.3.4 Injection-Varianten

13.3.5 Parametermanipulation

13.3.6 Transitive Zugriffe

13.3.7 Phishing

13.3.8 Treibermanipulationen

## 13.4 Angriffe gegen Clients

13.4.1 Drive by Attack

13.4.2 Böswillige Add-ons und Applets

13.4.3 Local Shared Objects (LSOs)

13.4.4 Spam, Spim und Spit

13.4.5 Typo squatting bzw. URL-Hijacking

13.4.6 URL-Redirection

13.4.7 Clickjacking

13.4.8 Domain Hijacking

13.4.9 Man in the Browser

## 13.5 Netzwerkangriffe

13.5.1 Denial of Service (DoS)

13.5.2 Distributed Denial of Service (DDoS)

13.5.3 Spoofing

13.5.4 Man in the Middle

13.5.5 Replay-Angriff

13.5.6 SSL-Downgrading

13.5.7 Session-Hijacking

13.5.8 Brechen von Schlüsseln

13.5.9 Backdoor

13.6 Angriffe gegen die Public Cloud

13.7 Steganografie

13.8 Akteure und ihre Motive

13.8.1 Generelle Eigenschaften der verschiedenen Angreifer

13.8.2 Von Hütern und Angreifern

13.8.3 Staatliche Akteure (State actors)

13.8.4 Organisierte Kriminalität (Criminal syndicates)

13.8.5 Wirtschaftsspionage (Competitors) und interne Täter

13.8.6 Hacktivisten (Hacktivists)

13.8.7 Script-Kiddies

13.8.8 Die Schatten-IT (Shadow IT)

13.8.9 Bug-Bounty

13.9 Fragen zu diesem Kapitel

## **Kapitel 14: Der sichere Remote-Zugriff**

14.1 Virtual Private Network

14.1.1 Site-to-Site-VPN

14.1.2 Remote-Access-VPN

14.1.3 Soft- und Hardwarelösungen

14.2 Remote Access Server

14.3 Protokolle für den entfernten Zugriff

14.3.1 802.1x

14.3.2 RADIUS

14.3.3 TACACS, XTACACS und TACACS+

14.3.4 L2TP und PPTP

14.3.5 IPsec

14.3.6 SSL/TLS

14.3.7 SSH

14.3.8 SRTP

14.4 Schwachstellen

14.5 Fragen zu diesem Kapitel

## **Kapitel 15: Drahtlose Netzwerke sicher gestalten**

15.1 Aller WLAN-Standard beginnt mit IEEE 802.11

15.1.1 Die frühen IEEE-Standards von 802.11

15.1.2 Die Gegenwart heißt Wi-Fi 6

15.2 Die Verbindungsaufnahme im WLAN

15.2.1 Das Ad-hoc-Netzwerk

15.2.2 Das Infrastrukturnetzwerk

15.2.3 Erweitertes Infrastrukturnetz

15.3 Ein WLAN richtig aufbauen

15.3.1 Aufbau der Hardware

15.3.2 Konfiguration des drahtlosen Netzwerks

15.4 Sicherheit in drahtlosen Verbindungen

15.4.1 Wired Equivalent Privacy

15.4.2 Von WPA bis WPA3

15.4.3 Die Implementierung von 802.1x

15.4.4 Das Extensible Authentication Protocol (EAP)

15.4.5 WAP (Wireless Application Protocol)

15.4.6 Near Field Communication

15.5 Grundlegende Sicherheitsmaßnahmen umsetzen

15.6 Wireless Intrusion Prevention System

15.7 Bluetooth – Risiken und Maßnahmen

15.8 Fragen zu diesem Kapitel

## **Kapitel 16: System- und Netzwerküberwachung**

16.1 Das OSI-Management-Framework

16.2 SNMP-Protokolle

16.3 Leistungsüberwachung

16.4 Das Monitoring von Netzwerken

16.5 Monitoring-Programme

16.5.1 Der Windows-Netzwerkmonitor

16.5.2 Wireshark

16.5.3 inSSIDer

16.5.4 MRTG bzw. RRDTools

16.5.5 Nagios

16.6 Proaktive Sicherheit dank SIEM

16.7 Kommandozeilenprogramme

16.7.1 ipconfig/ip

16.7.2 ping

16.7.3 ARP

16.7.4 tracert/traceroute

16.7.5 nslookup

16.7.6 netstat

16.8 Fragen zu diesem Kapitel

## **Kapitel 17: Brandschutzmauer für das Netzwerk**

17.1 Damit kein Feuer ausbricht

17.2 Personal Firewalls und dedizierte Firewalls

17.3 Das Regelwerk einer Firewall

17.3.1 Positive Exceptions (Positive Rules)

17.3.2 Negative Exceptions (Negative Rules)

17.4 Das Konzept der DMZ

- 17.4.1 Trennung Hostsystem von den virtuellen Maschinen
- 17.4.2 Trennung bei WLAN-Infrastrukturen
- 17.4.3 Extranet und Intranet
- 17.5 Nicht jede Firewall leistet dasselbe
  - 17.5.1 Wenn einfach auch reicht: Die Paketfilter-Firewall
  - 17.5.2 Der nächste Level: Stateful Packet Inspection Firewall
  - 17.5.3 Jetzt wird's gründlich: Application Level Gateway
  - 17.5.4 Anwendungsbeispiele
  - 17.5.5 Unified Threat Management Firewall
- 17.6 Die Angreifer kommen – aber Sie wissen's schon
- 17.7 Unified Threat Management
- 17.8 Fragen zu diesem Kapitel

## **Kapitel 18: Sicherheit überprüfen und analysieren**

- 18.1 Informationsbeschaffung
  - 18.1.1 Branchen- und Interessensverbände
  - 18.1.2 Fachmedien
  - 18.1.3 Schwachstelleninformationen
  - 18.1.4 Sicherheitskonferenzen
  - 18.1.5 Hersteller-Webseiten
- 18.2 Penetration Testing
  - 18.2.1 Organisatorische Einbettung
  - 18.2.2 Prinzipielle Vorgehensweise
  - 18.2.3 Black Box und White Box
  - 18.2.4 Security-Scanner



18.2.5 Datenbanken für Recherchen nach Sicherheitslücken

18.2.6 Passwort-Guesser und -Cracker

18.2.7 Paketgeneratoren und Netzwerk-Sniffer

18.2.8 Fuzzing

18.2.9 Metasploit Framework

### 18.3 Forensik

18.3.1 Vorbereitung

18.3.2 Sichern von Beweismitteln

18.3.3 Beweissicherung nach RFC 3227

18.3.4 Schutz und Analyse von Beweismitteln

18.3.5 Timeline

18.3.6 Data-Carving

18.3.7 Suche nach Zeichenketten

18.3.8 Nutzung von Hash-Datenbanken

18.3.9 Programme und Toolkits

### 18.4 Fragen zu diesem Kapitel

## **Kapitel 19: Wider den Notfall**

19.1 Was ist denn ein Notfall?

19.2 Resilienz dank Fehlertoleranz

19.2.1 Aller Anfang ist RAID

19.2.2 RAID Level

19.2.3 Duplexing

19.2.4 Übersicht RAID

19.3 Redundante Verbindungen und Systeme

19.3.1 Network Loadbalancing

19.3.2 Cluster

19.4 Notfallvorsorgeplanung

- 19.4.1 Bedrohungsanalyse
- 19.4.2 Von der Bedrohung bis zur Maßnahme
- 19.5 Ein guter Plan beginnt mit einer guten Analyse
  - 19.5.1 Ausfallszenarien
  - 19.5.2 Impact-Analyse
- 19.6 Methoden der Umsetzung
  - 19.6.1 Strategie und Planung
  - 19.6.2 Die Rolle des Risiko-Managements
  - 19.6.3 Verschiedene Implementierungsansätze
  - 19.6.4 Incident-Response-Prozesse und Incident Response Plan
- 19.7 Test und Wartung des Notfallplans
  - 19.7.1 Wartung der Disaster Recovery
  - 19.7.2 Punktuelle Anpassungen
  - 19.7.3 Regelmäßige Überprüfung
  - 19.7.4 Merkmale zur Datenwiederherstellung
- 19.8 Fragen zu diesem Kapitel

## **Kapitel 20: Security-Audit**

- 20.1 Grundlagen von Security-Audits
  - 20.1.1 Fragestellungen
  - 20.1.2 Prinzipielle Vorgehensweise
  - 20.1.3 Bestandteile eines Security-Audits
- 20.2 Standards
  - 20.2.1 ISO 27001
  - 20.2.2 IT-Grundschutz nach BSI
  - 20.2.3 Kombination aus ISO 27000 und IT-Grundschutz
- 20.3 Beispiel-Audit Windows Server 2019

- 20.3.1 Nutzung von Sicherheitsvorlagen
- 20.3.2 Einsatz von Kommandos und Scripts
- 20.3.3 Passwortschutz
- 20.3.4 Geräteschutz
- 20.3.5 Sichere Basiskonfiguration
- 20.3.6 Sichere Installation und Bereitstellung
- 20.3.7 Sichere Konfiguration der IIS-Basis-Komponente
- 20.3.8 Sichere Migration auf Windows Server 2019
- 20.3.9 Umgang mit Diensten unter Windows Server
- 20.3.10 Deinstallation nicht benötigter Client-Funktionen
- 20.3.11 Verwendung der Softwareeinschränkungsrichtlinie

## 20.4 Berichtswesen

- 20.4.1 Titelseite
- 20.4.2 Einleitung
- 20.4.3 Management-Summary
- 20.4.4 Ergebnisse der Untersuchung
- 20.4.5 Erforderliche Maßnahmen
- 20.4.6 Anhang

## 20.5 Ergänzende Maßnahmen

- 20.5.1 Logfile-Analyse
- 20.5.2 Echtzeitanalyse von Netzwerkverkehr und Zugriffen
- 20.5.3 Risikoanalyse

## 20.6 Fragen zu diesem Kapitel

# **Kapitel 21: Die CompTIA Security+-Prüfung**

## 21.1 Was von Ihnen verlangt wird

21.2 Wie Sie sich vorbereiten können

21.3 Wie eine Prüfung aussieht

21.4 Beispielprüfung zum Examen CompTIA Security+

## **Anhang A: Anhänge**

A.1 Antworten zu den Vorbereitungsfragen

A.2 Antworten zu den Kapitelfragen

A.3 Antworten zu Fragen der Beispielprüfung

A.4 Weiterführende Literatur

A.4.1 Nützliche Literatur zum Thema

A.4.2 Weiterführende Links zum Thema

## **Anhang B: Abkürzungsverzeichnis**

Mathias Gut, Markus Kammermann

# **CompTIA Security+**

**IT-Sicherheit verständlich erklärt**

**Die umfassende  
Prüfungsvorbereitung zur CompTIA-  
Prüfung SYO-601**

**CompTIA**<sup>®</sup>

 **certins**<sup>®</sup>  
certified technical trainings and courseware



**mitp**