20.11 Trainer – Angriffe, Schutzmaßnahmen und IT-Sicherheit

Diese Trainer-Seite wiederholt typische Angriffe, Schutzziele, Risiken und passende Schutzmaßnahmen.

Ziel ist, Sicherheitsfragen in der Prüfung sauber einzuordnen:

- Welches Schutzziel ist betroffen?
- Welche Angriffsmethode liegt vor?
- Welche Maßnahme passt dazu?
- Warum ist die Maßnahme sinnvoll?

Merksatz:

Sicherheitsfragen bestehen oft aus:
Schutzziel,
Risiko,
Maßnahme
und Wirkung.

Lernziele

Nach dieser Seite solltest du sicher können:

- Vertraulichkeit,
  Integrität
  und Verfügbarkeit unterscheiden
- Schwachstelle,
  Bedrohung
  und Risiko erklären
- typische Angriffe erkennen
- Malware-Arten unterscheiden
- Phishing und Social Engineering einordnen
- Passwortangriffe unterscheiden
- Webangriffe grob erklären
- IDS,

IPS,
EDR
und SIEM unterscheiden
- passende Schutzmaßnahmen auswählen
- prüfungssichere Sicherheitsantworten formulieren

Kurzüberblick: Schutzziele

Schutzziel	Bedeutung	Beispiel
Vertraulichkeit	Schutz vor unberechtigtem Lesen	Datenabfluss
Integrität	Schutz vor unbemerkter Veränderung	manipulierte Datei
Verfügbarkeit	Systeme und Daten sind nutzbar	DDoS oder Ausfall
Authentizität	Echtheit prüfen	echter Server oder echter Benutzer
Nachvollziehbarkeit	Ereignisse rekonstruieren	Logs und Protokolle

Merksatz:

CIA =
Confidentiality,
Integrity,
Availability.

Deutsch:
Vertraulichkeit,
Integrität,
Verfügbarkeit.

Kurzüberblick: Angriffe und Maßnahmen

Angriff oder Risiko	Passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
bekannte Sicherheitslücke	Patchmanagement
unnötige Dienste	Hardening
Ransomware	Offline- oder Immutable-Backup
Phishing	Awareness, Mailfilter, MFA

Angriff oder Risiko	Passende Maßnahme
DDoS	DDoS-Schutz, Rate Limiting, CDN
Man-in-the-Middle	TLS, Zertifikatsprüfung, VPN
SQL Injection	Prepared Statements
XSS	Output Encoding, CSP, HttpOnly
unklare Vorfälle	Logging, SIEM, Monitoring

Merksatz:

```
Maßnahme muss zum Risiko passen.
```

Aufgabe 1

Was bedeutet Vertraulichkeit?

Antwort anzeigen

Vertraulichkeit bedeutet:

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

Beispielverletzung:

```
Kundendaten werden unberechtigt ausgelesen.
```

Passende Maßnahmen:

```
Verschlüsselung

Rechtekonzept

MFA

Zugriffskontrolle
```

DLP

Merksatz:

Vertraulichkeit schützt vor unberechtigtem Mitlesen.

Aufgabe 2

Was bedeutet Integrität?

Antwort anzeigen

Integrität bedeutet:

Daten dürfen nicht unbemerkt verändert werden.

Beispielverletzung:

Eine Konfigurationsdatei wird manipuliert.

Passende Maßnahmen:

Hashwerte

digitale Signaturen

Rechtebegrenzung

Versionskontrolle

Logging

Merksatz:

Integrität schützt vor unbemerkter Veränderung.

Aufgabe 3

Was bedeutet Verfügbarkeit?

Antwort anzeigen

Verfügbarkeit bedeutet:

Systeme,
Dienste
und Daten stehen bei Bedarf zur Verfügung.

Beispielverletzung:

Ein Server ist durch DDoS nicht erreichbar.

Passende Maßnahmen:

Redundanz

Monitoring

Backup

DDoS-Schutz

Notfallplan

Merksatz:

Verfügbarkeit schützt Nutzbarkeit.

Aufgabe 4

Ordne das Schutzziel zu.

Ereignis	Schutzziel
Daten werden gestohlen	?
Datei wird manipuliert	?
Server ist nicht erreichbar	?
Absender wird gefälscht	?

Antwort anzeigen

Ereignis	Schutzziel
Daten werden gestohlen	Vertraulichkeit
Datei wird manipuliert	Integrität
Server ist nicht erreichbar	Verfügbarkeit
Absender wird gefälscht	Authentizität

Merksatz:

Lesen = Vertraulichkeit.
Verändern = Integrität.
Ausfall = Verfügbarkeit.
Echtheit = Authentizität.

Aufgabe 5

Was ist der Unterschied zwischen Schwachstelle, Bedrohung und Risiko?

Antwort anzeigen

Schwachstelle:

ausnutzbare Lücke

Beispiel:

ungepatchter Server

Bedrohung:

mögliches schädliches Ereignis

Beispiel:

Angreifer nutzt die Lücke aus

Risiko:

bewertete Gefahr aus Wahrscheinlichkeit und Auswirkung

Beispiel:

Datenverlust durch Angriff auf den ungepatchten Server

Merksatz:

Schwachstelle = Lücke.
Bedrohung = mögliches Ereignis.
Risiko = bewertete Gefahr.

Aufgabe 6

Was ist Malware?

Antwort anzeigen

Malware bedeutet:

Schadsoftware

Beispiele:

Virus

Wurm

Trojaner

Ransomware

Spyware

Keylogger

Rootkit

Botnet-Client

Merksatz:

Malware ist der Oberbegriff für Schadsoftware.

Aufgabe 7

Was ist der Unterschied zwischen Virus, Wurm und Trojaner?

Antwort anzeigen

Virus:

hängt sich an Dateien oder Programme an

verbreitet sich meist durch Ausführung oder Weitergabe

Wurm:

verbreitet sich selbstständig über Netzwerke

Trojaner:

```
tarnt sich als nützliches Programm,
enthält aber schädliche Funktionen
```

Merksatz:

```
Virus braucht oft Wirt.
Wurm verbreitet sich selbst.
Trojaner täuscht Nutzen vor.
```

Aufgabe 8

Was ist Ransomware?

Antwort anzeigen

Ransomware ist Schadsoftware, die Daten verschlüsselt oder Systeme sperrt und häufig Lösegeld fordert.

Betroffene Schutzziele:

```
Verfügbarkeit

bei Datenabfluss zusätzlich:
Vertraulichkeit
```

Passende Maßnahmen:

```
Offline-Backup

Immutable Backup

Patchmanagement

EDR
```

Segmentierung

Least Privilege

Restore-Test

Merksatz:

Ransomware betrifft vor allem Verfügbarkeit.

Aufgabe 9

Warum sind Offline- oder Immutable-Backups bei Ransomware wichtig?

Antwort anzeigen

Ransomware versucht häufig, auch Backups zu löschen oder zu verschlüsseln.

Offline-Backups sind nicht dauerhaft verbunden.

Immutable Backups können für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Dadurch bleibt eine Wiederherstellungsmöglichkeit erhalten.

Merksatz:

Backups müssen vor Angreifern geschützt werden.

Aufgabe 10

Was ist Phishing?

Antwort anzeigen

Phishing ist Täuschung, um vertrauliche Daten oder Zugangsdaten zu erhalten.

Typische Kanäle:

```
E-Mail

SMS

Messenger

Telefon

QR-Code

gefälschte Webseite
```

Ziele:

```
Passwörter

MFA-Codes

Bankdaten

Zugangsdaten
```

Merksatz:

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

Aufgabe 11

Was ist Spear Phishing?

Antwort anzeigen

Spear Phishing ist gezieltes Phishing gegen bestimmte Personen, Abteilungen oder Organisationen.

Merkmale:

persönlicher Bezug

glaubwürdiger Absender

Bezug auf echte Projekte

gezielte Vorbereitung

Merksatz:

Spear Phishing ist gezielt und oft glaubwürdiger.

Aufgabe 12

Was ist Social Engineering?

Antwort anzeigen

Social Engineering nutzt menschliches Verhalten, Vertrauen, Hilfsbereitschaft oder Zeitdruck aus.

Beispiele:

falscher IT-Support

angeblicher Chef fordert Zahlung

gefälschter Lieferant

Besucher ohne Berechtigung

manipulierter Anruf

Merksatz:

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

Aufgabe 13

Was ist CEO-Fraud?

Antwort anzeigen

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

Ziel:

```
Zahlung auslösen

vertrauliche Daten erhalten

schnelle Entscheidung erzwingen
```

Typische Methode:

```
Autorität und Zeitdruck ausnutzen
```

Merksatz:

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

Aufgabe 14

Was ist Brute Force?

Antwort anzeigen

Brute Force bedeutet:

systematisches Ausprobieren vieler Passwörter.

Schutzmaßnahmen:

starke Passwörter

MFA

Account Lockout

Rate Limiting

Monitoring

Passwortmanager

Merksatz:

Brute Force probiert viele Möglichkeiten aus.

Aufgabe 15

Was ist Password Spraying?

Antwort anzeigen

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.
```

Aufgabe 16

Was ist Credential Stuffing?

Antwort anzeigen

Credential Stuffing nutzt bereits geleakte Zugangsdaten.

Prinzip:

```
bekannte E-Mail-Passwort-Kombinationen
werden bei anderen Diensten ausprobiert.
```

Grund:

```
Benutzer verwenden Passwörter oft mehrfach.
```

Schutzmaßnahmen:

```
MFA

Passwortmanager

einzigartige Passwörter
```

Leak-Prüfung

Monitoring

Merksatz:

Credential Stuffing nutzt wiederverwendete geleakte Passwörter.

Aufgabe 17

Ordne zu.

Angriff	Beschreibung
Brute Force	?
Password Spraying	?
Credential Stuffing	?

Antwort anzeigen

Angriff	Beschreibung
Brute Force	viele Passwortversuche
Password Spraying	ein Passwort gegen viele Konten
Credential Stuffing	geleakte Zugangsdaten bei anderen Diensten testen

Merksatz:

Brute Force = viele Versuche.
Spraying = ein Passwort, viele Konten.
Stuffing = geleakte Daten.

Aufgabe 18

Was ist DoS?

Antwort anzeigen

DoS steht für:

Denial of Service

Ziel:

einen Dienst überlasten oder nicht mehr verfügbar machen

Betroffenes Schutzziel:

Verfügbarkeit

Merksatz:

DoS greift Verfügbarkeit an.

Aufgabe 19

Was ist DDoS?

Antwort anzeigen

DDoS steht für:

Distributed Denial of Service

Unterschied zu DoS:

Angriff kommt verteilt von vielen Systemen.

Häufige Quelle:

Botnetze

Schutzmaßnahmen:

```
DDoS-Schutz

CDN

Rate Limiting

Filterung

Provider-Schutz

Skalierung
```

Merksatz:

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

Aufgabe 20

Was ist Man-in-the-Middle?

Antwort anzeigen

Man-in-the-Middle bedeutet:

```
Ein Angreifer sitzt zwischen zwei Kommunikationspartnern.
```

Ziele:

```
mitlesen

verändern

umleiten
```

Sitzung übernehmen

Betroffene Schutzziele:

Vertraulichkeit

Integrität

Schutzmaßnahmen:

TLS

Zertifikatsprüfung

VPN

HSTS

sichere WLANs

Merksatz:

MitM gefährdet Vertraulichkeit und Integrität.

Aufgabe 21

Was ist Spoofing?

Antwort anzeigen

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.

Aufgabe 22

Was ist ARP-Spoofing?

Antwort anzeigen

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.
```

Aufgabe 23

Was ist DNS-Spoofing?

Antwort anzeigen

DNS-Spoofing liefert falsche DNS-Antworten.

Ziel:

```
Benutzer auf falsche Server umleiten.
```

Risiken:

```
Phishing

Malware

Credential Theft

Man-in-the-Middle
```

Schutzmaßnahmen:

vertrauenswürdige DNS-Server

DNSSEC je nach Einsatz

TLS-Zertifikatsprüfung

Monitoring

Merksatz:

DNS-Spoofing manipuliert Namensauflösung.

Aufgabe 24

Was ist SQL Injection?

Antwort anzeigen

SQL Injection bedeutet:

Angreifer schleust SQL-Code in Eingaben ein.

Ziele:

Daten auslesen

Daten verändern

Anmeldung umgehen

Daten löschen

Schutzmaßnahmen:

Prepared Statements

Parametrisierung

Eingabevalidierung

Rechtebegrenzung für Datenbankkonten

sichere Fehlerausgaben

Merksatz:

SQL Injection betrifft unsichere Datenbankabfragen.

Aufgabe 25

Was ist XSS?

Antwort anzeigen

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
```

Merksatz:

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

Aufgabe 26

Was ist CSRF?

Antwort anzeigen

CSRF steht für:

```
Cross-Site Request Forgery
```

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

Schutzmaßnahmen:

```
CSRF-Token

SameSite-Cookies

erneute Bestätigung kritischer Aktionen

Origin-Prüfung
```

Merksatz:

> CSRF missbraucht eine bestehende Sitzung.

Aufgabe 27

Ordne Webangriffe zu.

Angriff	Kurzbeschreibung
SQL Injection	?
XSS	?
CSRF	?

Antwort anzeigen

Angriff	Kurzbeschreibung
SQL Injection	SQL-Code in Eingaben einschleusen
XSS	Skriptcode im Browser anderer Benutzer ausführen
CSRF	gültige Sitzung für ungewollte Aktion missbrauchen

Merksatz:

> SQLi betrifft Datenbankabfragen.
> XSS betrifft Browser.
> CSRF betrifft Sitzungen.

Aufgabe 28

Was ist ein Zero-Day?

Antwort anzeigen

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

Risiko:

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

Merksatz:

```
Zero-Day = neue oder ungepatchte Schwachstelle.
```

Aufgabe 29

Was ist ein Supply-Chain-Angriff?

Antwort anzeigen

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

Beispiele:

```
kompromittiertes Update

manipuliertes Softwarepaket

unsichere Bibliothek

kompromittierter Dienstleisterzugang
```

Schutzmaßnahmen:

```
Signaturprüfung

Dependency-Scanning

Lieferantenprüfung

Least Privilege
```

Monitoring

Merksatz:

Supply-Chain-Angriff kommt über Abhängigkeiten.

Aufgabe 30

Was bedeutet Insider Threat?

Antwort anzeigen

Insider Threat bedeutet:

Gefahr durch Personen innerhalb der Organisation
oder mit berechtigtem Zugriff.

Beispiele:

absichtlicher Datenabfluss

fahrlässige Fehlkonfiguration

Missbrauch von Adminrechten

Zugriff nach Rollenwechsel nicht entfernt

Schutzmaßnahmen:

Least Privilege

Rechteprüfung

Vier-Augen-Prinzip

Logging

Offboarding

Merksatz:

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

Aufgabe 31

Was bedeutet Least Privilege?

Antwort anzeigen

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.

Aufgabe 32

Was bedeutet MFA?

Antwort anzeigen

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.
```

Aufgabe 33

Was ist Hardening?

Antwort anzeigen

Hardening bedeutet:

```
Systeme sicherer konfigurieren,
indem unnötige Funktionen deaktiviert
```

oder eingeschränkt werden.

Beispiele:

unnötige Dienste deaktivieren

Standardpasswörter ändern

unsichere Protokolle abschalten

Rechte begrenzen

sichere Einstellungen setzen

Logging aktivieren

Merksatz:

Hardening verringert die Angriffsfläche.

Aufgabe 34

Was ist Patchmanagement?

Antwort anzeigen

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

Ziel:

bekannte Schwachstellen schließen.

Merksatz:

Patchmanagement reduziert bekannte Risiken.

Aufgabe 35

Was ist der Unterschied zwischen IDS und IPS?

Antwort anzeigen

IDS:

```
Intrusion Detection System

erkennt und meldet Angriffe
```

IPS:

```
Intrusion Prevention System

erkennt Angriffe
und blockiert zusätzlich
```

Merksatz:

```
IDS meldet.
IPS blockiert.
```

Aufgabe 36

Was ist EDR?

Antwort anzeigen

EDR steht für:

```
Endpoint Detection and Response
```

Aufgabe:

Endgeräte überwachen

verdächtiges Verhalten erkennen

Reaktion ermöglichen

Angriffe analysieren

Merksatz:

EDR schützt und überwacht Endgeräte.

Aufgabe 37

Was ist SIEM?

Antwort anzeigen

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.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Ein Dienst ist durch sehr viele Anfragen nicht mehr erreichbar.
Welches Schutzziel ist betroffen?

Antwort A:

Vertraulichkeit,
weil alles geheim ist.

Antwort B:

Verfügbarkeit,
weil der Dienst nicht mehr nutzbar ist.

Antwort anzeigen

B ist besser.

Begründung:

Wenn ein Dienst nicht mehr erreichbar oder nutzbar ist,
ist die Verfügbarkeit betroffen.

Merksatz:

Ausfall = Verfügbarkeit.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

```
Warum ist MFA eine sinnvolle Maßnahme gegen gestohlene Passwörter?
```

Antwort A:

```
Weil MFA moderner ist.
```

Antwort B:

```
MFA verlangt zusätzlich zum Passwort einen weiteren Faktor.
Dadurch reicht ein gestohlenes Passwort allein nicht mehr aus,
um Zugriff zu erhalten.
```

Antwort anzeigen

B ist besser.

Begründung:

```
Die Antwort nennt die konkrete Schutzwirkung.
```

Merksatz:

```
Maßnahme immer mit Wirkung erklären.
```

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

```
Warum ist Hardening sinnvoll?
```

Antwort A:

Weil man Systeme härter macht.

Antwort B:

Hardening reduziert die Angriffsfläche,
indem unnötige Dienste,
Standardzugänge,
unsichere Protokolle
und zu weitgehende Rechte entfernt oder eingeschränkt werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt,
wie Hardening wirkt
und warum es sicherheitsrelevant ist.

Merksatz:

Fachbegriff plus Wirkung nennen.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Vertraulichkeit schützt vor was?	unberechtigtem Lesen
Integrität schützt vor was?	unbemerkter Veränderung
Verfügbarkeit schützt was?	Nutzbarkeit
Was ist Malware?	Schadsoftware
Was ist Ransomware?	Verschlüsselung oder Sperrung gegen Lösegeld
Was ist Phishing?	Täuschung zur Datenpreisgabe
Was ist DDoS?	verteilter Angriff auf Verfügbarkeit
Was ist MitM?	Angreifer zwischen Kommunikationspartnern

Frage	Antwort
Was ist Spoofing?	Vortäuschen von Identität oder Herkunft
Was ist SQL Injection?	SQL-Code in Eingaben einschleusen
Was ist XSS?	Skriptcode im Browser anderer Benutzer
Was ist CSRF?	Missbrauch einer bestehenden Sitzung
Was macht IDS?	melden
Was macht IPS?	blockieren
Was macht SIEM?	Sicherheitsereignisse korrelieren

Mini-Prüfung: Angriff und Maßnahme

Angriff oder Risiko	passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
ungepatchter Server	Patchmanagement
unnötige Dienste	Hardening
Ransomware	Offline- oder Immutable-Backup
Phishing	Awareness, Mailfilter, MFA
SQL Injection	Prepared Statements
XSS	Output Encoding, CSP, HttpOnly
DDoS	DDoS-Schutz, Rate Limiting
Man-in-the-Middle	TLS, Zertifikatsprüfung
unklare Vorfälle	Logging, SIEM
kompromittiertes Endgerät	EDR

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinlichstes Thema
viele Loginversuche	Brute Force
ein Passwort gegen viele Konten	Password Spraying
geleakte Zugangsdaten werden getestet	Credential Stuffing
gefälschte Loginseite	Phishing
angeblicher Chef fordert Zahlung	CEO-Fraud
Dateien verschlüsselt, Lösegeldforderung	Ransomware

Fehlerbild	Wahrscheinlichstes Thema
Dienst überlastet	DoS oder DDoS
falsche DNS-Antwort	DNS-Spoofing
Verkehr wird umgeleitet	Man-in-the-Middle
SQL-Fehler nach Eingabe	SQL Injection
fremdes Skript im Browser	XSS
Aktion über bestehende Sitzung ausgelöst	CSRF

IHK-sichere Kurzformulierung

Informationssicherheit schützt die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Vertraulichkeit schützt vor unberechtigtem Lesen, Integrität vor unbemerkter Veränderung und Verfügbarkeit vor Ausfall. Eine Schwachstelle ist eine ausnutzbare Lücke, eine Bedrohung ein mögliches schädliches Ereignis und ein Risiko die bewertete Gefahr. Typische Angriffe sind Malware, Ransomware, Phishing, Social Engineering, Brute Force, Credential Stuffing, 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 Awareness.

Merksätze

Sicherheit schützt Schutzziele.

CIA bedeutet Vertraulichkeit,
Integrität
und Verfügbarkeit.

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

Authentizität schützt Echtheit.

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.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Rechte.

Patchmanagement schließt bekannte Lücken.

Hardening reduziert Angriffsfläche.

IDS meldet.

IPS blockiert.

EDR schützt Endgeräte.

SIEM korreliert Sicherheitsereignisse.

Backup ist Wiederherstellungsvorsorge.

Maßnahme muss zum Risiko passen.

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.