19.8 Sicherheitsbegriffe und Angriffe Spickzettel

Dieser Spickzettel fasst wichtige Begriffe der IT-Sicherheit und typische Angriffe kompakt zusammen.

Er ist besonders wichtig für:

- Prüfungsaufgaben zur Informationssicherheit
- Angriffsszenarien
- Schutzmaßnahmen
- Risikoanalyse
- Sicherheitskonzepte
- Fehlersuche bei Sicherheitsvorfällen

Merksatz:

Sicherheit bedeutet:
Risiken erkennen,
Schutzziele verstehen
und passende Maßnahmen auswählen.

Grundidee der Informationssicherheit

Informationssicherheit schützt Informationen und IT-Systeme vor:

unberechtigtem Zugriff
Manipulation
Ausfall
Missbrauch
Datenverlust
Täuschung
Sabotage

Merksatz:

Informationssicherheit schützt Daten,
Systeme
Prozesse

und Zugriffe.

Die drei wichtigsten Schutzziele

Die wichtigsten Schutzziele werden oft als CIA-Triade bezeichnet.

Schutzziel	Bedeutung	Beispielverletzung
Vertraulichkeit	Schutz vor unberechtigtem Lesen	Kundendaten werden gestohlen
Integrität	Schutz vor unbemerkter Veränderung	Konfiguration wird manipuliert
Verfügbarkeit	Systeme und Daten sind nutzbar	Server ist durch DDoS nicht erreichbar

Merksatz:

```
CIA =
Confidentiality,
Integrity,
Availability.

Auf Deutsch:
Vertraulichkeit,
Integrität,
Verfügbarkeit.
```

Vertraulichkeit

Vertraulichkeit bedeutet:

```
Informationen dürfen nur von berechtigten Personen,
Systemen
oder Prozessen gelesen werden.
```

Beispiele für Verletzungen:

```
Datenabfluss
unberechtigter Zugriff
mitgelesene Passwörter
verlorener Laptop ohne Verschlüsselung
falsch freigegebener Cloud-Ordner
```

Schutzmaßnahmen:

Verschlüsselung
Rechtekonzept
MFA
Zugriffskontrolle
DLP
sichere Freigaben

Merksatz:

Vertraulichkeit schützt vor unberechtigtem Mitlesen.

Integrität

Integrität bedeutet:

Daten dürfen nicht unbemerkt verändert werden.

Beispiele für Verletzungen:

manipulierte Konfigurationsdatei
veränderte Überweisung
geänderte Logdatei
manipuliertes Softwarepaket
beschädigte Datenbank

Schutzmaßnahmen:

Hashwerte
digitale Signaturen
Rechtebegrenzung
Versionskontrolle
Logging
Vier-Augen-Prinzip

Merksatz:

Integrität schützt vor unbemerkter Veränderung.

Verfügbarkeit

Verfügbarkeit bedeutet:

Systeme,
Dienste
und Daten stehen bei Bedarf zur Verfügung.

Beispiele für Verletzungen:

Serverausfall
DDoS-Angriff
Ransomware
Stromausfall
defekte Festplatte
Netzwerkstörung

Schutzmaßnahmen:

Redundanz
Backup
Monitoring
Patchmanagement
DDoS-Schutz
Notfallplan

Merksatz:

Verfügbarkeit schützt die Nutzbarkeit.

Weitere Schutzziele

Schutzziel	Bedeutung
Authentizität	Echtheit einer Identität oder Nachricht

Schutzziel	Bedeutung
Nichtabstreitbarkeit	Handlung kann später nicht glaubhaft bestritten werden
Nachvollziehbarkeit	Ereignisse können geprüft und rekonstruiert werden
Zurechenbarkeit	Aktionen können einer Identität zugeordnet werden

Merksatz:

Authentizität fragt:
Ist es echt?

Nichtabstreitbarkeit fragt:
Kann die Handlung nachgewiesen werden?

Authentizität

Authentizität bedeutet:

Echtheit einer Identität,
Nachricht
oder Quelle.

Beispiele:

Ist der Server wirklich der richtige Server?

Ist die E-Mail wirklich vom angegebenen Absender?

Ist der Benutzer wirklich die angemeldete Person?

Schutzmaßnahmen:

Zertifikate
digitale Signaturen
MFA
sichere Authentifizierung
DNSSEC je nach Einsatz

Merksatz:

Authentizität schützt vor Täuschung über Identität oder Herkunft.

Nichtabstreitbarkeit

Nichtabstreitbarkeit bedeutet:

Eine Handlung kann später nicht glaubhaft abgestritten werden.

Beispiele:

digitale Signatur
revisionssichere Logs
protokollierte Freigaben
signierte Dokumente

Merksatz:

Nichtabstreitbarkeit macht Handlungen nachweisbar.

Schwachstelle, Bedrohung und Risiko

Begriff	Bedeutung	Beispiel
Schwachstelle	ausnutzbare Lücke	ungepatchter Server
Bedrohung	mögliches schädliches Ereignis	Angreifer nutzt Lücke aus
Risiko	Wahrscheinlichkeit und Auswirkung	Datenverlust durch Angriff
Maßnahme	reduziert Risiko	Patch installieren

Merksatz:

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

Angriff

Ein Angriff ist der Versuch, eine Schwachstelle auszunutzen oder ein Schutzziel zu verletzen.

Beispiele:

```
Passwortangriff
Malware-Infektion
Phishing
DDoS
SQL Injection
Man-in-the-Middle
```

Merksatz:

```
Angriff = aktiver Versuch,
Schaden oder unberechtigten Zugriff zu erreichen.
```

Malware

Malware bedeutet:

```
Schadsoftware
```

Beispiele:

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

Merksatz:

```
Malware ist der Oberbegriff für Schadsoftware.
```

Virus

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

Merksatz:

> Virus braucht meist eine Wirtsdatei oder Aktion zur Verbreitung.

Wurm

Ein Wurm verbreitet sich selbstständig über Netzwerke, ohne zwingend eine Wirtsdatei zu benötigen.

Risiko:

> schnelle Ausbreitung
> Netzlast
> Masseninfektion

Merksatz:

> Wurm verbreitet sich selbstständig.

Trojaner

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

Merksatz:

> Trojaner täuscht Nutzen vor.

Ransomware

Ransomware verschlüsselt oder sperrt Daten und fordert häufig Lösegeld.

Betroffene Schutzziele:

> Verfügbarkeit

bei Datenabfluss zusätzlich:

Vertraulichkeit

Schutzmaßnahmen:

Offline-Backup
Immutable Backup
Patchmanagement
EDR
Segmentierung
Least Privilege
Restore-Test

Merksatz:

Ransomware betrifft vor allem Verfügbarkeit,
bei Datenabfluss auch Vertraulichkeit.

Spyware und Keylogger

Spyware:

spioniert Daten aus

Keylogger:

zeichnet Tastatureingaben auf

Ziel:

Passwörter
Zugangsdaten
vertrauliche Informationen

Merksatz:

Spyware und Keylogger gefährden besonders Vertraulichkeit.

Rootkit

Ein Rootkit versteckt Schadsoftware oder Angreiferzugriff tief im System.

Ziel:

Erkennung erschweren
dauerhaften Zugriff sichern
Spuren verbergen

Merksatz:

Rootkit versteckt Kompromittierung.

Botnet

Ein Botnet besteht aus vielen kompromittierten Geräten, die zentral gesteuert werden.

Nutzung:

DDoS
Spam
Credential Stuffing
Malware-Verteilung
Kryptomining

Merksatz:

Botnet = viele fremdgesteuerte kompromittierte Geräte.

Phishing

Phishing ist Täuschung, um vertrauliche Daten zu erhalten.

Typische Ziele:

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

Kanäle:

```
E-Mail
SMS
Messenger
Telefon
QR-Code
gefälschte Webseiten
```

Merksatz:

```
Phishing täuscht Benutzer zur Preisgabe von Daten.
```

Spear Phishing

Spear Phishing ist gezieltes Phishing gegen bestimmte Personen oder Organisationen.

Merkmale:

```
persönlicher Bezug
glaubwürdiger Absender
Bezug auf echte Projekte
gezielte Vorbereitung
```

Merksatz:

```
Spear Phishing ist gezielter und oft glaubwürdiger.
```

Whaling

Whaling ist Phishing gegen besonders wichtige Personen.

Beispiele:

```
Geschäftsführung
Abteilungsleitung
Administratoren
Personen mit Zahlungsfreigaben
```

Merksatz:

```
Whaling zielt auf große oder besonders wertvolle Ziele.
```

Social Engineering

Social Engineering nutzt menschliches Verhalten, Vertrauen oder Druck aus.

Beispiele:

```
falscher IT-Support
dringender Anruf vom angeblichen Chef
gefälschter Lieferant
Besucher ohne Berechtigung
manipulierte E-Mail
```

Merksatz:

```
Social Engineering greift Menschen an,
nicht nur Technik.
```

CEO-Fraud

CEO-Fraud ist ein Betrug, bei dem sich Angreifer als Geschäftsführung oder Vorgesetzte ausgeben.

Ziel:

```
Zahlung auslösen
vertrauliche Daten erhalten
schnelle Entscheidung erzwingen
```

Merksatz:

```
CEO-Fraud nutzt Autorität und Zeitdruck.
```

Brute Force

Brute Force bedeutet:

```
systematisches Ausprobieren vieler Passwörter.
```

Schutzmaßnahmen:

```
starke Passwörter
Account Lockout
Rate Limiting
MFA
Monitoring
Passwortmanager
```

Merksatz:

```
Brute Force probiert viele Möglichkeiten aus.
```

Password Spraying

Password Spraying bedeutet:

```
ein häufiges Passwort wird gegen viele Konten getestet.
```

Beispiel:

```
Winter2026!
```

gegen viele Benutzerkonten.

Ziel:

Kontosperren vermeiden,
weil pro Konto nur wenige Versuche stattfinden.

Merksatz:

Password Spraying:
ein Passwort,
viele Konten.

Credential Stuffing

Credential Stuffing nutzt bereits geleakte Zugangsdaten.

Prinzip:

Benutzer verwenden Passwörter oft mehrfach.

Angreifer testen:

bekannte E-Mail-Passwort-Kombinationen
bei anderen Diensten.

Schutzmaßnahmen:

MFA
Passwortmanager
einzigartige Passwörter
Leak-Prüfung
Monitoring

Merksatz:

Credential Stuffing nutzt wiederverwendete Passwörter.

DoS

DoS steht für:

Denial of Service

Ziel:

Dienst überlasten
oder nicht mehr verfügbar machen

Betroffenes Schutzziel:

Verfügbarkeit

Merksatz:

DoS greift Verfügbarkeit an.

DDoS

DDoS steht für:

Distributed Denial of Service

Unterschied zu DoS:

Angriff kommt verteilt von vielen Systemen.

Häufig aus:

Botnetzen

Schutzmaßnahmen:

DDoS-Schutz
CDN
Rate Limiting
Filterung
Skalierung

```
Provider-Schutz
```

Merksatz:

```
DDoS = verteilter Angriff auf Verfügbarkeit.
```

Man-in-the-Middle

Man-in-the-Middle wird oft abgekürzt:

```
MitM
```

Dabei sitzt der Angreifer zwischen zwei Kommunikationspartnern.

Ziele:

```
mitlesen
verändern
umleiten
Sitzung übernehmen
```

Schutzmaßnahmen:

```
TLS
Zertifikatsprüfung
VPN
HSTS
sichere WLANs
ARP-Schutz
```

Merksatz:

```
MitM gefährdet Vertraulichkeit und Integrität.
```

Spoofing

Spoofing bedeutet:

Identität,
Adresse
Absender
oder Herkunft 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 ARP-Zuordnungen im lokalen Netz.

Ziel:

Datenverkehr umleiten
Man-in-the-Middle ermöglichen
Kommunikation stören

Schutzmaßnahmen:

Dynamic ARP Inspection
Netzwerksegmentierung
Switch-Sicherheitsfunktionen
Monitoring
Verschlüsselung höherer Schichten

Merksatz:

ARP-Spoofing betrifft lokale IPv4-Kommunikation.

DNS-Spoofing

DNS-Spoofing liefert falsche DNS-Antworten.

Ziel:

Benutzer auf falsche Server umleiten

Risiken:

Phishing
Malware
Credential Theft
Man-in-the-Middle

Schutzmaßnahmen:

DNSSEC je nach Einsatz
vertrauenswürdige DNS-Server
TLS-Zertifikatsprüfung
Monitoring

Merksatz:

DNS-Spoofing manipuliert Namensauflösung.

SQL Injection

SQL Injection bedeutet:

Angreifer schleust SQL-Code in Eingaben ein.

Ziel:

Daten auslesen
Daten verändern
Anmeldung umgehen
Daten löschen

Schutzmaßnahmen:

Prepared Statements
Parametrisierung
Eingabevalidierung
Rechtebegrenzung der Datenbankkonten
Web Application Firewall
sichere Fehlerausgaben

Merksatz:

SQL Injection betrifft unsichere Datenbankabfragen.

XSS

XSS steht für:

Cross-Site Scripting

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

Ziele:

Session stehlen
Benutzeraktionen manipulieren
Inhalte verändern
Phishing innerhalb einer Webseite

Schutzmaßnahmen:

```
Output Encoding
Eingabevalidierung
Content Security Policy
HttpOnly-Cookies
sichere Frameworks
```

Merksatz:

```
XSS greift Benutzer im Browser an.
```

CSRF

CSRF steht für:

```
Cross-Site Request Forgery
```

Dabei wird eine gültige Sitzung des Benutzers missbraucht, um ungewollte Aktionen auszuführen.

Beispiel:

```
Benutzer ist angemeldet.
Angreifer bringt ihn dazu,
eine Aktion im Hintergrund auszulösen.
```

Schutzmaßnahmen:

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

Merksatz:

```
CSRF missbraucht eine bestehende Sitzung.
```

Zero-Day

Ein Zero-Day ist eine Schwachstelle, für die es noch keinen bekannten Patch gibt oder die gerade erst bekannt wurde.

Risiko:

```
hohe Gefahr,
weil Schutzmaßnahmen noch nicht vollständig verfügbar sind.
```

Merksatz:

```
Zero-Day = Schwachstelle ohne fertige Standardlösung.
```

Supply-Chain-Angriff

Ein Supply-Chain-Angriff zielt auf Lieferkette, Softwareabhängigkeiten oder Dienstleister.

Beispiele:

```
kompromittiertes Update
manipuliertes Paket
unsicherer Dienstleisterzugang
kompromittierte Bibliothek
```

Schutzmaßnahmen:

```
Signaturprüfung
SBOM
Dependency-Scanning
Lieferantenprüfung
Least Privilege für Dienstleister
Monitoring
```

Merksatz:

```
Supply-Chain-Angriff kommt über Abhängigkeiten.
```

Insider Threat

Insider Threat bedeutet:

```
Gefahr durch Personen innerhalb der Organisation
oder mit berechtigtem Zugriff.
```

Beispiele:

```
absichtlicher Datenabfluss
fahrlässige Fehlkonfiguration
Missbrauch von Adminrechten
unbemerkter Zugriff nach Rollenwechsel
```

Schutzmaßnahmen:

```
Least Privilege
Rechteprüfung
Vier-Augen-Prinzip
Logging
Trennung von Aufgaben
Offboarding
```

Merksatz:

```
Insider haben bereits Zugriff,
deshalb sind Rechte und Logs wichtig.
```

Technische Schutzmaßnahmen

Beispiele:

```
Firewall
IDS
IPS
EDR
Antivirus
Verschlüsselung
MFA
Backup
```

Netzwerksegmentierung
Patchmanagement
Hardening
SIEM

Merksatz:

Technische Maßnahmen wirken direkt auf Systeme und Daten.

Organisatorische Schutzmaßnahmen

Beispiele:

Sicherheitsrichtlinien
Berechtigungskonzept
Notfallplan
Change Management
Vier-Augen-Prinzip
Schulungskonzept
Incident-Response-Prozess
Rollen und Verantwortlichkeiten

Merksatz:

Organisatorische Maßnahmen regeln Abläufe und Verantwortung.

Personelle Schutzmaßnahmen

Beispiele:

Schulungen
Awareness
Rollenklärung
Verpflichtung auf Vertraulichkeit
Hintergrundprüfungen je nach Rolle
Sensibilisierung für Phishing

Merksatz:

Personelle Maßnahmen betreffen Menschen und Verhalten.

Physische Schutzmaßnahmen

Beispiele:

Zutrittskontrolle
Serverraum abschließen
Brandmeldeanlage
USV
Klimatisierung
Diebstahlschutz
Videoüberwachung je nach Rechtslage

Merksatz:

Physische Sicherheit schützt Räume,
Geräte
und Infrastruktur.

Defense in Depth

Defense in Depth bedeutet:

Sicherheit durch mehrere Schutzschichten.

Beispiele:

Firewall
Segmentierung
MFA
EDR
Logging
Backup
Schulung
Patchmanagement

Merksatz:

```
Nicht eine Maßnahme allein,
sondern mehrere Schichten schützen besser.
```

Least Privilege

Least Privilege bedeutet:

```
Benutzer,
Dienste
und Prozesse erhalten nur die Rechte,
die sie wirklich benötigen.
```

Ziel:

```
Schaden bei Fehlern oder Angriffen begrenzen.
```

Merksatz:

```
So wenig Rechte wie möglich,
so viele wie nötig.
```

Zero Trust

Zero Trust bedeutet:

```
keinem Zugriff automatisch vertrauen.
```

Grundidee:

```
Identität prüfen
Gerät prüfen
Kontext prüfen
Zugriff begrenzen
kontinuierlich überwachen
```

Merksatz:

```
Zero Trust heißt:
Vertrauen wird geprüft,
nicht vorausgesetzt.
```

MFA

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

Dabei werden mehrere Faktoren kombiniert.

Faktoren:

```
Wissen:
Passwort

Besitz:
Token,
Smartphone,
Smartcard

Sein:
biometrisches Merkmal
```

Merksatz:

```
MFA sorgt dafür,
dass ein Passwort allein nicht reicht.
```

IDS und IPS

System	Bedeutung	Aufgabe
IDS	Intrusion Detection System	erkennt und meldet Angriffe
IPS	Intrusion Prevention System	erkennt und blockiert Angriffe

Merksatz:

IDS meldet.
IPS blockiert zusätzlich.

EDR

EDR steht für:

Endpoint Detection and Response

Aufgabe:

Endgeräte überwachen
verdächtiges Verhalten erkennen
Reaktion ermöglichen
Angriffe analysieren

Merksatz:

EDR schützt und überwacht Endgeräte.

SIEM

SIEM steht für:

Security Information and Event Management

Aufgabe:

Logs sammeln
Sicherheitsereignisse korrelieren
Alarme erzeugen
Vorfälle analysieren
Nachvollziehbarkeit verbessern

Merksatz:

SIEM verbindet Sicherheitsereignisse aus vielen Quellen.

Patchmanagement

Patchmanagement sorgt dafür, dass Sicherheitsupdates geplant, getestet und eingespielt werden.

Ziel:

bekannte Schwachstellen schließen

Merksatz:

Patchmanagement reduziert bekannte Risiken.

Hardening

Hardening bedeutet:

Systeme sicherer konfigurieren,
indem unnötige Funktionen entfernt oder eingeschränkt werden.

Beispiele:

unnötige Dienste deaktivieren
Standardpasswörter ändern
sichere Protokolle verwenden
unsichere Ports schließen
Rechte begrenzen
Logging aktivieren

Merksatz:

Hardening verringert die Angriffsfläche.

Backup als Sicherheitsmaßnahme

Backup schützt besonders gegen:

Datenverlust
Ransomware
Fehlkonfiguration
versehentliche Löschung
Hardwaredefekt

Wichtig:

Restore-Test
Offline-Backup
Immutable Backup
Zugriffsschutz
Verschlüsselung

Merksatz:

Backup ist Wiederherstellungsvorsorge.

Angriffe und Schutzziele zuordnen

Angriff	Betroffenes Schutzziel
Datenabfluss	Vertraulichkeit
Manipulation	Integrität
DDoS	Verfügbarkeit
Ransomware	Verfügbarkeit, eventuell Vertraulichkeit
Man-in-the-Middle	Vertraulichkeit und Integrität
Phishing	Authentizität, Vertraulichkeit
Spoofing	Authentizität
Logmanipulation	Integrität und Nachvollziehbarkeit

Merksatz:

Erst Schutzziel erkennen,
dann passende Maßnahme nennen.

Risiko und Maßnahme zuordnen

Risiko	passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
Malware	EDR, Patchmanagement
Ransomware	Backup, Segmentierung, Immutable Backup
DDoS	DDoS-Schutz, CDN, Rate Limiting
Datenabfluss	Verschlüsselung, DLP, Rechtekonzept
unsichere Freigaben	Rechteprüfung, Ablaufdatum, Logging
Fehlkonfiguration	Change Management, Vier-Augen-Prinzip
unklare Sicherheitsvorfälle	Logging, SIEM, Monitoring
Phishing	Awareness, Mailfilter, MFA

Merksatz:

> Maßnahme muss direkt zum Risiko passen.

Typische Prüfungsfallen

> Vertraulichkeit,
> Integrität
> und Verfügbarkeit verwechseln.
>
> Schwachstelle,
> Bedrohung
> und Risiko gleichsetzen.
>
> Phishing nur als technisches Problem sehen.
>
> Ransomware nur als Vertraulichkeitsproblem sehen.
>
> DDoS nicht der Verfügbarkeit zuordnen.
>
> IDS und IPS verwechseln.

MFA als Ersatz für Rechtekonzept verstehen.

Backup als Schutz vor Angriff statt Wiederherstellungsvorsorge beschreiben.

Zero Trust als einzelnes Produkt verstehen.

Hardening und Patchmanagement verwechseln.

Brute Force und Credential Stuffing verwechseln.

Merksatz:

Sicherheitsaufgaben prüfen oft saubere Begriffsabgrenzung.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet Vertraulichkeit?
- Was bedeutet Integrität?
- Was bedeutet Verfügbarkeit?
- Was ist der Unterschied zwischen Schwachstelle,
  Bedrohung
  und Risiko?
- Was ist Malware?
- Was ist Ransomware?
- Was ist Phishing?
- Was ist Social Engineering?
- Was ist ein DDoS-Angriff?
- Was ist Man-in-the-Middle?
- Was ist Spoofing?
- Was ist SQL Injection?
- Was ist XSS?
- Was ist CSRF?
- Was ist MFA?
- Was ist Least Privilege?
- Was ist der Unterschied zwischen IDS und IPS?
- Was ist SIEM?

- Was ist Hardening?
- Warum ist Backup bei Ransomware wichtig?

IHK-sichere Kurzformulierung

Informationssicherheit schützt die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Vertraulichkeit schützt vor unberechtigtem Lesen, Integrität vor unbemerkter Veränderung und Verfügbarkeit vor Ausfall oder Nichtnutzbarkeit. Eine Schwachstelle ist eine ausnutzbare Lücke, eine Bedrohung ein mögliches schädliches Ereignis und ein Risiko die bewertete Kombination aus Eintrittswahrscheinlichkeit und Auswirkung. Typische Angriffe sind Malware, Ransomware, Phishing, Social Engineering, DDoS, Man-in-the-Middle, Spoofing, SQL Injection, XSS und CSRF. Passende Schutzmaßnahmen sind unter anderem MFA, Least Privilege, Patchmanagement, Hardening, Firewall, IDS, IPS, EDR, SIEM, Backup, Segmentierung und Schulung.

Merksätze

Sicherheit schützt Schutzziele.

CIA bedeutet Vertraulichkeit,
Integrität
und Verfügbarkeit.

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

Authentizität schützt Echtheit.

Nichtabstreitbarkeit macht Handlungen nachweisbar.

Schwachstelle ist die Lücke.

Bedrohung ist das mögliche Ereignis.

Risiko ist die bewertete Gefahr.

Maßnahme reduziert Risiko.

Malware ist Schadsoftware.

Virus braucht meist eine Wirtsdatei.

Wurm verbreitet sich selbstständig.

Trojaner täuscht Nutzen vor.

Ransomware verschlüsselt oder sperrt Daten.

Phishing täuscht Benutzer.

Social Engineering greift Menschen an.

Brute Force probiert viele Passwörter.

Password Spraying:
ein Passwort,
viele Konten.

Credential Stuffing nutzt geleakte Zugangsdaten.

DoS greift Verfügbarkeit an.

DDoS ist verteilter DoS.

MitM sitzt zwischen Kommunikationspartnern.

Spoofing täuscht Identität oder Herkunft vor.

SQL Injection betrifft Datenbankabfragen.

XSS betrifft Browser anderer Benutzer.

CSRF missbraucht eine gültige Sitzung.

Zero-Day ist eine neue oder ungepatchte Schwachstelle.

Supply-Chain-Angriff kommt über Abhängigkeiten.

Insider Threat kommt von innen oder mit berechtigtem Zugriff.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Rechte.

IDS meldet.

IPS blockiert zusätzlich.

EDR schützt Endgeräte.

SIEM korreliert Sicherheitsereignisse.

Patchmanagement schließt bekannte Lücken.

Hardening verringert Angriffsfläche.

Backup ist Wiederherstellungsvorsorge.

Defense in Depth nutzt mehrere Schutzschichten.

Zero Trust prüft Vertrauen kontinuierlich.

Maßnahme muss zum Risiko passen.