16.7 Sicherheitsmaßnahmen: Firewall, IDS, IPS, EDR, SIEM und Backup

Sicherheitsmaßnahmen schützen Systeme, Netzwerke, Daten und Benutzer vor Angriffen.

Es gibt nicht die eine Maßnahme, die alles schützt.

Stattdessen werden mehrere Schutzmaßnahmen kombiniert.

Typische Sicherheitsmaßnahmen sind:

```
- Firewall
- Netzwerksegmentierung
- IDS
- IPS
- Antivirus
- EDR
- SIEM
- MFA
- Backup
- Patchmanagement
- Hardening
- Logging
- Monitoring
- Schulung
- Incident Response
```

Merksatz:

```
IT-Sicherheit entsteht durch mehrere Schutzschichten.
```

Warum mehrere Schutzmaßnahmen nötig sind

Einzelne Schutzmaßnahmen können versagen.

Beispiele:

```
Firewall-Regel ist zu breit.
Benutzer fällt auf Phishing herein.
Antivirus erkennt neue Malware nicht.
Patch ist noch nicht verfügbar.
Backup wurde nicht getestet.
Passwort wurde wiederverwendet.
Adminrechte wurden zu großzügig vergeben.
```

Deshalb braucht man mehrere Schutzschichten.

Merksatz:

```
Sicherheit darf nicht von einer einzigen Maßnahme abhängen.
```

Defense in Depth

Defense in Depth bedeutet:

```
Sicherheit durch mehrere Schutzschichten.
```

Beispiel:

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

Wenn eine Schutzschicht versagt, sollen andere Schichten den Schaden begrenzen.

Merksatz:

Defense in Depth = mehrschichtige Verteidigung.

Prävention, Erkennung und Reaktion

Sicherheitsmaßnahmen lassen sich grob einteilen in:

Bereich	Ziel	Beispiele
Prävention	Angriff verhindern	Firewall, MFA, Patchmanagement
Erkennung	Angriff erkennen	IDS, EDR, SIEM, Logging
Reaktion	Schaden begrenzen	Incident Response, Isolation, Restore

Merksatz:

Gute Sicherheit verhindert,
erkennt
und reagiert.

Firewall

Eine Firewall filtert Netzwerkverkehr anhand von Regeln.

Sie entscheidet, ob Verkehr erlaubt oder blockiert wird.

Typische Kriterien:

Quelle
Ziel
Port
Protokoll
Richtung
Zustand der Verbindung
Anwendung je nach Firewalltyp
Benutzer je nach System

Merksatz:

Firewall = kontrollierte Netzwerkgrenze.

Firewall-Aufgaben

Eine Firewall kann:

```
interne Netze schützen
Internetzugriffe filtern
DMZ absichern
VPN-Zugänge begrenzen
Serverdienste schützen
Netzwerkbereiche trennen
unerwünschten Verkehr blockieren
Verbindungsversuche protokollieren
```

Merksatz:

```
Firewalls begrenzen,
welche Kommunikation erlaubt ist.
```

Paketfilter-Firewall

Eine Paketfilter-Firewall prüft einzelne Pakete anhand einfacher Merkmale.

Beispiele:

```
Quell-IP
Ziel-IP
Quellport
Zielport
Protokoll
```

Vorteil:

```
schnell
grundlegend wirksam
```

Nachteil:

```
erkennt nicht immer den Zusammenhang einer Verbindung
versteht Anwendungen nur begrenzt
```

Merksatz:

```
Paketfilter prüfen grundlegende Paketinformationen.
```

Stateful Firewall

Eine Stateful Firewall merkt sich Verbindungszustände.

Sie erkennt, ob ein Paket zu einer bestehenden erlaubten Verbindung gehört.

Vorteil:

```
Rückverkehr kann automatisch korrekt zugeordnet werden.
```

Beispiel:

```
Client baut Verbindung zu Webserver auf.
Antwortpakete werden als zugehörig erkannt.
```

Merksatz:

```
Stateful Firewall kennt den Zustand von Verbindungen.
```

Application Firewall

Eine Application Firewall prüft Verkehr auf Anwendungsebene.

Beispiele:

```
HTTP-Anfragen
Webanwendungsangriffe
ungewöhnliche Parameter
SQL-Injection-Muster
XSS-Muster
```

Protokollverstöße

Eine Web Application Firewall ist eine spezielle Form für Webanwendungen.

Merksatz:

Application Firewall schaut tiefer in Anwendungsverkehr.

Next-Generation Firewall

Eine Next-Generation Firewall kann mehr als einfache Portfilterung.

Typische Funktionen:

Stateful Inspection
Anwendungserkennung
Benutzerbezug
IDS/IPS-Funktionen
URL-Filter
Malware-Erkennung
VPN
Logging
Richtlinien nach Anwendungen

Merksatz:

Next-Generation Firewall kombiniert mehrere Sicherheitsfunktionen.

Firewall-Regeln richtig formulieren

Gute Firewall-Regeln sind:

notwendig
eindeutig
dokumentiert
möglichst eng
nach Quelle,
Ziel,

Port
und Protokoll definiert
regelmäßig geprüft

Schlechte Regel:

Any to Any allow

Bessere Regel:

Webserver darf TCP 5432 zur Datenbank auf bestimmter IP nutzen.

Merksatz:

Erlaube nur,
was wirklich benötigt wird.

Default Deny

Default Deny bedeutet:

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

Vorteil:

weniger ungewollte Kommunikation
bessere Kontrolle
geringere Angriffsfläche

Merksatz:

Default Deny ist sicherer als pauschales Erlauben.

Firewall-Logging

Firewall-Logs zeigen, welcher Verkehr erlaubt oder blockiert wurde.

Typische Inhalte:

```
Zeit
Quelle
Ziel
Port
Protokoll
Aktion
Regelname
Interface
Benutzer je nach System
```

Merksatz:

```
Firewall-Logs helfen bei Fehlersuche und Sicherheitsanalyse.
```

Netzwerksegmentierung

Netzwerksegmentierung bedeutet:

```
Netzwerke werden in getrennte Bereiche aufgeteilt.
```

Beispiele:

```
Clientnetz
Servernetz
Managementnetz
Gastnetz
IoT-Netz
Produktionsnetz
Backupnetz
DMZ
```

Vorteil:

```
Angriffe können sich schlechter ausbreiten.
Zugriffe können gezielter gesteuert werden.
```

Merksatz:

```
Segmentierung begrenzt Schaden und Ausbreitung.
```

VLANs als Segmentierung

VLANs trennen Netzwerke logisch auf Schicht 2.

Beispiele:

```
VLAN 10 Clients
VLAN 20 Server
VLAN 30 Gäste
VLAN 40 Management
```

Zwischen VLANs sollte kontrolliert geroutet und gefiltert werden.

Merksatz:

```
VLAN trennt logisch,
Firewall-Regeln steuern den Verkehr dazwischen.
```

DMZ als Schutzmaßnahme

Eine DMZ ist ein gesonderter Netzwerkbereich für öffentlich erreichbare Dienste.

Typische Systeme:

```
Webserver
Reverse Proxy
Mail-Gateway
VPN-Gateway
DNS-Server
```

Ziel:

```
öffentliche Dienste vom internen Netz trennen.
```

Merksatz:

```
DMZ schützt interne Netze vor direktem Zugriff aus dem Internet.
```

IDS

IDS steht für:

```
Intrusion Detection System
```

Ein IDS erkennt verdächtige Aktivitäten und meldet sie.

Es blockiert normalerweise nicht selbst, sondern erzeugt Alarme.

Beispiele für Erkennung:

```
Portscan
bekannte Angriffssignatur
verdächtiger Netzwerkverkehr
ungewöhnliche Loginversuche
Exploit-Versuch
```

Merksatz:

```
IDS erkennt Angriffe,
blockiert aber nicht zwingend.
```

IPS

IPS steht für:

```
Intrusion Prevention System
```

Ein IPS erkennt verdächtige Aktivitäten und kann sie zusätzlich blockieren.

Beispiele:

```
Verbindung abbrechen
Paket verwerfen
```

Quelle blockieren

Angriffsmuster stoppen

Merksatz:

IPS erkennt und verhindert Angriffe aktiv.

IDS und IPS vergleichen

Merkmal	IDS	IPS
Bedeutung	Intrusion Detection System	Intrusion Prevention System
Hauptaufgabe	erkennen und melden	erkennen und blockieren
Wirkung	passiv oder beobachtend	aktiv eingreifend
Risiko	Angriff wird nur gemeldet	Fehlalarm kann legitimen Verkehr blockieren

Merksatz:

IDS meldet.

IPS greift ein.

Signaturbasierte Erkennung

Signaturbasierte Erkennung sucht nach bekannten Mustern.

Beispiele:

bekannte Malware-Signatur

bekannte Exploit-Anfrage

bekannter Angriffspfad

bekannter Hashwert

bekannte Netzwerksequenz

Vorteil:

gut gegen bekannte Angriffe

Nachteil:

schwächer gegen neue oder veränderte Angriffe

Merksatz:

Signaturen erkennen Bekanntes.

Anomaliebasierte Erkennung

Anomaliebasierte Erkennung sucht nach ungewöhnlichem Verhalten.

Beispiele:

Benutzer meldet sich plötzlich aus fremdem Land an
Server sendet ungewöhnlich viel Datenverkehr
Client verbindet sich zu vielen internen Systemen
Konto hat plötzlich viele Fehlversuche
Prozess verschlüsselt viele Dateien

Vorteil:

kann neue Angriffe erkennen

Nachteil:

mehr Fehlalarme möglich

Merksatz:

Anomalieerkennung erkennt Abweichungen vom Normalverhalten.

False Positive und False Negative

False Positive:

Ein Alarm wird ausgelöst,
obwohl kein echter Angriff vorliegt.

False Negative:

```
Ein echter Angriff wird nicht erkannt.
```

Beides ist problematisch.

Merksatz:

```
Sicherheitsalarme müssen bewertet und verbessert werden.
```

Antivirus

Antivirus-Software erkennt und blockiert bekannte Schadsoftware.

Typische Funktionen:

```
Dateiscan
Echtzeitschutz
Signaturprüfung
Quarantäne
Malware-Entfernung
einfache Verhaltensprüfung
```

Grenze:

```
Antivirus allein reicht nicht gegen moderne Angriffe.
```

Merksatz:

```
Antivirus ist eine Schutzschicht,
aber kein vollständiges Sicherheitskonzept.
```

EDR

EDR steht für:

```
Endpoint Detection and Response
```

EDR überwacht Endgeräte tiefer als klassischer Antivirus.

Typische Funktionen:

```
Prozessüberwachung
Verhaltensanalyse
Angriffserkennung
Isolation eines Endgeräts
Untersuchung von Vorfällen
zentrale Verwaltung
Reaktionsmaßnahmen
```

Merksatz:

```
EDR erkennt und untersucht Angriffe auf Endgeräten.
```

Endpoint

Ein Endpoint ist ein Endgerät oder System, das im Netzwerk genutzt wird.

Beispiele:

```
Notebook
Desktop-PC
Server
virtuelle Maschine
mobiles Gerät
Cloud-VM
```

Merksatz:

```
Endpoint = Endsystem,
auf dem Benutzer oder Dienste arbeiten.
```

EDR-Reaktionen

EDR kann bei einem Verdacht reagieren.

Beispiele:

```
Prozess beenden
Datei isolieren
Gerät vom Netzwerk trennen
Verbindung blockieren
Alarm erzeugen
forensische Daten sammeln
Datei in Quarantäne verschieben
```

Merksatz:

```
EDR ist nicht nur Erkennung,
sondern auch Reaktion.
```

XDR

XDR steht für:

```
Extended Detection and Response
```

XDR erweitert Erkennung und Reaktion über mehrere Bereiche.

Beispiele:

```
Endgeräte
E-Mail
Netzwerk
Cloud
Identitäten
Anwendungen
```

Ziel:

```
Ereignisse aus mehreren Quellen zusammenführen.
```

Merksatz:

```
XDR verbindet Sicherheitsdaten aus mehreren Bereichen.
```

SIEM

SIEM steht für:

```
Security Information and Event Management
```

Ein SIEM sammelt, speichert und analysiert Sicherheitsereignisse aus vielen Quellen.

Quellen können sein:

```
Firewalls
Server
Clients
Cloud-Dienste
IAM-Systeme
VPN
EDR
IDS
IPS
Webserver
Datenbanken
```

Merksatz:

```
SIEM ist zentrale Sicherheitslog-Auswertung.
```

SIEM-Aufgaben

Ein SIEM hilft bei:

```
Angriffserkennung
Korrelation von Ereignissen
Alarmierung
Nachvollziehbarkeit
Compliance
forensischer Analyse
Reporting
Incident Response
```

Beispiel:

```
Viele fehlgeschlagene Logins
plus
erfolgreicher Login aus fremdem Land
plus
Datenexport
```

Das SIEM kann diese Ereignisse zusammenführen.

Merksatz:

```
SIEM erkennt Zusammenhänge,
die einzelne Systeme allein nicht zeigen.
```

Korrelation

Korrelation bedeutet:

```
mehrere Ereignisse werden miteinander in Beziehung gesetzt.
```

Beispiel:

```
Loginfehler
danach erfolgreicher Login
danach Rollenänderung
danach Datenexport
```

Ein einzelnes Ereignis wirkt vielleicht harmlos. Zusammen kann es verdächtig sein.

Merksatz:

```
Korrelation erkennt Muster über mehrere Logs hinweg.
```

SOC

SOC steht für:

```
Security Operations Center
```

Ein SOC überwacht Sicherheitsereignisse, bewertet Alarme und koordiniert Reaktionen.

Aufgaben:

```
Monitoring
Analyse
Alarmbewertung
Incident Response
Kommunikation
Dokumentation
Verbesserung von Regeln
```

Merksatz:

```
SOC ist die organisatorische Stelle für Sicherheitsüberwachung.
```

SOAR

SOAR steht für:

```
Security Orchestration,
Automation and Response
```

SOAR automatisiert Sicherheitsabläufe.

Beispiele:

```
verdächtiges Konto automatisch sperren
IP-Adresse blockieren
Ticket erstellen
EDR-Isolation auslösen
Logdaten sammeln
Benachrichtigung senden
```

Merksatz:

SOAR automatisiert Reaktionen auf Sicherheitsereignisse.

MFA als Schutzmaßnahme

MFA steht für:

Multi-Faktor-Authentifizierung

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

Faktoren können sein:

Wissen:
Passwort oder PIN

Besitz:
Smartphone,
Token,
Smartcard

Sein:
biometrisches Merkmal

Merksatz:

MFA reduziert Schaden durch gestohlene Passwörter.

Starke Authentifizierung

Starke Authentifizierung bedeutet:

Anmeldung wird so abgesichert,
dass ein einzelnes schwaches Passwort nicht ausreicht.

Maßnahmen:

MFA
Hardwaretoken
Zertifikate
Conditional Access
Risikoanalyse
sichere Passwortregeln
Passwortmanager

Merksatz:

Starke Anmeldung schützt Identitäten.

Least Privilege als Schutzmaßnahme

Least Privilege bedeutet:

nur notwendige Rechte vergeben.

Vorteile:

weniger Schaden bei Kontoübernahme
weniger Risiko durch Fehler
weniger Angriffsfläche
bessere Kontrolle

Beispiele:

Benutzer kein lokaler Admin
Dienstkonto nur mit benötigten Rechten
Datenbankkonto ohne unnötige Löschrechte
Cloud-Rolle nur für konkrete Aufgabe

Merksatz:

Weniger Rechte bedeuten weniger möglicher Schaden.

Backup als Schutzmaßnahme

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

Besonders wichtig bei:

```
Ransomware
versehentlichem Löschen
Datenkorruption
Fehlkonfiguration
Hardwareausfall
Systemkompromittierung
```

Merksatz:

```
Backup ist Schutz gegen Datenverlust und Ausfallfolgen.
```

Gutes Backup-Konzept

Ein gutes Backup-Konzept klärt:

```
was gesichert wird
wie oft gesichert wird
wie lange gesichert wird
wo gesichert wird
wer Zugriff hat
wie Wiederherstellung getestet wird
wie Backups geschützt werden
wie schnell wiederhergestellt werden muss
wie viel Datenverlust erlaubt ist
```

Merksatz:

```
Backup ohne Restore-Test ist unvollständig.
```

Immutable Backup

Immutable bedeutet:

unveränderlich

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

Vorteile:

Schutz vor Ransomware
Schutz vor kompromittierten Adminzugängen
Schutz vor versehentlicher Löschung

Merksatz:

Immutable Backups schützen Wiederherstellungsmöglichkeiten.

Restore-Test

Ein Restore-Test prüft, ob Wiederherstellung wirklich funktioniert.

Zu prüfen:

Daten vollständig?
Anwendung startet?
Rechte passen?
Schlüssel vorhanden?
Wiederherstellungszeit akzeptabel?
Daten konsistent?
Dokumentation korrekt?

Merksatz:

Nur getestete Backups sind verlässlich.

Logging als Schutzmaßnahme

Logging bedeutet:

Ereignisse werden protokolliert.

Wichtige Logs:

```
Anmeldungen
Adminaktionen
Firewall-Entscheidungen
Dateiänderungen
Datenbankzugriffe
VPN-Zugriffe
Cloud-Audit-Logs
EDR-Meldungen
Webserver-Logs
```

Merksatz:

```
Logs machen Ereignisse nachvollziehbar.
```

Monitoring als Schutzmaßnahme

Monitoring überwacht Zustände und Metriken.

Beispiele:

```
ungewöhnliche Netzlast
viele Loginfehler
CPU-Spitzen
Speicher voll
Dienst nicht erreichbar
Zertifikat läuft ab
Backup fehlgeschlagen
viele Firewall-Drops
```

Merksatz:

```
Monitoring erkennt Probleme früh.
```

Alarmierung

Alarmierung informiert Verantwortliche automatisch, wenn Grenzwerte oder Sicherheitsereignisse auftreten.

Beispiele:

Malware-Fund
viele fehlgeschlagene Logins
Adminrolle vergeben
Backup fehlgeschlagen
ungewöhnlicher Datenexport
DDoS-Anzeichen
Cloud-Kostenanstieg

Merksatz:

Alarmierung macht kritische Ereignisse sichtbar.

Security Awareness

Security Awareness bedeutet:

Benutzer werden für Sicherheitsrisiken sensibilisiert.

Themen:

Phishing erkennen
Passwörter sicher nutzen
MFA-Anfragen richtig bewerten
vertrauliche Daten schützen
verdächtige Vorfälle melden
sichere Nutzung von Cloud-Diensten
Umgang mit USB-Geräten
Social Engineering erkennen

Merksatz:

Schulung macht Benutzer zu einem Teil der Verteidigung.

Incident Response

Incident Response bedeutet:

```
geplantes Vorgehen bei Sicherheitsvorfällen.
```

Typische Schritte:

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

Merksatz:

```
Incident Response muss vorbereitet sein,
bevor ein Vorfall passiert.
```

Containment

Containment bedeutet:

```
einen Sicherheitsvorfall eindämmen.
```

Beispiele:

```
infiziertes Gerät isolieren
Konto sperren
API-Schlüssel widerrufen
Firewall-Regel setzen
VPN-Zugang deaktivieren
kompromittierten Server vom Netz nehmen
Ausbreitung stoppen
```

Merksatz:

Containment begrenzt Schaden und Ausbreitung.

Eradication

Eradication bedeutet:

Ursache und Schadsoftware werden entfernt.

Beispiele:

Malware entfernen
System neu aufsetzen
Schwachstelle patchen
Backdoor entfernen
unsichere Konfiguration korrigieren
kompromittierte Zugangsdaten ersetzen

Merksatz:

Eradication beseitigt die Ursache des Vorfalls.

Recovery

Recovery bedeutet:

Systeme werden wiederhergestellt und kontrolliert in Betrieb genommen.

Dazu gehören:

Restore aus Backup
Systeme prüfen
Dienste starten
Monitoring beobachten
Benutzer informieren
erneute Kompromittierung ausschließen

Merksatz:

Recovery bringt Systeme sicher zurück in den Betrieb.

Lessons Learned

Lessons Learned bedeutet:

Nach einem Vorfall wird ausgewertet,
was verbessert werden muss.

Fragen:

Wie kam es zum Vorfall?
Was hat gut funktioniert?
Was hat nicht funktioniert?
Welche Maßnahmen fehlen?
Welche Regeln müssen geändert werden?
Welche Schulung ist nötig?
Welche Technik muss verbessert werden?

Merksatz:

Jeder Vorfall sollte zu besserer Sicherheit führen.

Physische Sicherheitsmaßnahmen

IT-Sicherheit umfasst auch physischen Schutz.

Beispiele:

Zutrittskontrolle
abschließbarer Serverraum
Videoüberwachung
Brandschutz
USV
Klimatisierung
gesicherte Netzwerkschränke
sichere Entsorgung von Datenträgern

Merksatz:

> Ohne physischen Schutz kann technische Sicherheit umgangen werden.

Organisatorische Sicherheitsmaßnahmen

Organisatorische Maßnahmen regeln, wie Sicherheit umgesetzt wird.

Beispiele:

> Sicherheitsrichtlinien
> Rollen und Verantwortlichkeiten
> Vier-Augen-Prinzip
> Freigabeprozesse
> Change Management
> Notfallhandbuch
> Berechtigungskonzept
> Schulungsplan
> Offboarding-Prozess

Merksatz:

> Sicherheit braucht klare Prozesse und Verantwortlichkeiten.

Technische Sicherheitsmaßnahmen

Technische Maßnahmen schützen Systeme direkt.

Beispiele:

> Firewall
> MFA
> Verschlüsselung
> EDR
> IDS
> IPS
> Backup
> Patchmanagement

Hardening
Netzwerksegmentierung
Logging
Monitoring
Zugriffskontrolle

Merksatz:

Technische Maßnahmen wirken nur gut,
wenn sie richtig konfiguriert und betrieben werden.

Personelle Sicherheitsmaßnahmen

Personelle Maßnahmen betreffen das Verhalten von Menschen.

Beispiele:

Schulungen
Sensibilisierung
klare Meldewege
sichere Passwortnutzung
Verhalten bei Phishing
Umgang mit vertraulichen Daten
Wissen über Social Engineering

Merksatz:

Menschen müssen wissen,
wie sie sicher handeln sollen.

Sicherheitsmaßnahmen nach Angriffsziel

Angriffsziel	passende Maßnahmen
Passwortdiebstahl	MFA, Passwortmanager, Schulung
Malware	EDR, Patchmanagement, Rechtebegrenzung
Ransomware	Backup, Immutable Backup, Segmentierung
DDoS	DDoS-Schutz, Rate Limiting, CDN

Angriffsziel	passende Maßnahmen
Webangriffe	Secure Coding, WAF, Code Review
Datenabfluss	DLP, Verschlüsselung, Rechtekonzept
Insider-Risiko	Logging, Least Privilege, Vier-Augen-Prinzip
Kontoübernahme	MFA, Conditional Access, Monitoring

Merksatz:

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

Typische Kombinationen in der Praxis

Beispiel Webserver:

```
Firewall
WAF
Patchmanagement
TLS
Logging
Monitoring
Backup
Rechtebegrenzung
```

Beispiel Client:

```
EDR
Patchmanagement
keine lokalen Adminrechte
E-Mail-Schutz
Makro-Schutz
Schulung
```

Beispiel Cloud:

```
MFA
IAM
Security Groups
```

Audit-Logs
Verschlüsselung
Backup
Kostenalarme

Merksatz:

Unterschiedliche Systeme brauchen unterschiedliche Schutzpakete.

Typische Fehler bei Sicherheitsmaßnahmen

Häufige Fehler:

nur eine Maßnahme einsetzen
Firewall-Regeln nie prüfen
Logs nicht aktivieren
Alarme ignorieren
Backups nicht testen
MFA-Ausnahmen zu breit erlauben
Adminrechte dauerhaft vergeben
EDR nur installieren,
aber nicht überwachen
SIEM ohne klare Regeln betreiben
Schulung vernachlässigen
Incident Response nicht üben

Merksatz:

Sicherheitsmaßnahmen müssen betrieben,
geprüft
und verbessert werden.

Checkliste: Schutzmaßnahmen sinnvoll kombinieren

Risiken bestimmen.
Schutzziele festlegen.
Systeme inventarisieren.

```
Firewall-Regeln prüfen.
Segmentierung planen.
MFA aktivieren.
Rechte minimieren.
Patchmanagement organisieren.
Hardening durchführen.
EDR einsetzen.
Logs zentral sammeln.
SIEM oder zentrale Auswertung nutzen.
Backups schützen.
Restore testen.
Benutzer schulen.
Incident Response vorbereiten.
Maßnahmen regelmäßig prüfen.
```

Merksatz:

```
Sicherheit ist ein Prozess,
kein einmaliger Zustand.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was ist Defense in Depth?
- Was ist eine Firewall?
- Was ist der Unterschied zwischen Paketfilter und Stateful Firewall?
- Was ist eine Next-Generation Firewall?
- Was bedeutet Default Deny?
- Warum ist Netzwerksegmentierung wichtig?
- Was ist eine DMZ?
- Was ist ein IDS?
- Was ist ein IPS?
- Was ist der Unterschied zwischen IDS und IPS?
- Was ist EDR?
- Was ist SIEM?
- Was bedeutet Korrelation im SIEM?
- Was ist ein SOC?
```

- Was ist SOAR?
- Warum ist MFA wichtig?
- Warum ist Backup eine Sicherheitsmaßnahme?
- Was ist ein Restore-Test?
- Was ist Incident Response?
- Was bedeutet Containment?
- Warum sind Schulungen wichtig?

Typische Prüfungsfallen

Firewall ersetzt kein Patchmanagement.

Antivirus ersetzt kein Sicherheitskonzept.

IDS und IPS unterscheiden.

IDS erkennt,
IPS blockiert.

EDR ist mehr als klassischer Antivirus.

SIEM sammelt und korreliert Logs.

SOC ist organisatorische Sicherheitsüberwachung.

SOAR automatisiert Reaktionen.

Backup verhindert keinen Angriff,
hilft aber bei Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Immutable Backup schützt vor Manipulation.

MFA schützt stark gegen Passwortmissbrauch,
aber nicht gegen alles.

Segmentierung begrenzt Ausbreitung.

Default Deny ist sicherer als pauschales Erlauben.

Logs müssen vor dem Vorfall aktiv sein.

Alarme müssen bearbeitet werden.

Schulungen sind Sicherheitsmaßnahme.

Incident Response muss vorbereitet sein.

Sicherheit braucht Technik,
Organisation
und Menschen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Sicherheitsmaßnahme	Maßnahme zur Risikoreduzierung
Defense in Depth	mehrschichtige Verteidigung
Prävention	Angriff verhindern
Erkennung	Angriff feststellen
Reaktion	auf Angriff reagieren
Firewall	Filter für Netzwerkverkehr
Paketfilter	prüft grundlegende Paketdaten
Stateful Firewall	merkt sich Verbindungszustände
Application Firewall	prüft Anwendungsebene
NGFW	Next-Generation Firewall
Default Deny	standardmäßig alles blockieren
Segmentierung	Trennung von Netzbereichen
VLAN	logische Netztrennung
DMZ	Zone für öffentlich erreichbare Dienste
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Signatur	bekanntes Angriffsmuster
Anomalie	Abweichung vom Normalverhalten

Begriff	Kurze Erklärung
False Positive	falscher Alarm
False Negative	nicht erkannter Angriff
Antivirus	Schutz gegen bekannte Schadsoftware
EDR	Endpoint Detection and Response
Endpoint	Endgerät oder Endsystem
XDR	erweiterte Erkennung und Reaktion
SIEM	zentrale Sicherheitslog-Auswertung
Korrelation	Verknüpfung mehrerer Ereignisse
SOC	Security Operations Center
SOAR	automatisierte Sicherheitsreaktion
MFA	Multi-Faktor-Authentifizierung
Least Privilege	minimale notwendige Rechte
Backup	zusätzliche Datensicherung
Immutable Backup	unveränderliches Backup
Restore-Test	Prüfung der Wiederherstellung
Logging	Ereignisprotokollierung
Monitoring	Zustandsüberwachung
Alerting	automatische Alarmierung
Awareness	Sicherheitsbewusstsein
Incident Response	Reaktion auf Sicherheitsvorfälle
Containment	Eindämmung
Eradication	Beseitigung der Ursache
Recovery	Wiederherstellung
Lessons Learned	Auswertung und Verbesserung

IHK-sichere Kurzformulierung

Sicherheitsmaßnahmen sollen Risiken für Vertraulichkeit, Integrität und Verfügbarkeit reduzieren. Da einzelne Maßnahmen versagen können, werden mehrere Schutzschichten nach dem Prinzip Defense in Depth kombiniert. Firewalls begrenzen Netzwerkverkehr, Segmentierung trennt Netzbereiche, IDS erkennt Angriffe, IPS kann sie zusätzlich blockieren, EDR überwacht Endgeräte und SIEM sammelt und korreliert Sicherheitslogs. MFA schützt Identitäten, Least Privilege begrenzt Rechte, Backups und Restore-Tests sichern Wiederherstellung, und Incident Response regelt das Vorgehen bei Sicherheitsvorfällen. Gute IT-Sicherheit verbindet technische, organisatorische,

personelle und physische Maßnahmen.

Merksätze

Sicherheit braucht mehrere Schutzschichten.

Defense in Depth kombiniert Maßnahmen.

Prävention verhindert.

Erkennung erkennt.

Reaktion begrenzt Schaden.

Firewall filtert Netzwerkverkehr.

Paketfilter prüft Paketdaten.

Stateful Firewall kennt Verbindungen.

Application Firewall prüft Anwendungsebene.

Default Deny ist sicherer.

Segmentierung begrenzt Ausbreitung.

VLAN trennt logisch.

DMZ schützt interne Netze.

IDS erkennt Angriffe.

IPS blockiert zusätzlich.

Signaturen erkennen Bekanntes.

Anomalien erkennen Abweichungen.

False Positive ist falscher Alarm.

False Negative ist verpasster Angriff.

Antivirus ist nur eine Schutzschicht.

EDR erkennt und reagiert auf Endgeräten.

XDR verbindet mehrere Sicherheitsbereiche.

SIEM sammelt und korreliert Logs.

SOC überwacht Sicherheit organisatorisch.

SOAR automatisiert Reaktionen.

MFA schützt Identitäten.

Least Privilege begrenzt Schaden.

Backup hilft bei Wiederherstellung.

Immutable Backup schützt Backups.

Restore-Test beweist Backup-Nutzbarkeit.

Logging macht Ereignisse nachvollziehbar.

Monitoring erkennt Probleme.

Alarmierung muss bearbeitet werden.

Schulung ist Sicherheitsmaßnahme.

Incident Response braucht Vorbereitung.

Containment begrenzt Ausbreitung.

Eradication beseitigt Ursache.

Recovery stellt Betrieb wieder her.

Lessons Learned verbessern Sicherheit.

Sicherheit ist ein Prozess,

kein einmaliger Zustand.