16.1 Angriffe und Schutzmaßnahmen

IT-Systeme und Netzwerke sind vielen möglichen Angriffen ausgesetzt.

Ein Angriff kann sich richten gegen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Identitäten
- Daten
- Anwendungen
- Netzwerke
- Endgeräte
- Server
- Cloud-Dienste

Merksatz:

IT-Sicherheit schützt nicht nur Technik,
sondern auch Daten,
Prozesse
und Verfügbarkeit.

Grundziele der Informationssicherheit

Die drei wichtigsten Grundziele sind:

Vertraulichkeit

Integrität

Verfügbarkeit

Diese drei Begriffe werden oft als Schutzziele bezeichnet.

Merksatz:

Vertraulichkeit,
Integrität
und Verfügbarkeit sind die Grundpfeiler der IT-Sicherheit.

Vertraulichkeit

Vertraulichkeit bedeutet:

Informationen dürfen nur von berechtigten Personen gelesen werden.

Beispiele:

Kundendaten
Passwörter
Personalakten
Geschäftsgeheimnisse
medizinische Daten
interne Dokumente
Zugangsdaten

Angriffe auf Vertraulichkeit:

Datenabfluss
unberechtigter Zugriff
Abhören
Phishing
gestohlene Zugangsdaten
öffentlich freigegebene Cloud-Speicher

Merksatz:

Vertraulichkeit schützt vor unberechtigtem Lesen.

Integrität

Integrität bedeutet:

Daten dürfen nicht unbemerkt verändert werden.

Beispiele:

Rechnung darf nicht manipuliert werden.
Konfigurationsdatei darf nicht heimlich geändert werden.
Softwarepaket darf nicht verfälscht werden.
Logdatei darf nicht manipuliert werden.

Angriffe auf Integrität:

Manipulation
Schadsoftware
unberechtigte Änderungen
Datenbankänderungen
Man-in-the-Middle
Supply-Chain-Angriffe

Merksatz:

Integrität schützt vor unbemerkter Veränderung.

Verfügbarkeit

Verfügbarkeit bedeutet:

Systeme,
Dienste
und Daten sind bei Bedarf nutzbar.

Beispiele:

Webserver erreichbar
E-Mail funktioniert
Datenbank antwortet
Backup kann wiederhergestellt werden
Netzwerk ist verfügbar

Cloud-Dienst läuft

Angriffe auf Verfügbarkeit:

DoS
DDoS
Ransomware
Sabotage
Überlastung
Ausfall kritischer Komponenten

Merksatz:

Verfügbarkeit schützt die Nutzbarkeit von Systemen.

CIA-Triade

Die drei Schutzziele werden oft zusammengefasst als:

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 E-Mail wirklich vom angegebenen Absender?
Ist das Zertifikat gültig?

Merksatz:

Authentizität schützt vor falscher Identität.

Nichtabstreitbarkeit

Nichtabstreitbarkeit bedeutet:

Eine Handlung kann später nicht glaubwürdig abgestritten werden.

Beispiel:

Eine digital signierte Bestellung kann einer Person oder Organisation zugeordnet werden.

Mittel:

digitale Signatur
Protokollierung
Zeitstempel
eindeutige Benutzerkonten

Merksatz:

Nichtabstreitbarkeit sorgt für Nachweisbarkeit.

Angriffsarten im Überblick

Typische Angriffsarten:

```
- Phishing
- Social Engineering
- Malware
- Ransomware
- DoS und DDoS
- Man-in-the-Middle
- Passwortangriffe
- Brute Force
- Credential Stuffing
- Spoofing
- Sniffing
- SQL Injection
- Cross-Site Scripting
- Zero-Day-Angriff
- Supply-Chain-Angriff
- Insider-Bedrohung
```

Merksatz:

```
Angriffe können technisch,
organisatorisch
oder menschlich ansetzen.
```

Angreiferziele

Angreifer verfolgen unterschiedliche Ziele.

Beispiele:

```
Daten stehlen
Geld erpressen
Systeme verschlüsseln
Zugangsdaten sammeln
Dienste lahmlegen
```

Systeme übernehmen
Spionage betreiben
Sabotage durchführen
Rechenleistung missbrauchen
interne Bewegung im Netz erreichen

Merksatz:

Angriffe haben ein Ziel,
auch wenn sie zunächst zufällig wirken.

Angriffsfläche

Angriffsfläche bedeutet:

alle Stellen,
an denen ein System angegriffen werden kann.

Beispiele:

offene Ports
Webanwendungen
VPN-Zugänge
Benutzerkonten
E-Mail
Cloud-Portale
APIs
veraltete Software
unsichere Freigaben
mobile Geräte
externe Dienstleister

Merksatz:

Je größer die Angriffsfläche,
desto mehr mögliche Angriffspunkte.

Angriffsfläche reduzieren

Maßnahmen:

```
unnötige Dienste deaktivieren
offene Ports schließen
alte Software entfernen
Standardkonten deaktivieren
Rechte begrenzen
MFA aktivieren
Netzsegmentierung nutzen
Systeme patchen
öffentliche Zugriffe prüfen
sichere Konfiguration verwenden
```

Merksatz:

```
Nicht benötigte Angriffsfläche entfernen.
```

Schwachstelle

Eine Schwachstelle ist eine Sicherheitslücke oder ein Fehler, der ausgenutzt werden kann.

Beispiele:

```
veraltete Software
unsichere Konfiguration
schwaches Passwort
fehlende Zugriffskontrolle
Programmierfehler
offener Adminport
öffentlich freigegebener Speicher
```

Merksatz:

```
Schwachstelle = ausnutzbare Sicherheitslücke.
```

Bedrohung

Eine Bedrohung ist ein mögliches Ereignis, das Schaden verursachen kann.

Beispiele:

```
Angreifer
Malware
Feuer
Diebstahl
Stromausfall
Fehlbedienung
Datenverlust
Insider
```

Merksatz:

```
Bedrohung = mögliches schädliches Ereignis.
```

Risiko

Risiko beschreibt, wie wahrscheinlich ein Schaden ist und wie groß die Auswirkung wäre.

Vereinfacht:

```
Risiko = Eintrittswahrscheinlichkeit × Schadenshöhe
```

Beispiel:

```
Ein öffentlich erreichbarer Server mit alter Software hat ein hohes Risiko.
```

Merksatz:

```
Risiko verbindet Wahrscheinlichkeit und Auswirkung.
```

Schutzmaßnahme

Eine Schutzmaßnahme reduziert ein Risiko.

Beispiele:

Patch einspielen
MFA aktivieren
Firewall-Regel setzen
Backup erstellen
Benutzer schulen
Rechte begrenzen
Verschlüsselung nutzen
Monitoring aktivieren

Merksatz:

Schutzmaßnahmen senken Eintrittswahrscheinlichkeit oder Auswirkung.

Technische Schutzmaßnahmen

Technische Schutzmaßnahmen sind zum Beispiel:

Firewall
Antivirus
EDR
IDS
IPS
Verschlüsselung
MFA
Patchmanagement
Backup
Netzwerksegmentierung
Logging
Monitoring
Zugriffskontrolle
sichere Konfiguration

Merksatz:

Technische Maßnahmen schützen Systeme direkt.

Organisatorische Schutzmaßnahmen

Organisatorische Schutzmaßnahmen sind zum Beispiel:

Sicherheitsrichtlinien
Schulungen
Berechtigungskonzepte
Notfallpläne
Change Management
Rollenverteilung
Freigabeprozesse
Offboarding
Dokumentation
Verantwortlichkeiten

Merksatz:

Organisation entscheidet,
wie Sicherheit dauerhaft umgesetzt wird.

Personelle Schutzmaßnahmen

Personelle Schutzmaßnahmen betreffen Menschen.

Beispiele:

Schulung gegen Phishing
klare Meldewege
Sensibilisierung
Vier-Augen-Prinzip
sichere Passwortnutzung
Umgang mit vertraulichen Daten
Verhalten bei Sicherheitsvorfällen

Merksatz:

Menschen sind Teil der Sicherheit,
nicht nur Risiko.

Physische Schutzmaßnahmen

Physische Schutzmaßnahmen schützen Räume, Geräte und Infrastruktur.

Beispiele:

```
Zutrittskontrolle
abschließbare Serverräume
Videoüberwachung
Brandschutz
USV
Klimatisierung
Schutz vor Diebstahl
gesicherte Netzwerkschränke
```

Merksatz:

```
IT-Sicherheit beginnt auch bei physischem Schutz.
```

Defense in Depth

Defense in Depth bedeutet:

```
mehrere Schutzschichten werden kombiniert.
```

Beispiel:

```
Firewall
plus
MFA
plus
Patchmanagement
plus
EDR
plus
Backup
plus
Monitoring
```

Wenn eine Schutzschicht versagt, sollen andere Schichten weiter schützen.

Merksatz:

```
Defense in Depth = Sicherheit durch mehrere Schichten.
```

Least Privilege

Least Privilege bedeutet:

```
Benutzer,
Dienste
und Systeme bekommen nur die Rechte,
die sie wirklich benötigen.
```

Beispiele:

```
normaler Benutzer kein lokaler Administrator
Dienstkonto nur Zugriff auf benötigte Datenbank
VPN-Benutzer nur auf notwendige Systeme
Cloud-Rolle nur mit benötigten Aktionen
```

Merksatz:

```
Weniger Rechte bedeuten weniger Schaden bei Missbrauch.
```

Need to Know

Need to Know bedeutet:

```
Zugriff nur auf Informationen,
die für die Aufgabe erforderlich sind.
```

Beispiel:

```
Personalabteilung sieht Personalakten.
Support sieht technische Tickets.
Praktikant sieht keine vertraulichen Finanzdaten.
```

Merksatz:

```
Nicht jeder muss alles wissen.
```

Zero Trust

Zero Trust bedeutet:

```
keinem Zugriff automatisch vertrauen.
```

Es wird geprüft:

```
Benutzer
Gerät
Standort
Risiko
Anwendung
Berechtigung
MFA
Gerätezustand
```

Merksatz:

```
Zero Trust heißt:
immer prüfen,
nie pauschal vertrauen.
```

Phishing

Phishing ist der Versuch, Benutzer zur Preisgabe vertraulicher Informationen zu verleiten.

Ziele:

```
Passwörter
MFA-Codes
Kreditkartendaten
Zugangsdaten
interne Informationen
```

Typische Mittel:

```
gefälschte E-Mails
gefälschte Webseiten
gefälschte Loginseiten
angebliche Rechnungen
angebliche Paketmeldungen
angebliche Sicherheitswarnungen
```

Merksatz:

```
Phishing greift den Menschen über Täuschung an.
```

Spear Phishing

Spear Phishing ist gezieltes Phishing gegen bestimmte Personen oder Organisationen.

Beispiel:

```
Angreifer schreibt eine E-Mail,
die genau zu einer Firma,
einem Projekt
oder einer Rolle passt.
```

Spear Phishing wirkt oft glaubwürdiger als Massenphishing.

Merksatz:

```
Spear Phishing ist gezieltes Phishing.
```

Whaling

Whaling ist Phishing gegen besonders wichtige Personen.

Beispiele:

```
Geschäftsführung
Administratoren
```

Finanzleitung
Personalabteilung
Projektleitung

Merksatz:

Whaling richtet sich gegen besonders wertvolle Ziele.

Social Engineering

Social Engineering nutzt menschliches Verhalten aus.

Beispiele:

Vertrauen erschleichen
Zeitdruck erzeugen
Hilfsbereitschaft ausnutzen
Autorität vortäuschen
Angst erzeugen
Neugier ausnutzen

Merksatz:

Social Engineering manipuliert Menschen statt Technik.

Schutz vor Phishing und Social Engineering

Maßnahmen:

Schulungen
klare Meldewege
MFA
E-Mail-Filter
sichere Passwortmanager
keine Links blind anklicken
Absender prüfen
ungewöhnliche Anfragen hinterfragen
Vier-Augen-Prinzip bei Zahlungen

Sensibilisierung für Druck und Täuschung

Merksatz:

Technik und Schulung gemeinsam schützen besser.

Malware

Malware ist Schadsoftware.

Beispiele:

Virus
Wurm
Trojaner
Ransomware
Spyware
Keylogger
Rootkit
Botnet-Client
Cryptominer

Merksatz:

Malware ist Software mit schädlicher Funktion.

Virus

Ein Virus hängt sich an Dateien oder Programme und verbreitet sich, wenn diese ausgeführt oder weitergegeben werden.

Merksatz:

Virus braucht meist eine Wirtsdatei oder Benutzeraktion.

Wurm

Ein Wurm verbreitet sich selbstständig über Netzwerke oder Schwachstellen.

Gefahr:

schnelle Ausbreitung
hohe Netzlast
Infektion vieler Systeme
Ausnutzung ungepatchter Systeme

Merksatz:

Wurm verbreitet sich selbstständig.

Trojaner

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

Beispiele:

angebliches Tool
manipulierte Installationsdatei
Fake-Update
gecrackte Software

Merksatz:

Trojaner täuscht Nützlichkeit vor.

Ransomware

Ransomware verschlüsselt Daten oder sperrt Systeme und fordert Lösegeld.

Folgen:

Daten nicht verfügbar
Betriebsunterbrechung
Erpressung
Datenabfluss möglich
hohe Wiederherstellungskosten

Merksatz:

> Ransomware greift vor allem Verfügbarkeit und oft auch Vertraulichkeit an.

Schutz vor Ransomware

Maßnahmen:

> Offline- oder Immutable-Backups
> regelmäßige Restore-Tests
> Patchmanagement
> EDR
> Makros einschränken
> Least Privilege
> Netzwerksegmentierung
> MFA
> E-Mail-Schutz
> keine lokalen Adminrechte
> Monitoring
> schnelle Isolation infizierter Systeme

Merksatz:

> Gegen Ransomware sind Backups,
> Rechtebegrenzung
> und Segmentierung besonders wichtig.

Spyware

Spyware spioniert Benutzer oder Systeme aus.

Beispiele:

> Tastatureingaben aufzeichnen
> Bildschirm erfassen
> Browserdaten auslesen
> Zugangsdaten stehlen
> Benutzerverhalten beobachten

Merksatz:

```
Spyware sammelt heimlich Informationen.
```

Keylogger

Ein Keylogger zeichnet Tastatureingaben auf.

Ziel:

```
Passwörter
Zugangsdaten
Nachrichten
vertrauliche Eingaben
```

Merksatz:

```
Keylogger stehlen Eingaben.
```

Rootkit

Ein Rootkit versteckt Schadsoftware oder ermöglicht besonders tiefen Zugriff auf ein System.

Ziel:

```
Erkennung verhindern
Kontrolle behalten
Sicherheitssoftware umgehen
System manipulieren
```

Merksatz:

```
Rootkits verstecken und verankern Angriffe tief im System.
```

Botnet

Ein Botnet ist ein Netzwerk kompromittierter Systeme, die von Angreifern gesteuert werden.

Nutzung:

```
DDoS
Spam
Credential Stuffing
Malware-Verteilung
Cryptomining
Proxy-Missbrauch
```

Merksatz:

```
Botnet = viele fremdgesteuerte infizierte Systeme.
```

DoS

DoS steht für:

```
Denial of Service
```

Ziel:

```
Ein Dienst wird durch Überlastung oder Störung unbenutzbar.
```

Beispiel:

```
Ein Server erhält so viele Anfragen,
dass er nicht mehr antwortet.
```

Merksatz:

```
DoS greift die Verfügbarkeit an.
```

DDoS

DDoS steht für:

```
Distributed Denial of Service
```

Dabei kommt der Angriff von vielen Systemen gleichzeitig.

Oft werden Botnetze genutzt.

Merksatz:

```
DDoS ist verteilter DoS-Angriff.
```

Schutz vor DoS und DDoS

Maßnahmen:

```
DDoS-Schutzdienst
Rate Limiting
Load Balancer
Content Delivery Network
Firewall-Regeln
Anycast
Skalierung
Monitoring
Notfallplan
Provider-Unterstützung
```

Merksatz:

```
DDoS-Schutz braucht Technik,
Skalierung
und Vorbereitung.
```

Man-in-the-Middle

Man-in-the-Middle wird oft abgekürzt:

```
MitM
```

Dabei sitzt ein Angreifer zwischen zwei Kommunikationspartnern.

Ziele:

Daten mitlesen
Daten verändern
Sitzung übernehmen
Zertifikatswarnungen ausnutzen
Zugangsdaten abfangen

Merksatz:

MitM greift Kommunikation zwischen zwei Parteien an.

Schutz vor Man-in-the-Middle

Maßnahmen:

TLS korrekt nutzen
Zertifikate prüfen
keine Zertifikatswarnungen ignorieren
VPN in unsicheren Netzen
HSTS bei Webdiensten
sichere WLANs
Zertifikat-Pinning je nach Anwendung
starke Authentifizierung

Merksatz:

TLS schützt nur,
wenn Zertifikate korrekt geprüft werden.

Sniffing

Sniffing bedeutet:

Netzwerkverkehr wird mitgeschnitten oder beobachtet.

Nützlich für Administratoren:

```
Fehlersuche
Analyse
Protokollprüfung
```

Gefährlich durch Angreifer:

```
Zugangsdaten abfangen
unverschlüsselte Daten lesen
interne Kommunikation beobachten
```

Merksatz:

```
Sniffing ist Analysewerkzeug,
kann aber missbraucht werden.
```

Spoofing

Spoofing bedeutet:

```
eine falsche Identität oder Adresse wird vorgetäuscht.
```

Beispiele:

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

Merksatz:

```
Spoofing täuscht Herkunft oder Identität vor.
```

ARP-Spoofing

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

Ziel:

```
Verkehr über Angreifer leiten
Man-in-the-Middle ermöglichen
Kommunikation stören
```

Merksatz:

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

DNS-Spoofing

DNS-Spoofing manipuliert Namensauflösung.

Beispiel:

```
Benutzer ruft bank.example auf,
wird aber auf falsche IP geleitet.
```

Schutz:

```
DNSSEC
sichere DNS-Server
TLS-Zertifikatsprüfung
Monitoring
keine unsicheren DNS-Quellen
```

Merksatz:

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

Passwortangriffe

Passwortangriffe versuchen, Zugangsdaten zu erraten, zu stehlen oder wiederzuverwenden.

Typen:

Brute Force
Wörterbuchangriff
Credential Stuffing
Password Spraying
Phishing
Keylogger

Merksatz:

Passwortangriffe richten sich gegen Identitäten.

Brute Force

Brute Force bedeutet:

viele mögliche Passwörter werden systematisch ausprobiert.

Schutz:

starke Passwörter
MFA
Sperrmechanismen
Rate Limiting
Monitoring
keine Standardkonten
Passwortmanager

Merksatz:

Brute Force wird durch Begrenzung und starke Authentifizierung erschwert.

Credential Stuffing

Credential Stuffing bedeutet:

Angreifer nutzen bekannte Zugangsdaten aus früheren Datenlecks
und probieren sie bei anderen Diensten aus.

Schutz:

keine Passwortwiederverwendung
MFA
Passwortmanager
Leak-Prüfung
ungewöhnliche Loginversuche erkennen

Merksatz:

Credential Stuffing nutzt wiederverwendete Passwörter.

Password Spraying

Password Spraying bedeutet:

Ein Angreifer probiert wenige häufige Passwörter bei vielen Konten aus.

Beispiel:

Sommer2026!
bei vielen Benutzern

Ziel:

Kontosperren vermeiden,
weil pro Konto nur wenige Versuche auftreten.

Merksatz:

Password Spraying verteilt wenige Passwörter auf viele Konten.

Schutz vor Passwortangriffen

Maßnahmen:

```
MFA
starke Passwortrichtlinien
Passwortmanager
keine Wiederverwendung
Rate Limiting
Account Lockout mit Bedacht
Monitoring
Risikoanalyse bei Logins
Schulung
Standardkonten deaktivieren
```

Merksatz:

```
MFA ist eine der wichtigsten Maßnahmen gegen Passwortmissbrauch.
```

SQL Injection

SQL Injection ist ein Angriff auf Datenbankabfragen.

Dabei schleust ein Angreifer SQL-Code in Eingaben ein.

Mögliche Folgen:

```
Daten auslesen
Daten verändern
Login umgehen
Daten löschen
Anwendung manipulieren
```

Merksatz:

```
SQL Injection nutzt unsichere Eingaben in Datenbankabfragen aus.
```

Schutz vor SQL Injection

Maßnahmen:

Prepared Statements
parametrisierte Abfragen
Eingabevalidierung
Rechte der Datenbankbenutzer begrenzen
Fehlerausgaben vermeiden
Web Application Firewall
sichere Programmierung
Code Reviews

Merksatz:

Parametrisierte Abfragen sind zentral gegen SQL Injection.

Cross-Site Scripting

Cross-Site Scripting wird abgekürzt:

XSS

Dabei wird schädlicher Code in Webseiten eingeschleust, der im Browser anderer Benutzer ausgeführt wird.

Mögliche Folgen:

Sessiondiebstahl
Manipulation von Webseiten
Phishing im Browser
Aktionen im Namen des Benutzers

Merksatz:

XSS greift Benutzer über den Browser an.

Schutz vor XSS

Maßnahmen:

Eingaben validieren
Ausgaben korrekt escapen
Content Security Policy
HttpOnly Cookies
sichere Frameworks nutzen
keine ungeprüften HTML-Ausgaben
Code Reviews

Merksatz:

Gegen XSS müssen Ausgaben korrekt behandelt werden.

Zero-Day-Angriff

Ein Zero-Day-Angriff nutzt eine Schwachstelle, für die noch kein Patch verfügbar ist oder die dem Hersteller noch nicht bekannt ist.

Schutz ist schwierig, aber möglich durch:

Defense in Depth
EDR
Segmentierung
Least Privilege
Monitoring
WAF
Härtung
schnelle Reaktion

Merksatz:

Zero-Day bedeutet:
Schwachstelle wird ausgenutzt,
bevor ein regulärer Patch verfügbar ist.

Supply-Chain-Angriff

Ein Supply-Chain-Angriff richtet sich gegen Lieferkette oder Abhängigkeiten.

Beispiele:

```
manipuliertes Softwareupdate
kompromittierte Bibliothek
infizierter Installer
unsicherer Dienstleisterzugang
kompromittiertes Repository
```

Merksatz:

```
Supply-Chain-Angriff trifft Systeme über vertrauenswürdige Lieferwege.
```

Schutz vor Supply-Chain-Angriffen

Maßnahmen:

```
Softwarequellen prüfen
Signaturen prüfen
Abhängigkeiten überwachen
Updates aus vertrauenswürdigen Quellen
Dienstleisterzugriffe begrenzen
Code Reviews
SBOM
Paketquellen absichern
CI/CD schützen
```

Merksatz:

```
Lieferkette ist Teil der IT-Sicherheit.
```

Insider-Bedrohung

Insider sind Personen mit internem Zugriff, die absichtlich oder unabsichtlich Schaden verursachen.

Beispiele:

```
unzufriedener Mitarbeiter
Fehler durch Administrator
```

fahrlässiger Umgang mit Daten
kompromittiertes internes Konto
externer Dienstleister mit zu vielen Rechten

Merksatz:

Nicht jede Bedrohung kommt von außen.

Schutz vor Insider-Risiken

Maßnahmen:

Least Privilege
Vier-Augen-Prinzip
Logging
Rechteprüfung
Offboarding
Aufgabentrennung
Sensibilisierung
klare Prozesse
Monitoring
keine Sammelkonten

Merksatz:

Nachvollziehbarkeit und Rechtebegrenzung senken Insider-Risiken.

Patchmanagement

Patchmanagement bedeutet:

Sicherheitsupdates werden geplant,
getestet,
verteilt
und kontrolliert.

Wichtig für:

Betriebssysteme
Anwendungen
Firmware
Netzwerkgeräte
Firewalls
Cloud-Systeme
Container-Images
Abhängigkeiten

Merksatz:

Ungepatchte Systeme sind häufige Angriffsziele.

Hardening

Hardening bedeutet:

Systeme werden sicher konfiguriert,
indem unnötige Funktionen deaktiviert
und sichere Einstellungen gesetzt werden.

Beispiele:

unnötige Dienste deaktivieren
Standardpasswörter ändern
alte Protokolle abschalten
sichere TLS-Versionen nutzen
Adminzugriffe begrenzen
Logging aktivieren
Rechte minimieren

Merksatz:

Hardening reduziert Angriffsfläche.

Firewall

Eine Firewall filtert Netzwerkverkehr nach Regeln.

Sie kann prüfen:

```
Quelle
Ziel
Port
Protokoll
Richtung
Zustand
Anwendung je nach Firewalltyp
```

Merksatz:

```
Firewall begrenzt Netzwerkzugriffe.
```

IDS und IPS

IDS steht für:

```
Intrusion Detection System
```

Ein IDS erkennt verdächtige Aktivitäten und meldet sie.

IPS steht für:

```
Intrusion Prevention System
```

Ein IPS kann verdächtige Aktivitäten zusätzlich blockieren.

Merksatz:

```
IDS erkennt.
IPS blockiert zusätzlich.
```

Antivirus und EDR

Antivirus erkennt bekannte Schadsoftware.

EDR steht für:

```
Endpoint Detection and Response
```

EDR überwacht Endgeräte tiefer und hilft bei Erkennung, Analyse und Reaktion auf Angriffe.

Merksatz:

```
Antivirus erkennt Schadsoftware.
EDR unterstützt Erkennung und Reaktion auf Endgeräten.
```

Backup als Schutzmaßnahme

Backup schützt nicht vor jedem Angriff, aber es ermöglicht Wiederherstellung.

Wichtig:

```
regelmäßige Backups
getrennte Speicherung
Immutable Backup
Restore-Tests
Verschlüsselung
Zugriffsschutz
Dokumentation
```

Merksatz:

```
Backup ist eine Schutzmaßnahme gegen Datenverlust und Ransomware-Folgen.
```

Monitoring und Logging als Schutzmaßnahme

Monitoring und Logging helfen, Angriffe zu erkennen und aufzuklären.

Wichtige Logs:

```
Anmeldungen
Adminaktionen
Firewall-Entscheidungen
```

```
VPN-Zugriffe
EDR-Meldungen
DNS-Anfragen
Webserver-Logs
Cloud-Audit-Logs
```

Merksatz:

```
Was nicht protokolliert wird,
ist später schwer nachvollziehbar.
```

Incident Response

Incident Response bedeutet:

```
strukturierte Reaktion auf Sicherheitsvorfälle.
```

Schritte:

```
erkennen
bewerten
eindämmen
beseitigen
wiederherstellen
dokumentieren
verbessern
```

Merksatz:

```
Sicherheitsvorfälle brauchen vorbereitete Abläufe.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was sind die Schutzziele der Informationssicherheit?
- Was bedeutet Vertraulichkeit?
```

- Was bedeutet Integrität?
- Was bedeutet Verfügbarkeit?
- Was ist Phishing?
- Was ist Social Engineering?
- Was ist Malware?
- Was ist Ransomware?
- Was ist der Unterschied zwischen DoS und DDoS?
- Was ist Man-in-the-Middle?
- Was ist Spoofing?
- Was ist Brute Force?
- Was ist Credential Stuffing?
- Was ist SQL Injection?
- Was ist Cross-Site Scripting?
- Was ist ein Zero-Day-Angriff?
- Was ist ein Supply-Chain-Angriff?
- Was bedeutet Least Privilege?
- Was ist Defense in Depth?
- Was ist der Unterschied zwischen IDS und IPS?
- Warum sind Backups wichtig gegen Ransomware?
- Warum ist Patchmanagement wichtig?

Typische Prüfungsfallen

Vertraulichkeit,
Integrität
und Verfügbarkeit sauber unterscheiden.

Ransomware betrifft Verfügbarkeit
und oft auch Vertraulichkeit.

Phishing ist Täuschung,
nicht nur eine technische Lücke.

Social Engineering greift Menschen an.

DoS kommt von einer Quelle oder allgemein einem Angriffspunkt.

DDoS ist verteilt.

IDS erkennt,
IPS kann blockieren.

Backup verhindert keinen Angriff,
hilft aber bei Wiederherstellung.

Replikation ersetzt kein Backup.

MFA schützt nicht vor allen Angriffen,
senkt aber Passwortmissbrauch stark.

Firewall ersetzt kein Patchmanagement.

Verschlüsselung ersetzt keine Zugriffskontrolle.

Antivirus ersetzt kein Sicherheitskonzept.

Zero-Day ist nicht durch normales Patchen allein lösbar.

Supply Chain betrifft Lieferwege und Abhängigkeiten.

Least Privilege reduziert Schaden.

Defense in Depth kombiniert mehrere Maßnahmen.

Logs müssen vor dem Vorfall aktiv sein.

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	Handlung kann nachgewiesen werden
Angriffsfläche	Summe möglicher Angriffspunkte
Schwachstelle	ausnutzbare Sicherheitslücke

Begriff	Kurze Erklärung
Bedrohung	mögliches schädliches Ereignis
Risiko	Wahrscheinlichkeit mal Auswirkung
Schutzmaßnahme	reduziert Risiko
Defense in Depth	mehrere Schutzschichten
Least Privilege	minimale notwendige Rechte
Need to Know	Zugriff nur bei Bedarf
Zero Trust	kein automatisches Vertrauen
Phishing	Täuschung zur Datenpreisgabe
Spear Phishing	gezieltes Phishing
Whaling	Phishing gegen wichtige Personen
Social Engineering	Manipulation von Menschen
Malware	Schadsoftware
Virus	Schadsoftware mit Wirtsdatei
Wurm	selbstverbreitende Schadsoftware
Trojaner	getarnte Schadsoftware
Ransomware	erpresserische Verschlüsselung oder Sperrung
Spyware	Spionagesoftware
Keylogger	zeichnet Tastatureingaben auf
Rootkit	versteckt und verankert Schadsoftware
Botnet	Netzwerk fremdgesteuerter Systeme
DoS	Dienstverweigerung
DDoS	verteilter DoS
MitM	Man-in-the-Middle
Sniffing	Mitschneiden von Verkehr
Spoofing	Vortäuschen falscher Identität
ARP-Spoofing	Manipulation lokaler IP-MAC-Zuordnung
DNS-Spoofing	Manipulation von Namensauflösung
Brute Force	systematisches Ausprobieren
Credential Stuffing	Nutzung geleakter Zugangsdaten
Password Spraying	wenige Passwörter gegen viele Konten
SQL Injection	Einschleusen von SQL-Code
XSS	Cross-Site Scripting

Begriff	Kurze Erklärung
Zero-Day	ungepatchte oder unbekannte Schwachstelle
Supply Chain	Lieferkette und Abhängigkeiten
Insider	interne Bedrohung
Patchmanagement	Verwaltung von Sicherheitsupdates
Hardening	sichere Systemkonfiguration
IDS	Angriffserkennung
IPS	Angriffserkennung mit Blockierung
EDR	Endgeräteerkennung und Reaktion
Incident Response	Reaktion auf Sicherheitsvorfälle

IHK-sichere Kurzformulierung

Angriffe auf IT-Systeme können die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen. Vertraulichkeit schützt vor unberechtigtem Lesen, Integrität vor unbemerkter Veränderung und Verfügbarkeit vor Ausfall oder Nichtnutzbarkeit. Typische Angriffe sind Phishing, Social Engineering, Malware, Ransomware, DoS, DDoS, Man-in-the-Middle, Spoofing, Passwortangriffe, SQL Injection, Cross-Site Scripting, Zero-Day- und Supply-Chain-Angriffe. Schutzmaßnahmen sind unter anderem Patchmanagement, Hardening, Firewalls, MFA, Least Privilege, Netzwerksegmentierung, Backups, Monitoring, Logging, IDS/IPS, EDR, Schulungen und Incident Response. Ein gutes Sicherheitskonzept kombiniert mehrere Maßnahmen nach dem Prinzip Defense in Depth.

Merksätze

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

CIA-Triade = Vertraulichkeit,
Integrität,
Verfügbarkeit.

Authentizität prüft Echtheit.

Nichtabstreitbarkeit schafft Nachweisbarkeit.

Angriffsfläche reduzieren.

Schwachstelle ist ausnutzbare Lücke.

Bedrohung ist mögliches Schadereignis.

Risiko = Wahrscheinlichkeit und Auswirkung.

Schutzmaßnahmen senken Risiko.

Defense in Depth kombiniert Schutzschichten.

Least Privilege reduziert Schaden.

Need to Know begrenzt Datenzugriff.

Zero Trust vertraut nicht pauschal.

Phishing täuscht Benutzer.

Social Engineering manipuliert Menschen.

Malware ist Schadsoftware.

Wurm verbreitet sich selbstständig.

Trojaner tarnt sich.

Ransomware verschlüsselt oder sperrt.

DoS greift Verfügbarkeit an.

DDoS ist verteilter DoS.

MitM sitzt zwischen Kommunikationspartnern.

Sniffing kann Analyse oder Angriff sein.

Spoofing täuscht Identität vor.

Brute Force probiert systematisch.

Credential Stuffing nutzt geleakte Zugangsdaten.

SQL Injection greift Datenbankabfragen an.

XSS greift Browserbenutzer an.

Zero-Day ist schwer planbar.

Supply Chain betrifft Lieferwege.

Insider können intern Schaden verursachen.

Patchmanagement schließt bekannte Lücken.

Hardening reduziert Angriffsfläche.

IDS erkennt.

IPS blockiert zusätzlich.

Backup hilft bei Wiederherstellung.

Logs vor dem Vorfall aktivieren.

Incident Response vorbereiten.