16.7 Merksätze und Prüfungswissen zu Angriffen und Schutzmaßnahmen

Diese Seite fasst die wichtigsten Inhalte zu Angriffen, Schwachstellen, Schadsoftware, Phishing, Netzwerkangriffen, Webangriffen und Schutzmaßnahmen zusammen.

Das Thema ist prüfungsrelevant, weil es viele Bereiche verbindet:

```
- Informationssicherheit
- Netzwerktechnik
- Betriebssysteme
- Anwendungen
- Benutzerkonten
- Cloud
- Backup
- Datenschutz
- Monitoring
- Incident Response
```

Merksatz:

```
IT-Sicherheit schützt Vertraulichkeit,
Integrität
und Verfügbarkeit.
```

Die drei wichtigsten Schutzziele

Die wichtigsten Schutzziele der Informationssicherheit sind:

```
Vertraulichkeit

Integrität

Verfügbarkeit
```

Diese drei Begriffe bilden die Grundlage vieler Sicherheitsfragen.

Merksatz:

Vertraulichkeit,
Integrität
und Verfügbarkeit immer sauber unterscheiden.

Vertraulichkeit

Vertraulichkeit bedeutet:

Informationen dürfen nur von berechtigten Personen gelesen werden.

Beispiele:

Kundendaten
Passwörter
Personalakten
interne Dokumente
Zugangsdaten
Geschäftsgeheimnisse

Angriffe auf Vertraulichkeit:

Phishing
Sniffing
Spyware
Datenabfluss
unberechtigte Freigaben
gestohlene Zugangsdaten

Merksatz:

Vertraulichkeit schützt vor unberechtigtem Lesen.

Integrität

Integrität bedeutet:

Daten dürfen nicht unbemerkt verändert werden.

Beispiele:

Rechnung wird manipuliert.
Datenbankeintrag wird verändert.
Konfigurationsdatei wird heimlich angepasst.
Softwareupdate wird verfälscht.

Angriffe auf Integrität:

Man-in-the-Middle
Malware
SQL Injection
Supply-Chain-Angriff
unberechtigte Änderung

Merksatz:

Integrität schützt vor unbemerkter Manipulation.

Verfügbarkeit

Verfügbarkeit bedeutet:

Systeme,
Dienste
und Daten sind bei Bedarf nutzbar.

Beispiele:

Webseite erreichbar
Datenbank verfügbar
Netzwerk funktioniert
Dateien sind nutzbar
Backup kann wiederhergestellt werden

Angriffe auf Verfügbarkeit:

```
DoS
DDoS
Ransomware
Sabotage
Überlastung
Systemausfall
```

Merksatz:

```
Verfügbarkeit schützt die Nutzbarkeit von IT-Systemen.
```

CIA-Triade

CIA steht für:

```
Confidentiality
Integrity
Availability
```

Deutsch:

```
Vertraulichkeit
Integrität
Verfügbarkeit
```

Merksatz:

```
CIA-Triade = Vertraulichkeit,
Integrität
Verfügbarkeit.
```

Authentizität

Authentizität bedeutet:

Die Echtheit einer Person,
eines Systems
oder einer Nachricht ist überprüfbar.

Beispiele:

Ist der Benutzer wirklich der richtige Benutzer?
Ist der Server wirklich der richtige Server?
Stammt die Nachricht wirklich vom angegebenen Absender?

Merksatz:

Authentizität schützt vor falscher Identität.

Nichtabstreitbarkeit

Nichtabstreitbarkeit bedeutet:

Eine Handlung kann später nachgewiesen werden
und nicht glaubwürdig abgestritten werden.

Beispiele:

digitale Signatur
Zeitstempel
Audit-Log
eindeutiges Benutzerkonto

Merksatz:

Nichtabstreitbarkeit sorgt für Nachweisbarkeit.

Schwachstelle, Bedrohung und Risiko

Begriff	Bedeutung
Schwachstelle	ausnutzbare Sicherheitslücke

Begriff	Bedeutung
Bedrohung	mögliches schädliches Ereignis
Risiko	Wahrscheinlichkeit und Auswirkung eines Schadens
Schutzmaßnahme	reduziert ein Risiko

Merksatz:

> Schwachstelle ist die Lücke.
> Bedrohung ist das Ereignis.
> Risiko ist die bewertete Gefahr.

Angriffsfläche

Angriffsfläche bedeutet:

> alle Stellen,
> an denen ein System angegriffen werden kann.

Beispiele:

> offene Ports
> Webanwendungen
> Benutzerkonten
> VPN-Zugänge
> E-Mail
> APIs
> Cloud-Freigaben
> veraltete Software
> unsichere Dienste

Merksatz:

> Je größer die Angriffsfläche,
> desto mehr mögliche Angriffspunkte.

Angriffsfläche reduzieren

Maßnahmen:

```
unnötige Dienste deaktivieren
offene Ports reduzieren
Standardkonten deaktivieren
starke Authentifizierung nutzen
Systeme patchen
Rechte begrenzen
Netzbereiche segmentieren
öffentliche Freigaben prüfen
sichere Konfiguration verwenden
```

Merksatz:

```
Nicht benötigte Dienste und Zugänge entfernen.
```

Malware

Malware ist ein Oberbegriff für Schadsoftware.

Beispiele:

```
Virus
Wurm
Trojaner
Ransomware
Spyware
Keylogger
Rootkit
Botnet-Client
Cryptominer
```

Merksatz:

```
Malware ist Software mit schädlicher Funktion.
```

Virus

Ein Virus hängt sich häufig an Dateien oder Programme an und wird aktiv, wenn diese ausgeführt werden.

Merksatz:

```
Virus braucht oft eine Wirtsdatei oder Benutzeraktion.
```

Wurm

Ein Wurm verbreitet sich selbstständig über Netzwerke oder Schwachstellen.

Merksatz:

```
Wurm verbreitet sich selbstständig.
```

Trojaner

Ein Trojaner tarnt sich als nützliches Programm, enthält aber Schadfunktionen.

Merksatz:

```
Trojaner täuscht Harmlosigkeit oder Nützlichkeit vor.
```

Ransomware

Ransomware verschlüsselt Daten oder sperrt Systeme und fordert Lösegeld.

Sie betrifft besonders:

```
Verfügbarkeit
```

und oft zusätzlich:

```
Vertraulichkeit
```

Merksatz:

```
Ransomware greift Verfügbarkeit
und bei Datenabfluss auch Vertraulichkeit an.
```

Double Extortion

Double Extortion bedeutet:

```
Daten werden verschlüsselt

und

zusätzlich wird mit Veröffentlichung gestohlener Daten gedroht.
```

Merksatz:

```
Double Extortion = Verschlüsselung plus Datenabfluss.
```

Schutz vor Ransomware

Wichtige Maßnahmen:

```
Immutable Backups
Offline-Backups
regelmäßige Restore-Tests
Patchmanagement
EDR
MFA
Least Privilege
keine lokalen Adminrechte
Netzwerksegmentierung
Monitoring
schnelle Isolation betroffener Systeme
```

Merksatz:

```
Gegen Ransomware sind Backup,
Rechtebegrenzung
```

Segmentierung

und schnelle Reaktion besonders wichtig.

Phishing

Phishing ist Täuschung, um Benutzer zur Preisgabe vertraulicher Informationen oder zu gefährlichen Aktionen zu bringen.

Ziele:

Passwörter

MFA-Codes

Zugangstokens

Bankdaten

Cloud-Zugänge

VPN-Zugänge

interne Informationen

Merksatz:

Phishing greift Menschen über Täuschung an.

Social Engineering

Social Engineering manipuliert Menschen, um Sicherheitsmaßnahmen zu umgehen.

Angreifer nutzen:

Zeitdruck

Angst

Autorität

Hilfsbereitschaft

Vertrauen

Neugier

Gewohnheit

Merksatz:

Social Engineering greift Verhalten und Prozesse an.

Spear Phishing und Whaling

Spear Phishing:

gezieltes Phishing gegen bestimmte Personen oder Organisationen

Whaling:

Phishing gegen besonders wichtige Personen

Beispiele für Whaling-Ziele:

Geschäftsführung
Finanzleitung
Administratoren
Personalabteilung

Merksatz:

Spear Phishing ist gezielt.
Whaling trifft besonders wertvolle Ziele.

Smishing, Vishing und Quishing

Begriff	Bedeutung
Smishing	Phishing per SMS
Vishing	Phishing per Telefon
Quishing	Phishing über QR-Code

Merksatz:

Phishing ist nicht auf E-Mail beschränkt.

CEO-Fraud und BEC

CEO-Fraud:

```
Angreifer geben sich als Führungskraft aus
und fordern dringende Aktionen.
```

BEC:

```
Business E-Mail Compromise,
Missbrauch oder Nachahmung geschäftlicher E-Mail-Kommunikation.
```

Merksatz:

```
CEO-Fraud und BEC nutzen Vertrauen,
Autorität
und Geschäftsprozesse.
```

Identitätsangriffe

Identitätsangriffe richten sich gegen Benutzerkonten und Anmeldungen.

Typische Formen:

```
Brute Force
Credential Stuffing
Password Spraying
Phishing
Session Hijacking
MFA-Missbrauch
Account Takeover
```

Merksatz:

```
Wer Identitäten kontrolliert,
kontrolliert oft den Zugriff.
```

Brute Force

Brute Force bedeutet:

Passwörter werden systematisch ausprobiert.

Schutz:

starke Passwörter
MFA
Rate Limiting
Sperrmechanismen
Monitoring

Merksatz:

Brute Force wird durch Begrenzung und MFA erschwert.

Credential Stuffing

Credential Stuffing bedeutet:

geleakte Zugangsdaten aus anderen Diensten werden erneut ausprobiert.

Schutz:

eindeutige Passwörter
Passwortmanager
MFA
Leak-Erkennung

Merksatz:

Credential Stuffing nutzt Passwort-Wiederverwendung.

Password Spraying

Password Spraying bedeutet:

wenige häufige Passwörter werden gegen viele Konten getestet.

Merksatz:

```
Password Spraying verteilt wenige Passwörter auf viele Benutzer.
```

MFA

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

MFA schützt, weil zusätzlich zum Passwort ein weiterer Faktor nötig ist.

Merksatz:

```
MFA reduziert Schaden durch gestohlene Passwörter.
```

MFA ist nicht unfehlbar

Mögliche Angriffe trotz MFA:

```
MFA-Push-Fatigue
gestohlene Session-Tokens
Phishing mit Echtzeit-Weiterleitung
kompromittiertes Endgerät
Social Engineering beim Support
SIM-Swapping bei SMS-MFA
```

Merksatz:

```
MFA ist sehr wichtig,
aber kein vollständiger Ersatz für Sicherheitskonzept.
```

DoS und DDoS

DoS:

```
Denial of Service
```

DDoS:

```
Distributed Denial of Service
```

Unterschied:

Angriff	Bedeutung
DoS	Dienst wird gestört oder überlastet
DDoS	verteilter DoS von vielen Quellen

Merksatz:

```
DoS und DDoS greifen Verfügbarkeit an.
```

DDoS-Schutz

Maßnahmen:

```
DDoS-Schutzdienst
Provider-Unterstützung
CDN
Anycast
Load Balancer
Rate Limiting
Firewall-Regeln
WAF
Monitoring
Notfallplan
```

Merksatz:

```
DDoS-Schutz muss vorbereitet sein.
```

Man-in-the-Middle

Bei Man-in-the-Middle befindet sich ein Angreifer zwischen zwei Kommunikationspartnern.

Ziele:

Daten mitlesen
Daten verändern
Zugangsdaten abgreifen
Sitzungen übernehmen

Merksatz:

MitM sitzt zwischen Sender und Empfänger.

Schutz vor Man-in-the-Middle

Maßnahmen:

TLS korrekt nutzen
Zertifikate prüfen
Zertifikatswarnungen nicht ignorieren
VPN in unsicheren Netzen
HSTS
sichere WLAN-Konfiguration
DNS-Schutz
MFA

Merksatz:

TLS schützt nur,
wenn Zertifikate korrekt geprüft werden.

Sniffing

Sniffing bedeutet:

Netzwerkverkehr wird mitgeschnitten oder beobachtet.

Es kann genutzt werden für:

Fehlersuche

oder missbraucht werden für:

Abhören
Passwortdiebstahl
Sitzungsdiebstahl

Merksatz:

Sniffing ist Werkzeug und Risiko zugleich.

Spoofing

Spoofing bedeutet:

Herkunft,
Adresse
oder Identität wird vorgetäuscht.

Beispiele:

IP-Spoofing
MAC-Spoofing
ARP-Spoofing
DNS-Spoofing
E-Mail-Spoofing

Merksatz:

Spoofing täuscht Identität oder Herkunft vor.

ARP-Spoofing

ARP-Spoofing manipuliert die Zuordnung von IPv4-Adresse zu MAC-Adresse im lokalen Netz.

Mögliche Folge:

Man-in-the-Middle

Schutz:

```
DHCP Snooping
Dynamic ARP Inspection
Segmentierung
TLS
```

Merksatz:

```
ARP-Spoofing greift lokale Layer-2-Kommunikation an.
```

DNS-Spoofing

DNS-Spoofing manipuliert die Namensauflösung.

Folge:

```
Benutzer wird zu falscher IP-Adresse geleitet.
```

Schutz:

```
vertrauenswürdige DNS-Resolver
DNSSEC
TLS-Zertifikatsprüfung
sichere DHCP-Konfiguration
```

Merksatz:

```
DNS-Spoofing führt Namen zu falschen Zielen.
```

Rogue DHCP

Rogue DHCP bedeutet:

```
ein unautorisierter DHCP-Server verteilt falsche Netzwerkeinstellungen.
```

Mögliche Folgen:

falsches Gateway
falscher DNS-Server
Man-in-the-Middle
Netzwerkstörung

Schutz:

DHCP Snooping
Switchport-Sicherheit
Monitoring
physische Zugangskontrolle

Merksatz:

Rogue DHCP verteilt falsche Netzwerkkonfiguration.

WLAN-Angriffe

Typische WLAN-Angriffe:

Evil Twin
Rogue Access Point
unsichere Verschlüsselung
falsches Captive Portal
Deauthentication
Mitschneiden unverschlüsselter Kommunikation

Schutz:

WPA2-Enterprise oder WPA3
802.1X
starke Passwörter
Zertifikatsprüfung
Gastnetztrennung
Rogue-AP-Erkennung

Merksatz:

WLAN braucht Verschlüsselung,
Authentifizierung
und Segmentierung.

Webangriffe

Typische Webangriffe:

SQL Injection
Cross-Site Scripting
Cross-Site Request Forgery
Directory Traversal
File Upload Attack
Broken Authentication
Broken Access Control
unsichere APIs
unsichere Fehlerausgaben

Merksatz:

Webangriffe nutzen oft Eingaben,
Sitzungen
oder Berechtigungen aus.

SQL Injection

SQL Injection bedeutet:

Angreifer schleust SQL-Code in Eingaben ein.

Folgen:

Daten auslesen
Daten verändern
Login umgehen
Daten löschen

Schutz:

```
Prepared Statements
parametrisierte Abfragen
Eingabevalidierung
Datenbankrechte begrenzen
```

Merksatz:

```
SQL Injection macht Eingabe zu Datenbankbefehl.
```

Cross-Site Scripting

Cross-Site Scripting wird abgekürzt:

```
XSS
```

Dabei wird Skriptcode in eine Webseite eingeschleust, der im Browser anderer Benutzer ausgeführt wird.

Schutz:

```
Ausgabe escapen
Eingaben validieren
Content Security Policy
HttpOnly Cookies
sichere Frameworks
```

Merksatz:

```
XSS greift Benutzer über den Browser an.
```

CSRF

CSRF steht für:

```
Cross-Site Request Forgery
```

Dabei wird eine bestehende Anmeldung missbraucht, um ungewollte Aktionen auszulösen.

Schutz:

```
CSRF-Token
SameSite Cookies
Origin-Prüfung
erneute Bestätigung kritischer Aktionen
```

Merksatz:

```
CSRF missbraucht eine gültige Sitzung.
```

SQL Injection, XSS und CSRF unterscheiden

Angriff	Ziel	Kernproblem
SQL Injection	Datenbank	Eingabe wird SQL-Befehl
XSS	Browser anderer Benutzer	Eingabe wird Skript
CSRF	bestehende Sitzung	fremde Seite löst Aktion aus

Merksatz:

```
SQL Injection trifft Datenbank.
XSS trifft Browser.
CSRF missbraucht Sitzung.
```

Broken Authentication

Broken Authentication bedeutet:

```
Anmeldung oder Sitzungsverwaltung ist unsicher.
```

Beispiele:

```
kein MFA
schwache Passwörter
unsichere Passwortzurücksetzung
```

zu lange Sessions
Tokens unsicher gespeichert

Merksatz:

Broken Authentication gefährdet Konten und Sitzungen.

Broken Access Control

Broken Access Control bedeutet:

Benutzer können auf Daten oder Funktionen zugreifen,
für die sie keine Berechtigung haben.

Beispiele:

fremde Rechnung über geänderte ID anzeigen
Adminfunktion als normaler Benutzer aufrufen
API gibt fremde Daten zurück

Merksatz:

Zugriffskontrolle muss serverseitig geprüft werden.

IDOR

IDOR steht für:

Insecure Direct Object Reference

Dabei kann ein Benutzer durch Änderung einer ID auf fremde Objekte zugreifen.

Merksatz:

IDOR ist fehlende Objektberechtigung.

Schwachstellenmanagement

Schwachstellenmanagement bedeutet:

Schwachstellen erkennen,
bewerten,
priorisieren,
beheben
und dokumentieren.

Dazu gehören:

Inventarisierung
CVE-Bewertung
CVSS-Einordnung
Patchmanagement
Schwachstellenscans
Penetrationstests
Hardening
Dokumentation

Merksatz:

Schwachstellenmanagement ist ein dauerhafter Prozess.

CVE und CVSS

CVE:

eindeutige Kennung für bekannte Schwachstellen

CVSS:

Bewertung der Kritikalität einer Schwachstelle

Merksatz:

CVE benennt.
CVSS bewertet.

Exploit und Zero-Day

Exploit:

> Methode oder Code zur Ausnutzung einer Schwachstelle

Zero-Day:

> Schwachstelle,
> für die noch kein regulärer Patch verfügbar ist
> oder die noch nicht öffentlich bekannt war

Merksatz:

> Exploit nutzt eine Lücke.
> Zero-Day nutzt eine ungepatchte oder unbekannte Lücke.

Patchmanagement

Patchmanagement bedeutet:

> Updates werden geplant,
> getestet,
> verteilt
> geprüft
> und dokumentiert.

Betroffen sind:

> Betriebssysteme
> Anwendungen
> Browser
> Datenbanken
> Firewalls
> Router
> Switches
> Firmware

Container-Images
Bibliotheken
Cloud-Systeme

Merksatz:

Patchmanagement ist organisierte Update-Verwaltung.

Patchmanagement-Ablauf

Typischer Ablauf:

1. Systeme inventarisieren.
2. Schwachstellen prüfen.
3. Betroffenheit bewerten.
4. Kritikalität priorisieren.
5. Patch testen.
6. Wartungsfenster planen.
7. Patch ausrollen.
8. Funktion prüfen.
9. Erfolg dokumentieren.
10. Rest-Risiko bewerten.

Merksatz:

Patchmanagement braucht Inventar,
Priorisierung,
Test,
Rollback
und Dokumentation.

Hardening

Hardening bedeutet:

Systeme werden sicherer konfiguriert,
indem unnötige Funktionen deaktiviert

und sichere Einstellungen gesetzt werden.

Beispiele:

unnötige Dienste deaktivieren
offene Ports reduzieren
Standardpasswörter ändern
alte Protokolle abschalten
Rechte minimieren
Logging aktivieren
Adminzugriffe begrenzen

Merksatz:

Hardening reduziert Angriffsfläche.

Baseline

Eine Baseline ist ein definierter sicherer Grundzustand.

Beispiele:

erlaubte Dienste
Passwortregeln
Update-Einstellungen
Logging-Pflicht
Firewall-Grundregeln
TLS-Vorgaben
Rechtevorgaben

Merksatz:

Baseline = festgelegte sichere Standardkonfiguration.

Configuration Drift

Configuration Drift bedeutet:

Die tatsächliche Konfiguration weicht von der geplanten Baseline ab.

Ursachen:

manuelle Änderungen
Notfalländerungen
fehlende Dokumentation
unterschiedliche Installationen

Merksatz:

Configuration Drift macht Systeme schwerer sicher zu betreiben.

Firewall

Eine Firewall filtert Netzwerkverkehr.

Sie prüft zum Beispiel:

Quelle
Ziel
Port
Protokoll
Richtung
Verbindungszustand
Anwendung je nach Firewalltyp

Merksatz:

Firewall begrenzt Netzwerkzugriffe.

Default Deny

Default Deny bedeutet:

standardmäßig ist alles verboten,
nur ausdrücklich erlaubter Verkehr ist erlaubt.

Merksatz:

> Default Deny ist sicherer als pauschales Erlauben.

IDS und IPS

IDS:

> Intrusion Detection System
>
> erkennt und meldet Angriffe

IPS:

> Intrusion Prevention System
>
> erkennt und blockiert Angriffe zusätzlich

Merksatz:

> IDS meldet.
> IPS greift ein.

Antivirus, EDR und XDR

Antivirus:

> erkennt vor allem bekannte Schadsoftware

EDR:

> Endpoint Detection and Response,
> erkennt und untersucht Angriffe auf Endgeräten

XDR:

Extended Detection and Response,
verbindet mehrere Sicherheitsbereiche

Merksatz:

EDR ist umfassender als klassischer Antivirus.

SIEM, SOC und SOAR

SIEM:

sammelt und korreliert Sicherheitslogs

SOC:

Security Operations Center,
organisatorische Stelle für Sicherheitsüberwachung

SOAR:

automatisiert Sicherheitsreaktionen

Merksatz:

SIEM sammelt Daten.
SOC bewertet.
SOAR automatisiert Reaktionen.

Backup

Backup ist eine zusätzliche Sicherung zur Wiederherstellung.

Wichtig:

regelmäßig
geschützt

verschlüsselt
getrennt
dokumentiert
getestet

Merksatz:

Backup ohne Restore-Test ist unsicher.

Immutable Backup

Immutable Backup bedeutet:

Backup kann für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Schutz gegen:

Ransomware
versehentliche Löschung
kompromittierte Adminzugänge

Merksatz:

Immutable Backup schützt Wiederherstellungsmöglichkeiten.

Incident Response

Incident Response bedeutet:

strukturierte Reaktion auf Sicherheitsvorfälle.

Typische Schritte:

erkennen
bewerten
eindämmen
beseitigen

wiederherstellen
dokumentieren
verbessern

Merksatz:

Incident Response muss vorbereitet sein,
bevor ein Vorfall passiert.

Containment, Eradication und Recovery

Phase	Bedeutung
Containment	Vorfall eindämmen
Eradication	Ursache beseitigen
Recovery	Systeme wiederherstellen

Merksatz:

Erst eindämmen,
dann Ursache beseitigen,
dann sicher wiederherstellen.

Defense in Depth

Defense in Depth bedeutet:

mehrere Schutzschichten werden kombiniert.

Beispiel:

Firewall
plus
MFA
plus
Patchmanagement
plus
EDR

plus
Backup
plus
Monitoring
plus
Schulung

Merksatz:

Sicherheit darf nicht von einer einzigen Maßnahme abhängen.

Technische, organisatorische, personelle und physische Maßnahmen

Maßnahmenart	Beispiele
technisch	Firewall, MFA, EDR, Backup, Verschlüsselung
organisatorisch	Richtlinien, Prozesse, Verantwortlichkeiten
personell	Schulung, Awareness, klare Meldewege
physisch	Zutrittskontrolle, Serverraum, Brandschutz

Merksatz:

Sicherheit besteht aus Technik,
Organisation,
Menschen
und physischem Schutz.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was sind die drei Schutzziele der Informationssicherheit?
- Was bedeutet Vertraulichkeit?
- Was bedeutet Integrität?
- Was bedeutet Verfügbarkeit?
- Was ist der Unterschied zwischen Schwachstelle,
  Bedrohung
  und Risiko?

- Was ist Malware?
- Was ist der Unterschied zwischen Virus und Wurm?
- Was ist Ransomware?
- Was ist Phishing?
- Was ist Social Engineering?
- Was ist der Unterschied zwischen DoS und DDoS?
- Was ist Man-in-the-Middle?
- Was ist Spoofing?
- Was ist SQL Injection?
- Was ist XSS?
- Was ist CSRF?
- Was ist CVE?
- Was ist CVSS?
- Was ist Patchmanagement?
- Was ist Hardening?
- Was ist eine Firewall?
- Was ist der Unterschied zwischen IDS und IPS?
- Was ist EDR?
- Was ist SIEM?
- Warum sind Backups wichtig?
- Was ist Incident Response?
- Was bedeutet Defense in Depth?

Typische Prüfungsfallen

Vertraulichkeit,
Integrität
und Verfügbarkeit nicht verwechseln.

Ransomware betrifft nicht nur Verfügbarkeit,
sondern oft auch Vertraulichkeit.

Malware ist ein Oberbegriff.

Virus und Wurm unterscheiden.

Phishing ist nicht nur E-Mail.

Social Engineering ist nicht rein technisch.

DoS und DDoS unterscheiden.

DDoS ist verteilt.

MitM sitzt zwischen Kommunikationspartnern.

Spoofing täuscht Herkunft oder Identität vor.

DNSSEC schützt Integrität,
nicht automatisch Vertraulichkeit.

SQL Injection betrifft Datenbanken.

XSS betrifft Browser.

CSRF missbraucht Sitzungen.

Prepared Statements schützen gegen SQL Injection.

Frontend-Validierung ist keine Sicherheitsgrenze.

Zugriffskontrolle muss serverseitig erfolgen.

CVE benennt Schwachstellen.

CVSS bewertet Kritikalität.

Hoher CVSS-Wert ersetzt keine eigene Risikoanalyse.

Patchmanagement ist ein Prozess.

Hardening ist sichere Konfiguration.

Firewall ersetzt kein Patchmanagement.

Antivirus ersetzt kein Sicherheitskonzept.

IDS erkennt,
IPS blockiert zusätzlich.

EDR ist mehr als Antivirus.

SIEM sammelt und korreliert Logs.

Backup verhindert keinen Angriff,
hilft aber bei Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Security Awareness ist eine Schutzmaßnahme.

Incident Response muss vorbereitet sein.

Sicherheit ist ein Prozess,
kein einmaliger Zustand.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Vertraulichkeit	Schutz vor unberechtigtem Lesen
Integrität	Schutz vor unbemerkter Veränderung
Verfügbarkeit	Nutzbarkeit von Systemen und Daten
Authentizität	Echtheit einer Identität oder Nachricht
Nichtabstreitbarkeit	Nachweisbarkeit einer Handlung
Schwachstelle	ausnutzbare Sicherheitslücke
Bedrohung	mögliches schädliches Ereignis
Risiko	Wahrscheinlichkeit und Auswirkung
Angriffsfläche	Summe möglicher Angriffspunkte
Malware	Schadsoftware
Virus	Schadsoftware mit Wirtsdatei
Wurm	selbstverbreitende Schadsoftware
Trojaner	getarnte Schadsoftware
Ransomware	erpresserische Verschlüsselung oder Sperrung
Phishing	Täuschung zur Datenpreisgabe
Social Engineering	Manipulation von Menschen

Begriff	Kurze Erklärung
Brute Force	systematisches Ausprobieren
Credential Stuffing	Nutzung geleakter Zugangsdaten
Password Spraying	wenige Passwörter gegen viele Konten
DoS	Dienstverweigerung
DDoS	verteilte Dienstverweigerung
MitM	Man-in-the-Middle
Sniffing	Mitschneiden von Verkehr
Spoofing	Vortäuschen falscher Identität
ARP-Spoofing	Manipulation lokaler IP-MAC-Zuordnung
DNS-Spoofing	Manipulation von DNS-Antworten
Rogue DHCP	unautorisierter DHCP-Server
Evil Twin	gefälschter WLAN-Access-Point
SQL Injection	Einschleusen von SQL-Code
XSS	Cross-Site Scripting
CSRF	Cross-Site Request Forgery
IDOR	unsichere direkte Objekt-ID
CVE	Kennung bekannter Schwachstellen
CVSS	Kritikalitätsbewertung
Exploit	Ausnutzung einer Schwachstelle
Zero-Day	ungepatchte oder unbekannte Schwachstelle
Patchmanagement	organisierte Update-Verwaltung
Hardening	sichere Systemhärtung
Baseline	sicherer Grundzustand
Configuration Drift	Abweichung von Soll-Konfiguration
Firewall	Filter für Netzwerkverkehr
IDS	Angriffserkennung
IPS	Angriffserkennung mit Blockierung
Antivirus	Schutz gegen bekannte Schadsoftware
EDR	Endpoint Detection and Response
XDR	Extended Detection and Response
SIEM	Sicherheitslog-Auswertung
SOC	Security Operations Center

Begriff	Kurze Erklärung
SOAR	automatisierte Sicherheitsreaktion
MFA	Multi-Faktor-Authentifizierung
Least Privilege	minimale notwendige Rechte
Backup	zusätzliche Datensicherung
Immutable Backup	unveränderliches Backup
Restore-Test	Prüfung der Wiederherstellung
Incident Response	Reaktion auf Sicherheitsvorfälle
Defense in Depth	mehrschichtige Verteidigung

IHK-sichere Gesamtformulierung

Angriffe und Schutzmaßnahmen in der IT-Sicherheit beziehen sich auf den Schutz der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Angriffe können technische Schwachstellen, unsichere Konfigurationen, menschliches Verhalten, Identitäten, Netzwerke, Webanwendungen oder Lieferketten ausnutzen. Typische Angriffe sind Malware, Ransomware, Phishing, Social Engineering, DoS, DDoS, Man-in-the-Middle, Spoofing, SQL Injection, Cross-Site Scripting und Cross-Site Request Forgery. Schutzmaßnahmen sind unter anderem Patchmanagement, Hardening, Firewalls, Netzwerksegmentierung, MFA, Least Privilege, IDS/IPS, EDR, SIEM, Backups, Restore-Tests, Monitoring, Logging, Schulungen und Incident Response. Ein wirksames Sicherheitskonzept kombiniert mehrere technische, organisatorische, personelle und physische Maßnahmen nach dem Prinzip Defense in Depth.

Wichtigste Merksätze

IT-Sicherheit schützt Vertraulichkeit,
Integrität
und Verfügbarkeit.

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

Schwachstelle ist die Lücke.

Bedrohung ist das mögliche Ereignis.

Risiko ist Wahrscheinlichkeit und Auswirkung.

Angriffsfläche reduzieren.

Malware ist Schadsoftware.

Virus hängt sich an Dateien.

Wurm verbreitet sich selbstständig.

Trojaner tarnt sich.

Ransomware verschlüsselt oder sperrt.

Double Extortion bedeutet Verschlüsselung plus Datenabfluss.

Phishing täuscht Benutzer.

Social Engineering manipuliert Menschen.

Phishing ist nicht nur E-Mail.

MFA schützt stark,
aber nicht gegen alles.

Passwörter nicht wiederverwenden.

DoS und DDoS greifen Verfügbarkeit an.

DDoS ist verteilt.

MitM sitzt zwischen Sender und Empfänger.

Sniffing kann nützlich sein,
aber auch missbraucht werden.

Spoofing täuscht Identität oder Herkunft vor.

ARP-Spoofing betrifft lokale Netze.

DNS-Spoofing führt zu falschen Zielen.

Rogue DHCP verteilt falsche Netzwerkeinstellungen.

WLAN braucht starke Absicherung.

SQL Injection betrifft Datenbanken.

XSS betrifft Browser.

CSRF missbraucht Sitzungen.

Prepared Statements schützen vor SQL Injection.

Escaping schützt vor XSS.

CSRF-Token schützen vor CSRF.

Zugriffskontrolle immer serverseitig prüfen.

CVE benennt Schwachstellen.

CVSS bewertet Kritikalität.

Patchmanagement ist ein Prozess.

Hardening reduziert Angriffsfläche.

Baseline definiert sicheren Grundzustand.

Configuration Drift vermeiden.

Firewall begrenzt Netzwerkzugriffe.

Default Deny ist sicherer.

IDS erkennt.

IPS blockiert zusätzlich.

EDR schützt Endgeräte tiefer als Antivirus.

SIEM korreliert Sicherheitslogs.

Backup verhindert keinen Angriff,
hilft aber bei Wiederherstellung.

Restore-Test ist Pflicht.

Immutable Backup schützt vor Manipulation.

Incident Response vorbereiten.

Defense in Depth kombiniert Schutzschichten.

Sicherheit ist ein dauerhafter Prozess.