9 IT-Sicherheit und Datenschutz

- 01 Maßnahmen der IT-Sicherheit
- 02 Datenschutz
- 03 IT-Grundschutz/BSI
- 04 ISMS
- 05 Härtung von Betriebssystemen
- 06 Backup-Verfahren
- 07 Kryptografie
- 08 WLAN Sicherheit
- 09 VPN
- 10 Firewall
- 11 DMZ
- 12 Leitlinien für Software-Entwicklung

01 Maßnahmen der IT-Sicherheit

- Schutzziele
- Organisatorische Maßnahmen
  - IT-Sicherheitsbeauftragte
  - Datenschutzbeauftragte
- Technische Maßnahmen
- Personelle Maßnahmen
- Compliance
- Security by Default
- Security by Design
- Schwachstellenanalyse
- Log Management
- IAM
- Basis-Sicherheitscheck
- Penetrationstest
- 5 Stufen im Sicherheitstest

Schutzziele

Vertraulichkeit:	Integrität:	Verfügbarkeit:
• Schutz der Daten vor unberechtigtem Zugriff durch Zugriffsschutz und Verschlüsselung	• Schutz der Daten vor unbemerkten Veränderungen und Löschen durch Vorkehrungen, die Änderungen schnell erkennen	• Schutz der Daten vor unerwünschtem Ausfall z. B. mit Hilfe einer Risikoanalyse und entsprechenden Vorkehrungen

Organisatorische Maßnahmen

- Beziehen sich auf die Organisation und Verwaltung von IT-Systemen und -Prozessen
- Sicherstellen, dass alle Mitarbeiter im Unternehmen ein angemessenes Sicherheitsbewusstsein haben und die IT-Sicherheit im Unternehmen gewährleistet ist

Beispiele:

- Bestellung eines IT-Sicherheitsbeauftragten
- Erstellung einer IT-Sicherheitsrichtlinie (z.B. Passwort-Policy)
- Implementierung von Verhaltensregeln

IT-Sicherheitsbeauftragte

- Unterstützung und Beratung der Unternehmensführung in Fragen der IT-Sicherheit

Aufgaben:

- Erstellung eines IT-Sicherheitskonzeptes
- Entwicklung eines Risikomanagements
- Einführung eines Managementsystems
- Einführung unternehmensweiter Sicherheitsrichtlinien
- Überprüfung und Dokumentation des Sicherheitsniveaus im Unternehmen
- Schulung und Sensibilisierung der Mitarbeitenden und die Beratung der Unternehmensleitung in allen Bereichen der IT-Sicherheit

Datenschutzbeauftragte

- Gestaltung, Kontrolle sowie Kommunikation der Umsetzung datenschutzrechtlicher Vorgaben

Aufgaben:

- Sicherstellen der Umsetzung der Vorgaben der DSGVO und der sonstigen datenschutzrechtlichen Regelungen
- Verhindern von Datenschutzverletzungen
- Sensibilisierung und Schulung der Mitarbeitenden
- Beratung und Überwachung der Datenschutz-Folgeabschätzung
- Vermittler zwischen Unternehmen, Betroffenen und Aufsichts-behörden

Technische Maßnahmen

- Umfassen alle technischen Lösungen, die dazu dienen, IT-Systeme und Daten zu schützen

Beispiele:

- Einsatz von Virenschutzsystemen
- Personal Firewalls
- Portsecurity
- Anti-Spam-Systeme
- Verschlüsselung von Daten
- Überwachung von Zugriffen
- Einrichtung von Backup-Systemen
- Device Security Check (Gerätesicherheitsprüfung)

Personelle Maßnahmen

- Zielen auf die Mitarbeiter ab
- Sensibilisierung der Mitarbeitenden für die Bedeutung der Informationssicherheit
- Befähigung der Mitarbeitenden zur Erhöhung der Informationssicherheit im Unternehmen beizutragen
- Sicherheitsbewusstsein herstellen

Beispiele:

- Schulungen, um Mitarbeiter über Sicherheitsrisiken und Schutzmaßnahmen aufzuklären
- Einführung von Verhaltensregeln und die Implementierung von Anreizsystemen zur Förderung eines sicherheitsbewussten Verhaltens der Mitarbeiter

Compliance

- Regelkonformität eines Unternehmens oder einer Organisation im Hinblick auf:
  - Gesetze und Verordnungen
  - Verträge und Standards
  - interne Richtlinien und Ethikvorgaben
- In der IT betrifft Compliance insbesondere:
  - Datenschutzgesetze
  - IT-Sicherheitsvorgaben
  - branchenspezifische Standards
  - Lizenzbedingungen für Software
  - Pflichten zur Dokumentation und Nachvollziehbarkeit

Typische Compliance-Regelungen in der IT und im Datenschutz

- **Datenschutz & Informationssicherheit**
  - DSGVO, BDSG, BSI IT-Grundschutz
- **IT-Sicherheits- und Branchenvorgaben**
  - KRITIS-Verordnung, NIS2-Richtlinie
- **Technische und organisatorische Regelwerke**
  - Rechtemanagement, Homeoffice-Richtlinien, Protokollierungsrichtlinien
- **Softwarelizenz-Compliance**
  - Verwendung nur lizenzierter Software
  - Keine Urheberrechtsverletzungen durch illegale Kopien
  - Einhaltung von Lizenzmodellen (z. B. Open Source unter MIT, GPL, etc.)
  - Lizenznachweise für Audits bereithalten

Security by Design

- Integration der Sicherheit als grundlegendes Element in:
  - Software-Designphase
  - Software-Entwicklungsprozess
  - Produktlebenszyklus
- Produktsicherheit ist Kernelement des Entwurfsprozesses
- Software ist widerstandsfähig gegen gängige Sicherheitsbedrohungen

Beispiele:

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Memory Safe Programming

Security by Default

- Software ist bei Kauf sofort sicher ohne zusätzlicher Sicherheitskonfiguration
- Standardeinstellungen schützen sofort nach dem Auspacken gegen gängige Ausnutzungstechniken
- Oft minimale Änderungen durch Verbraucher erforderlich

Beispiele:

- Sicherheitseinstellung mit geringer Komplexität
- Forcieren von Multi-Faktor-Authentifikation
- Verzicht von Default-Passwörtern

Schwachstellenanalyse

- systematischer Prozess zur Identifikation, Bewertung und Dokumentation von Sicherheitslücken in IT-Systemen, Anwendungen oder Infrastrukturen, bevor diese von Angreifern ausgenutzt werden können

Bestandteil der Analyse	Beschreibung
Asset-Erfassung	Welche Systeme, Dienste, Anwendungen und Geräte existieren überhaupt?
Informationssammlung	Erhebung technischer Details (IP-Adressen, Softwareversionen, Dienste etc.)
Identifikation von Schwachstellen	Abgleich gegen bekannte Schwachstellen (z. B. CVEs)
Risikobewertung	Einschätzung von Eintrittswahrscheinlichkeit & Schadenshöhe
Kategorisierung & Priorisierung	Z. B. nach CVSS (Common Vulnerability Scoring System)
Dokumentation & Reporting	Ergebnisse werden verständlich und nachvollziehbar dokumentiert
Maßnahmenempfehlung	Welche Schwachstellen sollen wann und wie behoben werden?

Log Management

- umfasst die Erfassung, Speicherung, Verarbeitung, Analyse und Archivierung von Logdaten aus verschiedenen IT-Systemen, um sicherheitsrelevante und betriebliche Informationen sichtbar und auswertbar zu machen

Komponente	Beschreibung
Erzeugung (Logging)	Systeme (Server, Firewalls, Anwendungen etc.) generieren Logdaten
Sammeln (Collection)	Logs werden zentralisiert – z. B. via Agenten, Syslog, APIs
Speicherung (Storage)	Logs werden sicher gespeichert (z. B. manipulationssicher, komprimiert)
Analyse (Processing)	Suche nach Mustern, Korrelation, Filterung
Visualisierung	Darstellung über Dashboards, Graphen, Alerts
Archivierung & Aufbewahrung	Langfristige Speicherung für Forensik oder gesetzliche Nachweise
Alarmierung (Alerting)	Automatische Benachrichtigung bei bestimmten Ereignissen oder Anomalien
Löschung / Rotation	Alte Logs werden nach Aufbewahrungsfrist gelöscht oder archiviert

IAM 1/3

Identity and Access Management

- zentrales Konzept der IT-Sicherheit
- Identitäts- und Zugriffsverwaltung
- umfasst alle Prozesse, Technologien und Richtlinien, mit denen digitale Identitäten verwaltet und der Zugriff auf IT-Ressourcen gesteuert wird
- IAM-Systeme verwalten:
  - **Identitäten** (Benutzer, Rollen, Maschinenkonten)
  - **Authentifizierung** (Ist die Person, wer sie vorgibt zu sein?)
  - **Autorisierung** (Was darf die Person tun?)
  - **Rechteverwaltung** (Zugriffssteuerung auf Daten, Systeme, Anwendungen)
  - **Nutzerlebenszyklen** (Anlegen, ändern, sperren, löschen von Accounts)

IAM 2/3

Ziele

Ziel	Erklärung
Vertraulichkeit	Nur berechtigte Nutzer sehen sensible Daten
Integrität	Nur autorisierte Personen dürfen Daten verändern
Verfügbarkeit	Benutzer haben jederzeit Zugriff auf benötigte Ressourcen – falls berechtigt
Nachvollziehbarkeit	Wer hat wann worauf zugegriffen?
Automatisierung & Effizienz	Zentrale Verwaltung statt manueller Einzelrechte
Regelkonformität (Compliance)	DSGVO, ISO 27001, BSI-Grundschutz etc.

IAM 3/3

Komponenten

Komponente	Funktion
Identitätsmanagement	Verwaltung von Nutzeridentitäten, Rollen und Gruppen
Authentifizierung	Überprüfung der Identität (z. B. Passwort, 2FA, biometrisch)
Autorisierung	Zugriffskontrolle auf Ressourcen basierend auf Rollen oder Richtlinien
Zugriffsprotokollierung	Audit-Trails und Logs über Anmelde- und Zugriffsvorgänge
Provisioning/Deprovisioning	Automatisiertes Einrichten und Entfernen von Accounts

Basis-Sicherheitscheck

- vereinfachter, strukturierter Schnelltest, der einen ersten Überblick über das aktuelle IT-Sicherheitsniveau einer Organisation liefert
- eignet sich besonders für kleine und mittelständische Unternehmen, Behörden oder Bildungseinrichtungen
- Systematisches Erkennen sicherheitsrelevanter Schwachstellen – ohne tiefgehender Fachkenntnisse oder komplexer Werkzeuge
- Ergänzt durch Sicherheitsanalyse mit Risikoanalyse (BSI-Standards 100-3)

Sicherheitsanalyse mit Risikoanalyse (BSI-Standards 100-3)

- detaillierte Risikoanalyse, bei der spezifische Gefährdungen, die über den IT-Grundschutz hinausgehen, identifiziert, bewertet und behandelt werden (z. B. bei Staatsgeheimnissen, kritischer Infrastruktur etc.)
- Integriert in IT-Grundschutz nach BSI und ISMS

- Bestandteile:
  - Schutzbedarfsfeststellung
  - Ermittlung ergänzender Gefährdungen
  - Risikoanalyse
  - Bewertung der Risiken
  - Entwicklung & Auswahl von Maßnahmen
  - Maßnahmenumsetzung & Erfolgskontrolle

Penetrationstest 1/3

- geplanter, autorisierter Sicherheitsangriff auf ein System oder Netzwerk, um Schwachstellen aufzudecken – bevor sie von echten Angreifern ausgenutzt werden
- durch interne oder externe Security-Expert*innen durchgeführt
- simuliert realistische Angriffsszenarien, inklusive technischer, organisatorischer und – bei Social Engineering – menschlicher Schwächen
- **Typische Bewertungsskala nach BSI-Standards**

Risikoklasse	Eintrittswahrscheinlichkeit	Schadenshöhe	Priorität
Hoch	Sehr wahrscheinlich	Kritisch (z. B. Datenklau)	Sofortige Maßnahme
Mittel	Möglich	Spürbarer Betriebsausfall	Bald behandeln
Niedrig	Unwahrscheinlich	Gering (z. B. Infoleck)	Beobachten

Penetrationstest 2/3

- BSI Klassifikationsschema

Kriterium	Klassifikationsausprägungen
Testziel	Schwachstellen finden / Wirksamkeit von Maßnahmen prüfen / Resilienz testen
Testumfang	Einzelrechner, Applikation, ganzes Netz, KRITIS-Teilbereich
Testtiefe	Oberflächliche Analyse → bis zu tiefem Angriff mit Exploit-Nutzung
Kenntnisstand (Black/Grey/White Box)	Black Box = keine Infos; White Box = Quellcode, Architektur offengelegt
Beteiligungsgrad	IT-Abteilung informiert (offener Test) vs. verdeckter Test (Red Teaming)
Angriffsart	Technisch (Netzwerk, Web, Client), organisatorisch (z. B. Prozesse) oder menschlich (Social Eng.)

Penetrationstest 3/3

- Arten von Sicherheitstests gem. BSI

Testart	Zielsetzung	Beispiele
Technischer Penetrationstest	Test von Netzwerken, Anwendungen, Geräten	z. B. Portscan, SQL Injection, RCE-Tests
Social-Engineering-Test	Test der Mensch-Faktor-Sicherheit	z. B. Phishing, Telefonangriff, USB-Drop
Physical Penetrationtest	Test physischer Zutrittskontrollen	z. B. Zutritt zu Serverraum, Zugang via Schlüsselkarte
Red-Teaming (mehrtägig)	Simulierte Angriffe über alle Ebenen (technisch, menschlich, physisch)	Realitätsnahe KRITIS-Tests mit Zielerreichung
Schwachstellenscan (Vulnerability Assessment)	Breite Erkennung bekannter Schwachstellen mit automatisierten Tools	z. B. OpenVAS, Nessus

5 Stufen eines Sicherheitstest 1/3

1. Vorbereitungsphase (Planung und Zieldefinition)

- **Ziel:**
  - Klärung von Rahmenbedingungen und Zielsetzungen
  - Sicherstellen, dass alle Beteiligten informiert und einverstanden sind
- **Typische Aufgaben:**
  - Festlegung des Testumfangs
  - Testziele definieren
  - Testart wählen
  - Genehmigungen einholen
  - Risikoabschätzung und Kommunikationsplan
  - Auswahl von Tools, Methoden und Testenden (intern/extern)

2. Informationsbeschaffung (Reconnaissance / Footprinting)

- **Ziel:**
  - Möglichst viele verwertbare Informationen über die Zielsysteme sammeln
- **Typische Aufgaben:**
  - Passive Informationsbeschaffung:
    - Whois-Abfragen, DNS-Informationen, Google-Hacking, OSINT-Quellen
  - Aktive Erkundung (falls erlaubt):
    - Netzwerkscans
    - Banner Grabbing
    - Erkennung von Firewall- und IDS/IPS-Schutzmaßnahmen
    - Subdomain-Enumeration, API-Endpunkte, Testsysteme

5 Stufen eines Sicherheitstest 2/3

3. Bewertung der Informationen (Schwachstellenanalyse)

- **Ziel:**
  - Identifikation und Bewertung potenzieller Schwachstellen und Angriffspunkte
- **Typische Aufgaben:**
  - Zuordnung der gefundenen Infos zu bekannten CVE-Einträgen
  - Abgleich mit Schwachstellendatenbanken
  - Analyse offener Ports und Dienste
  - Risikobewertung:
    - Eintrittswahrscheinlichkeit × Schadenshöhe
    - ggf. Bewertung nach CVSS (Common Vulnerability Scoring System)
  - Priorisierung

4. Versuch des aktiven Eindringens (Exploitation)

- **Ziel:**
  - Nachweis, dass Schwachstellen ausgenutzt werden können → „Proof of Concept“
- **Typische Aufgaben:**
  - Durchführung gezielter Angriffe auf gefundene Schwachstellen
  - Nutzung von Exploits
  - Versuch der Privilegienerweiterung
  - Optional: Persistenz einrichten
  - Dokumentation aller Schritte, Screenshots, Payloads, Reaktionen

5 Stufen eines Sicherheitstest 3/3

5. Auswertung der Ergebnisse (Bericht & Handlungsempfehlung)

- **Ziel:**
  - Alle Ergebnisse dokumentieren, Schwachstellen priorisieren, Maßnahmen vorschlagen
- **Typische Aufgaben:**
  - Übersicht getesteter Systeme
  - Beschreibung jeder identifizierten Schwachstelle:
    - Technischer Hintergrund
    - Angriffsvektor und Erfolgswahrscheinlichkeit
    - Potenzieller Schaden
  - Nachweis der Ausnutzung (Beweise, Screenshots, Logs)
  - Empfehlungen zur Behebung:
    - Sofortmaßnahmen
    - Mittel- und langfristige Verbesserungen
  - Gesamtrisikobewertung
  - Abschlussgespräch / Ergebnispräsentation für IT & Management

02 Datenschutz

- DSGVO
- BDSG
- Datenschutzgrundsaätze nach Art. 5 DSGVO
- Definition personenbezogener Daten
- Maßnahmen des Datenschutzes
- Betroffenenrechte
- Persönlichkeitsrechte
- Anonymisierung vs. Pseudonymisierung
- Archivierung

DSGVO

Datenschutz-Grundverordnung

- DSGVO steht über nationalem Recht
- Andere Regelungen sind nur möglich, wenn die DSGVO das erlaubt (Öffnungsklauseln der DSGVO)
- Ziele:
  - Harmonisierung des Datenschutzes in den Mitgliedsstaaten der Europäischen Union
- Seit Mai 2018 als EU-weites einheitliches Datenschutzgesetz anwendbar

BDSG

Bundesdatenschutzgesetz

- Neue Fassung vom Mai 2018 (BDSG-neu)
- Gilt in den Bereichen, in denen die DSGVO das zulässt
- BDSG und DSGVO ergänzen sich gegenseitig

- Gültigkeit:
  - Gilt für öffentlichen Stellen des Bundes (Bundesverwaltung), nicht-öffentliche Bereiche und die öffentliche Hand wenn diese im Wettbewerb stehen
  - Nicht-öffentliche Bereiche: Wirtschaftsunternehmen, Vereine

Datenschutz Grundsätze nach Art. 5 DSGVO

1. Rechtmäßigkeit (Gesetzmäßigkeit)

- **Definition:**
  Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn **eine gesetzliche Grundlage** besteht (z. B. Einwilligung, Vertrag, rechtliche Pflicht)

- **Beispiel:**
  Ein Onlineshop darf Kundendaten zur Vertragserfüllung (z. B. Versand) verarbeiten – nicht aber für Werbung ohne Zustimmung

2. Transparenz

- **Definition:**
  Betroffene müssen verständlich und leicht zugänglich informiert werden

- **Beispiel:**
  Datenschutzerklärung auf Websites, Informationspflichten bei Erhebung von Daten

3. Zweckbindung

- **Definition:**
  Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden

  nicht für andere, unvereinbare Zwecke

- **Beispiel:**
  Daten, die zur Bewerbung verarbeitet wurden, dürfen nicht ohne Weiteres für Werbezwecke verwendet werden

4. Datenminimierung / Verhältnismäßigkeit

- **Definition:**
  Nur so viele Daten wie erforderlich dürfen erhoben werden

  Grundsatz: So wenig wie möglich, so viel wie nötig

- **Beispiel:**
  Eine App zur Essensbestellung benötigt keine Angaben zur Religionszugehörigkeit des Nutzers

5. Richtigkeit

- **Definition:**
  Daten müssen sachlich richtig und auf dem neuesten Stand sein. Unrichtige Daten sind zu löschen oder zu korrigieren

- **Beispiel:**
  Falsche Adressdaten im Kundenkonto müssen korrigiert werden, wenn der Kunde dies mitteilt

6. Speicherbegrenzung

- **Definition:**
  Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist

  Danach: Löschung oder Anonymisierung

- **Beispiel:**
  Bewerbungsdaten nicht erfolgreicher Kandidaten sollten nach 6 Monaten gelöscht werden

7. Integrität und Vertraulichkeit

- **Definition:**
  Daten müssen durch geeignete technische und organisatorische Maßnahmen (TOMs) geschützt werden:
  - gegen unbefugten Zugriff
  - gegen Verlust oder Zerstörung

- **Beispiel:**
  Zugriffsschutz, Verschlüsselung, Firewalls, Zugriffsrechte

8. Rechenschaftspflicht („Accountability“)

- **Definition:**
  Der Verantwortliche muss nachweisen können, dass alle Datenschutzgrundsätze eingehalten werden

- **Beispiel:**
  Dokumentation von Einwilligungen, Datenschutz-Folgenabschätzungen, Verarbeitungsverzeichnisse

9. Informationssicherheit

- **Definition:**
  Bezieht sich auf den technischen Schutz der Daten
  Teil von Integrität & Vertraulichkeit,
  eigenständig betont

- **Umfasst:**
  - Verfügbarkeit (Daten sind erreichbar, wenn sie gebraucht werden)
  - Integrität (Daten sind korrekt und vollständig)
  - Vertraulichkeit (Daten sind vor unbefugtem Zugriff geschützt)

Definition personenbezogener Daten

- Artikel 4 DSGVO
  - "alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** [...] beziehen"
- §46 Abs. 1 BDSG
  - "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren **natürlichen Person** (Betroffener)"

Beispiele

- Name
- Adresse
- Telefonnummer
- Kreditkarten- oder Personalnummer
- Autokennzeichen
- Kontodaten
- Online-Daten wie IP-Adresse oder Standortdaten
- physische Daten wie das Aussehen

Maßnahmen des Datenschutzes

- §3a BDSG
  - Datensparsamkeit und -vermeidung
- Art. 5 Abs. 1 DSGVO
  - Rechtmäßigkeit und Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit der Daten
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit

Betroffenenrechte

- Betroffene Personen haben Recht auf:
  - Auskunft
  - Berichtigung
  - Löschung
  - Einschränkung
  - Widerspruch
  - Datenübertragbarkeit

Persönlichkeitsrechte

- ergänzen die Datenschutzgrundrechte und sind wichtige Bestandteile des **allgemeinen Persönlichkeitsrechts** nach deutschem Verfassungs- und Zivilrecht
  - Recht auf informationelle Selbstbestimmung
  - Recht am eigenen Bild
  - Recht am geschriebenen/gesprochenen Wort
  - Recht auf Schutz vor Imitation der Persönlichkeit
  - Recht auf Schutz der Intim-, Privat- und Geheimsphäre

Anonymisierung vs. Pseudonymisierung

Anonymisierung

- Verändern personenbezogener Daten derart, dass diese Daten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können
- Vollständige Anonymisierung ist sehr schwer zu erlangen

Pseudonymisierung

- Ersetzen von Name oder eines anderen Identifikationsmerkmals durch ein Pseudonym (zumeist ein Code, bestehend aus einer Buchstaben- oder Zahlenkombination)
- Feststellung der Identität des Betroffenen wird ausgeschlossen oder wesentlich zu erschwert
- Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, bleiben erhalten
- Ermöglicht die Zuordnung von Daten zu einer Person, mit Hilfe eines Schlüssel

Archivierung

- **strukturierte, dauerhafte und unveränderbare Aufbewahren** von Daten, Dokumenten oder Informationen zu rechtlichen, geschäftlichen oder historischen Zwecken

- **Ziel:**
  - Beweissicherung
  - Nachvollziehbarkeit
  - rechtliche Absicherung
- **Daten müssen** lesbar, auffindbar und vor Veränderung geschützt sein
- **Typische Bsp.:** Rechnungen, Verträge, Geschäftsbriefe, Steuerunterlagen, Patientenakten

Archivierung – Technologische Anforderungen

- **Sicherheit & Integrität** (Schutz vor unbefugtem Zugriff, Digitale Signatur, Hash-Werte, Manipulationssicherheit)
- **Struktur & Wiederauffindbarkeit** (Metadaten für die Indexierung, Suchfunktionalität, Dokumentenklassifikation)
- **Revisionssicherheit** (Nachvollziehbarkeit, Unveränderbarkeit, Protokollierung von Zugriffen)

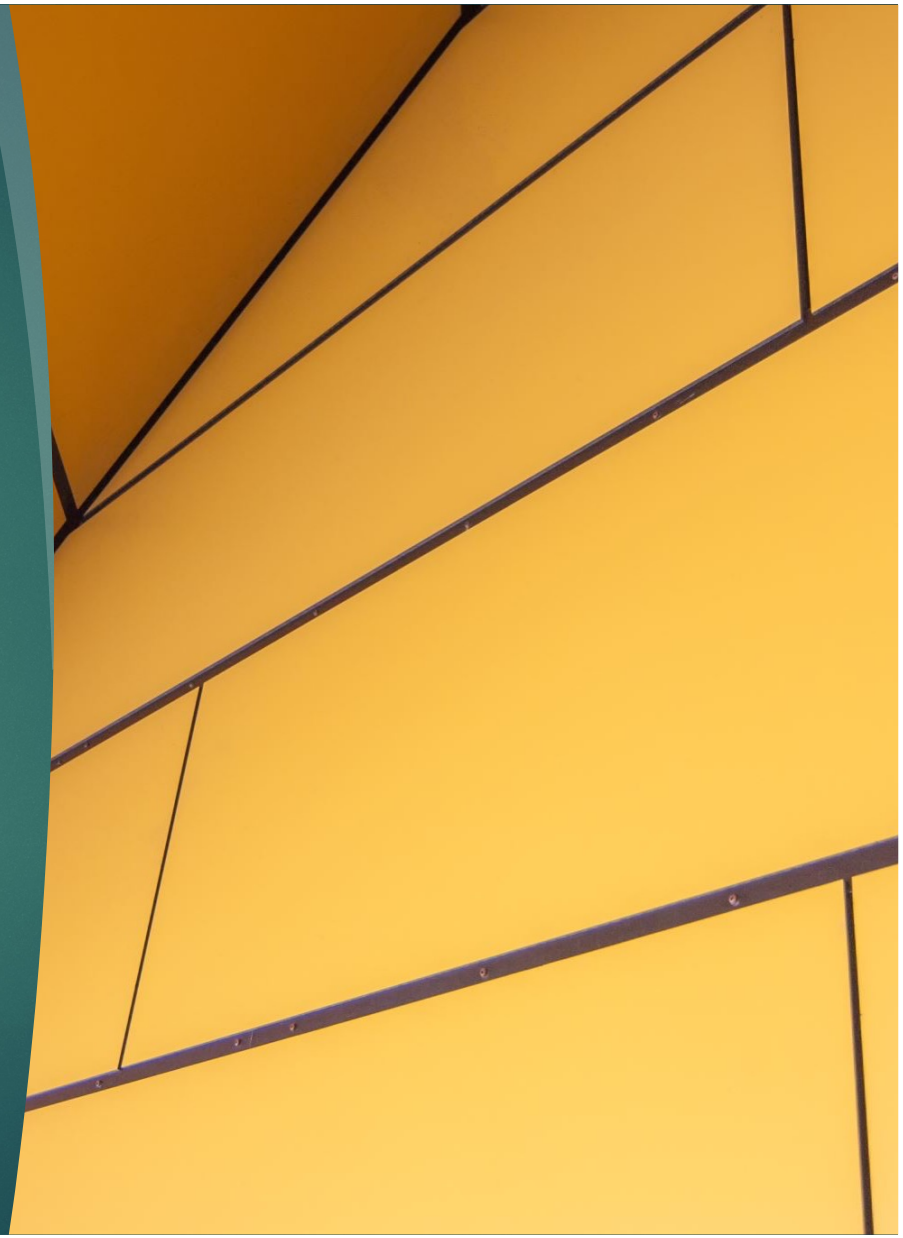
- **Formate & Standards:**
  - PDF/A, TIFF, XML
  - ISO 19005 (Langzeitarchivierung)

Archivierung – Fristen Beispiele

Dokument / Inhalt	Frist	Grundlage
Handelsbriefe, Buchungsbelege	6 Jahre	HGB, AO
Jahresabschlüsse, Bilanzen	10 Jahre	HGB
Steuerbescheide, Rechnungen	10 Jahre	AO
Patientenakten (ärztlich)	10 Jahre	BGB, ggf. länger nach Einzelfall
Arbeitsverträge, Personalakten	bis zu 10 Jahre	HGB, ArbZG, AGG

03 IT-Grundschutz des BSI

- IT-Grundschutz des BSI
- BSI-Standards
- IT-Grundschutz-Kompendium
- IT-Grundschutz Bausteine
- Schutzbedarfskategorien
- Schutzbedarfsanalyse
- Risikomatrix



IT-Grundschutz des BSI

BSI = Bundesamts für Sicherheit in der Informationstechnik

- Vorgehensweise zur Umsetzung um eines ganzheitlichen Informationssicherheits-Managementsystem (ISMS) in Institutionen (Behörden, Unternehmen und Organisationen)
- Umfasst sowohl das Sicherheitsmanagement als auch konkrete technische, infrastrukturelle, organisatorische und personelle Sicherheitsanforderungen
- Basiert auf einer Risikoanalyse, die das Unternehmen oder die Behörde durchführt, um die relevanten Bedrohungen und Schwachstellen in der IT-Infrastruktur zu ermitteln
- Hauptwerke des IT-Grundschutzes: BSI-Standards, IT-Grundschutz-Kompendium

BSI-Standards

- elementarer Bestandteil des IT-Grundschutzes
- enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit

- Standards:
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - BSI-Standard 200-4: Business Continuity Management (BCM)

IT-Grundschutz-Kompendium

- zentrales Dokument des IT-Grundschutzes des BSI
- bildet die Basis für eine umfassende Informationssicherheitsbetrachtung
- Nachschlagewerk und Werkzeug für die praktische Anwendung des IT-Grundschutzes und der BSI-Standards
- enthält die IT-Grundschutz-Bausteine, die spezifische Sicherheitsanforderungen für verschiedene IT-Bereiche definieren

IT-Grundschutz-Bausteine 1/4

- Die Bausteine im Detail

- Bestandteil des IT-Grundschutz-Kompendium
- Beschreibung typischer Gefährdungen und Sicherheitsanforderungen eines bestimmten Aspekts der Informationssicherheit
- Werden regelmäßig aktualisiert

IT-Grundschutz-Bausteine 2/4

Kern der Beschreibung eines Bausteins bilden die **Sicherheitsanforderungen**

vorrangig zu erfüllende Basis-Anforderungen MUSS-Anforderungen	für eine vollständige Umsetzung des IT-Grundschutzes und eine dem Stand der Technik gemäße Sicherheit zusätzlich zu erfüllende Standard-Anforderungen SOLLTE-Anforderungen	Anforderungen für den erhöhten Schutzbedarf SOLLTE-Anforderungen

IT-Grundschutz-Bausteine 3/4

Bereichsunterteilung

Infrastruktur	Netze und Kommunikation	Industrielle IT	IT-Systeme	Anwendungen
Detektion und Reaktion	Betrieb	Konzeption und Vorgehensweise	Organisation und Personal	Sicherheits-management

IT-Grundschutz-Bausteine 4/4

Beispiele für Bausteine

- Sensibilisierung und Schulung zur Informationssicherheit
- Kryptokonzept
- Cloud-Nutzung
- Office-Produkte
- Etc.

Schutzbedarfskategorien 1/2

- Definiert im IT-Grundschutz-Kompendium des BSI
- Dient der Differenzierung der Anforderungen an die IT-Sicherheit und der Anpassung der Sicherheitsmaßnahmen
- Hilfe zum Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme durch technische Sicherheitsmaßnahmen und infrastrukturelle, organisatorische und personelle Schutzmaßnahmen

Schutzbedarfskategorien 1/2

Normal:	Hoch:	Sehr hoch:
• Geeignet für IT-Systeme mit geringerem Schutzbedarf, bei denen kleinere Fehler toleriert werden können	• Geeignet für IT-Systeme, in denen verarbeitete Informationen definitiv korrekt sein müssen und in denen zeitkritische Vorgänge erfolgen	• Geeignet für IT-Systeme bei denen Informationen im höchsten Maße korrekt sein müssen und ohne die die Aufgaben des Unternehmens nicht mehr durchführbar sind

Schutzbedarfsanalyse nach IT-Grundschutz des BSI 1/2

- Verfahren, mit dem die Schutzziele für IT-Systeme und IT-Anwendungen identifiziert werden
- Durchführung einer Risikoanalyse zur Ermittlung der Bedrohungen und Schwachstellen
- Identifikation geeigneter Maßnahmen zur Risikominimierung

Schutzbedarfsanalyse nach IT-Grundschutz des BSI 2/2

Schutzobjekte

Anwendungen:

- Bewertung von IT-Anwendungen eines Unternehmens hinsichtlich ihrer Schutzziele
- Identifikation von Schwachstellen in der Anwendung
- Identifikation geeigneter Maßnahmen zur Risikominimierung

IT-Systeme

- Identifikation von Bedrohungen für IT-Systeme, um geeignete Schutzmaßnahmen zu ergreifen

Räume

- Bewertung der physischen Sicherheit von Räumen, in denen IT-Systeme aufbewahrt werden
- Mögliche Schwachstellen: unbefugter Zugang, Diebstahl oder Feuer
- Identifikation geeigneter Maßnahmen zur Risikominimierung

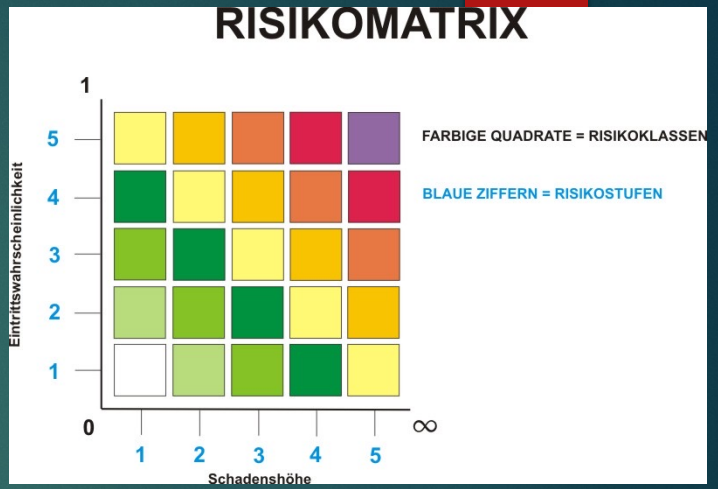
Kommunikationsverbindungen

- Bewertung der Sicherheit von Kommunikationsverbindungen
- Mögliche Bedrohungen: unbefugter Zugang, Datendiebstahl, Manipulation von Daten
- Identifikation geeigneter Maßnahmen zur Risikominimierung

Risikomatrix

- Dient zur Klassifikation von Risiken
- Standardinstrument des Risikomanagements
- Anhand der Risikomatrix kann der Schadenerwartungswert berechnet werden, durch die Multiplikation der Eintrittswahrscheinlichkeit und des Schadensausmaßes des Risikos
- Grundlage für weitere Risikokategorisierungen
- Auf dessen Basis kann eine Unterteilung in weitere Wirkungsklassen stattfinden
- Außerdem verwendet für die Risikoberichterstattung

Quelle



Im Arbeitsschutz wird gewöhnlich die Risikomatrix nach Nohl/Thiemecke verwendet

Risikomatrix nach Nohl

Schadensschwere / Wahrscheinlichkeit	leichte Verletzung oder Erkrankung	mittelschwere Verletzung oder Erkrankung	schwere Verletzung oder Erkrankung	möglicher Tod, Katastrophe
sehr gering	1	2	3	4
gering	2	3	4	5
mittel	3	4	5	6
hoch	4	5	6	7

04 ISMS

- IT-Sicherheitsmanagement
- ISMS
- ISMS implementieren
- Wichtige Prozesse

IT-Sicherheitsmanagement

- fortlaufenden Prozess innerhalb eines Unternehmens oder Organisation zur Gewährleistung der IT-Sicherheit

Aufgaben

- Systematische Absicherung eines informationsverarbeitenden IT-Verbundes
- Abwehr/Verhinderung von Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes eines Unternehmens oder einer Organisation
- Auswahl und Umsetzung technischer, infrastruktureller, organisatorischer und personeller Schutzmaßnahmen, die auf die spezifischen Anforderungen des Unternehmens abgestimmt sind.
- ISO 27001: umfasst zentrale Komponenten wie Risikobewertung und -behandlung, Sicherheitsverfahren, Zugriffskontrollen sowie kontinuierliche Verbesserung

ISMS

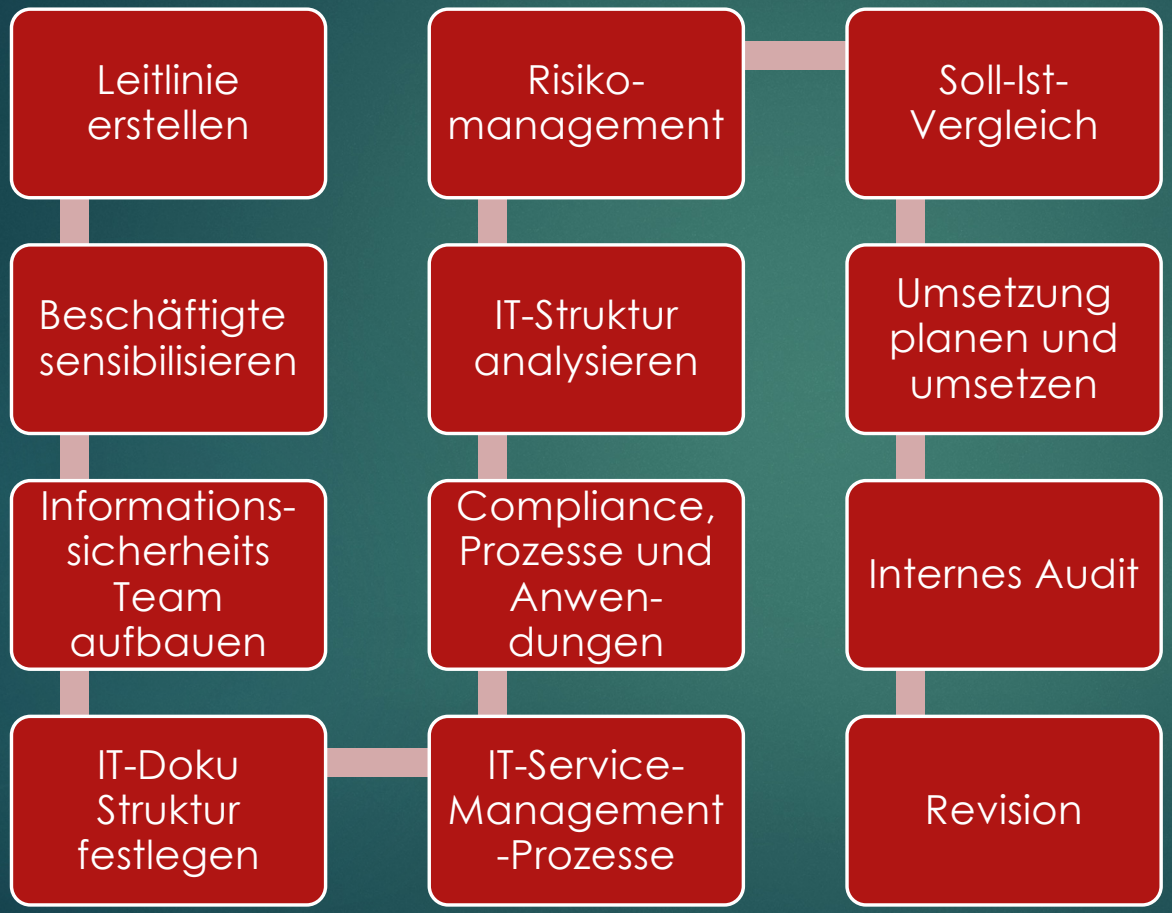
Information Security Management System

- Hilft dabei, ein unternehmensweites Sicherheitskonzept zu etablieren, das potenzielle Sicherheitsrisiken reduziert und effektiv gegen Hackerangriffe sowie Manipulationen schützt

Aufgaben:

- Identifikation von Risiken, Risikobewertung und Risikomanagement
- Erstellung von Informationssicherheitsrichtlinien:
- Festlegung von Verantwortlichkeiten und Zuständigkeiten für die Umsetzung
- Regelmäßige Überprüfung, Aktualisierung und Kommunikation der Richtlinien

ISMS in 12 Schritten



Schritte werden kontinuierlich, gemäß eines PDCA-Zyklus durchlaufen

Wichtige Prozesse 1/2

Risikomanagementprozess - Kernprozess des ISMS

- Identifizierung, Bewertung und Behandlung von Risiken im Zusammenhang mit der Informationssicherheit
- potenzielle Bedrohungen und Schwachstellen erkennen und entsprechende Gegenmaßnahmen ergreifen

Incident-Managementprozess

- Meldung, Analyse und Behebung von Sicherheitsvorfällen
- schnell und effektiv auf Bedrohungen oder Angriffe reagieren, um Schäden zu minimieren

Change-Managementprozess

- Umsetzung von Änderungen an IT-Systemen oder Prozessen, um sicherzustellen, dass diese Änderungen keine negativen Auswirkungen auf die Informationssicherheit haben

Wichtige Prozesse 2/2

Kontinuierlicher Verbesserungsprozess

- ständige Überprüfung und Verbesserung der ISMS-Prozesse, um sicherzustellen, dass sie den sich ändernden Anforderungen und Bedrohungen gerecht werden

Schulungs- und Sensibilisierungsprozess

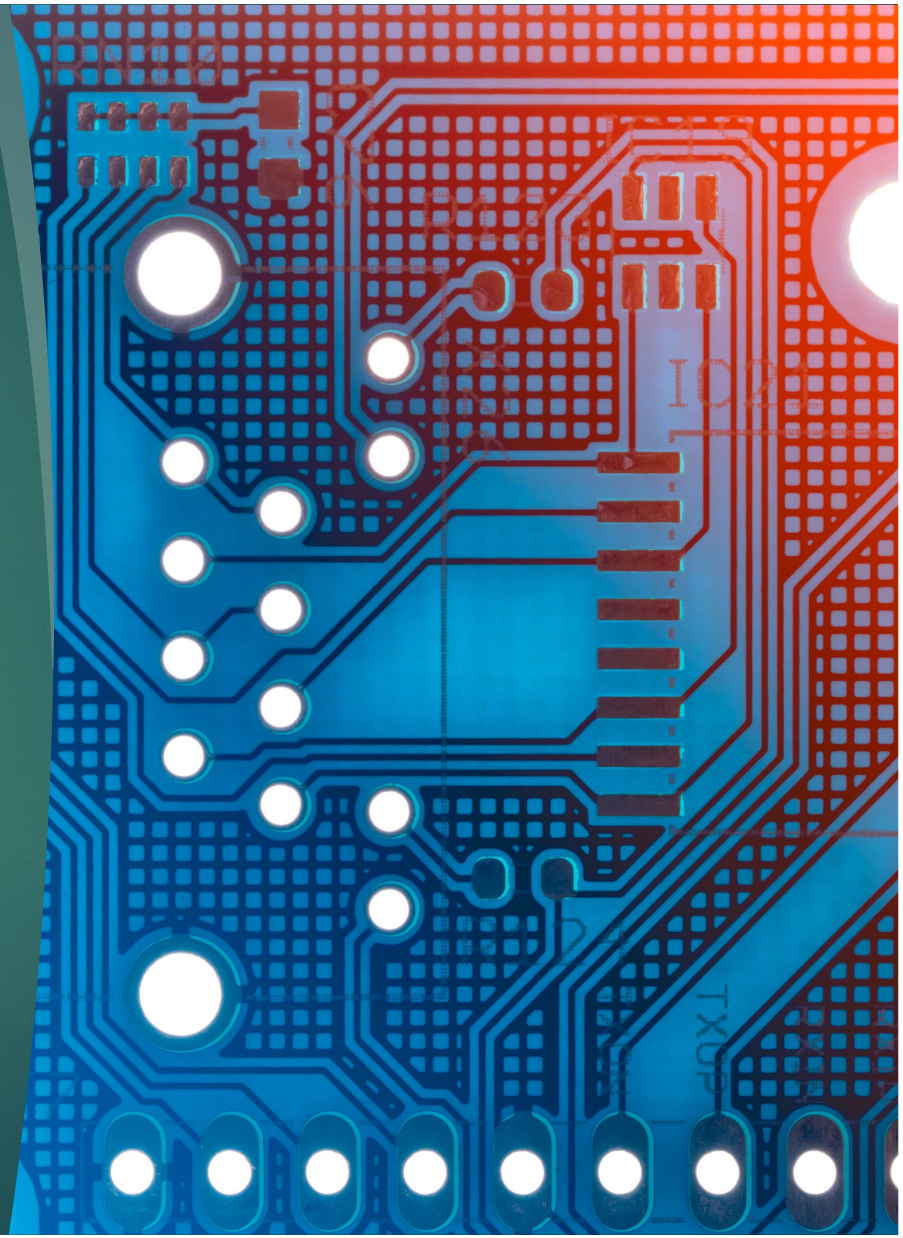
- Schulungen und Awareness-Kampagnen
- Sicherheitsbewusstsein und -wissen der Mitarbeiter verbessern

Überwachungs- und Messprozess

- Überwachung der Umsetzung der ISMS-Prozesse
- Messung und Bewertung der Wirksamkeit der implementierten Sicherheitsmaßnahmen

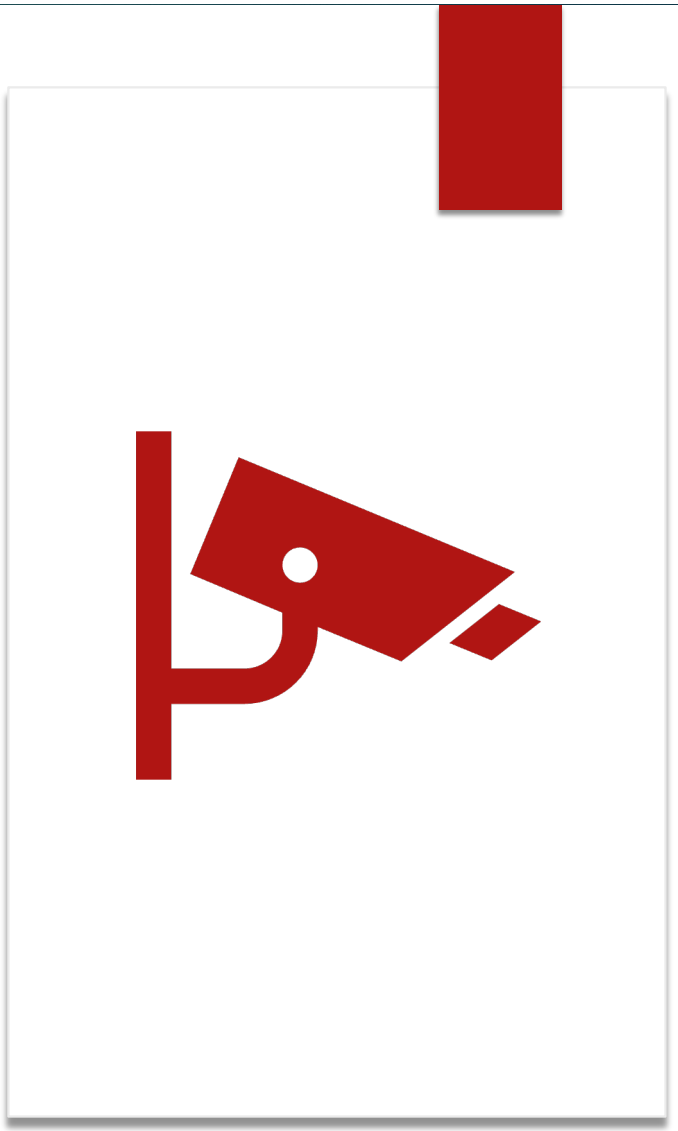
05 Härtung von Betriebssystemen

- Begriffsklärung
- Ziele
- Wann gilt ein Betriebssystem als gehärtet?
- Methoden
- Usermanagement



Begriffsklärung

- National Institute of Standards and Technology (NIST) definiert Härten in der IT-Sicherheit wie folgt:
  - „Ein Prozess, der dazu dient, eine Angriffsmöglichkeit zu eliminieren, indem Schwachstellen gepatcht und nicht benötigte Dienste abgeschaltet werden.“



Ziele


Reduktion der Möglichkeiten zur Ausnutzung von Verwundbarkeiten
Minimierung der möglichen Angriffsmethoden
Beschränkung der einem Angreifer nach einem erfolgreichen Angriff zur Verfügung stehenden Werkzeuge und Privilegien
Erhöhung der Wahrscheinlichkeit der Entdeckung eines erfolgreichen Angriffs

Wann gilt ein BS als gehärtet?

- nur die Komponenten und Dienste sind installiert, die zum eigentlichen Betrieb benötigt werden
- alle nicht benötigten Benutzerkonten sind gelöscht
- alle nicht benötigten Ports sind geschlossen
- restriktive Rechte sind gesetzt
- straffe Systemrichtlinien sind vergeben

Methoden

- Unnötige Dienste und Softwarekomponenten entfernen oder deaktivieren
- Benutzerberechtigungen und Gruppenrichtlinien einrichten
- Dateisystem- und Registry-Berechtigungen konfigurieren
- Authentifizierungsmechanismen nutzen (PW-Policy, 2FA)
- Verschlüsselung nutzen (Datenübertragung, Festplatte)
- Möglichst fehlerfreier Software ohne bekannte Verwundbarkeiten verwenden
- Automatische Updates und Patches aktivieren
- Alle Aktivitäten, Fehler und Warnungen protokollieren

Begriffsklärung: Usermanagement

- Verwaltung von Benutzerkonten, Zugriffsrechten und Rollen in IT-Systemen, Netzwerken, Anwendungen und Datenbanken

Aufgabe	Beschreibung
Benutzerkonten anlegen	Benutzer erhalten eindeutige Identität (z. B. Loginname)
Passwörter verwalten	Regeln für Passwortlänge, Ablauf, Änderung, Reset-Prozesse
Zugriffsrechte vergeben	Wer darf auf welche Ressourcen zugreifen?
Rollen zuweisen	Nutzer werden in Gruppen oder Rollen organisiert
Konten sperren/löschen	Bei Austritt, Sicherheitsvorfällen oder inaktiven Accounts
Protokollierung	Überwachung von Anmeldeversuchen, Zugriffen, Änderungen

06 Backup-Verfahren

- Gründe für Datenverluste
- Folgen von Datenverlust
- Maßnahmen gegen Datenverluste
- Sicherungswürdige Daten
- Inkrementelles, differenzielles, Vollbackup
- Generationenprinzip
- Backup Medien
- Hot vs. Cold
- NAS – SAN - DAS

Gründe für Datenverluste auf Servern

- Hardware- und Softwareausfälle
- menschliche Fehler, wie das versehentliche Löschen von Daten
- Cyberangriffe und Malware-Infektionen
- Naturkatastrophen, wie Überschwemmungen, Brände oder Erdbeben

Folgen von Datenverlust

- Verlust von Kundenvertrauen, was zu einem Rückgang der Kunden führen kann
- Reputationsschäden, die das Image und den Ruf des Unternehmens beeinträchtigen können
- Verlust von Geschäftsgeheimnissen und wertvollen Daten, was zu einem Wettbewerbsnachteil führen kann
- finanzielle Verluste, z.B. durch den Verlust von Verträgen, Kunden oder wertvollen Daten

Maßnahmen gegen Datenverluste 1/3

- regelmäßige Backups wichtiger Daten
- Redundanz in Hardware (z. B. RAID-Systeme, Cluster-Konfigurationen)
- Überwachung von Servern und Netzwerken, um Probleme frühzeitig zu erkennen
- Schulung von Mitarbeitern in IT-Sicherheitsmaßnahmen und die Sensibilisierung für das Thema Datenverlust und dessen Auswirkungen

Maßnahmen gegen Datenverluste 2/3

Auf Seiten der Mitarbeitenden

- Vermeiden von öffentlichen WLAN-Netzwerken und das Arbeiten auf öffentlichen Computern
- Nicht-Weitergabe von vertraulichen Informationen an unbefugte Personen
- Nicht-Öffnen verdächtiger E-Mails oder Links
- Regelmäßige Installation von Updates und Patches für Software und Systeme

Maßnahmen gegen Datenverluste 3/3

Regelmäßige Backups wichtiger Daten

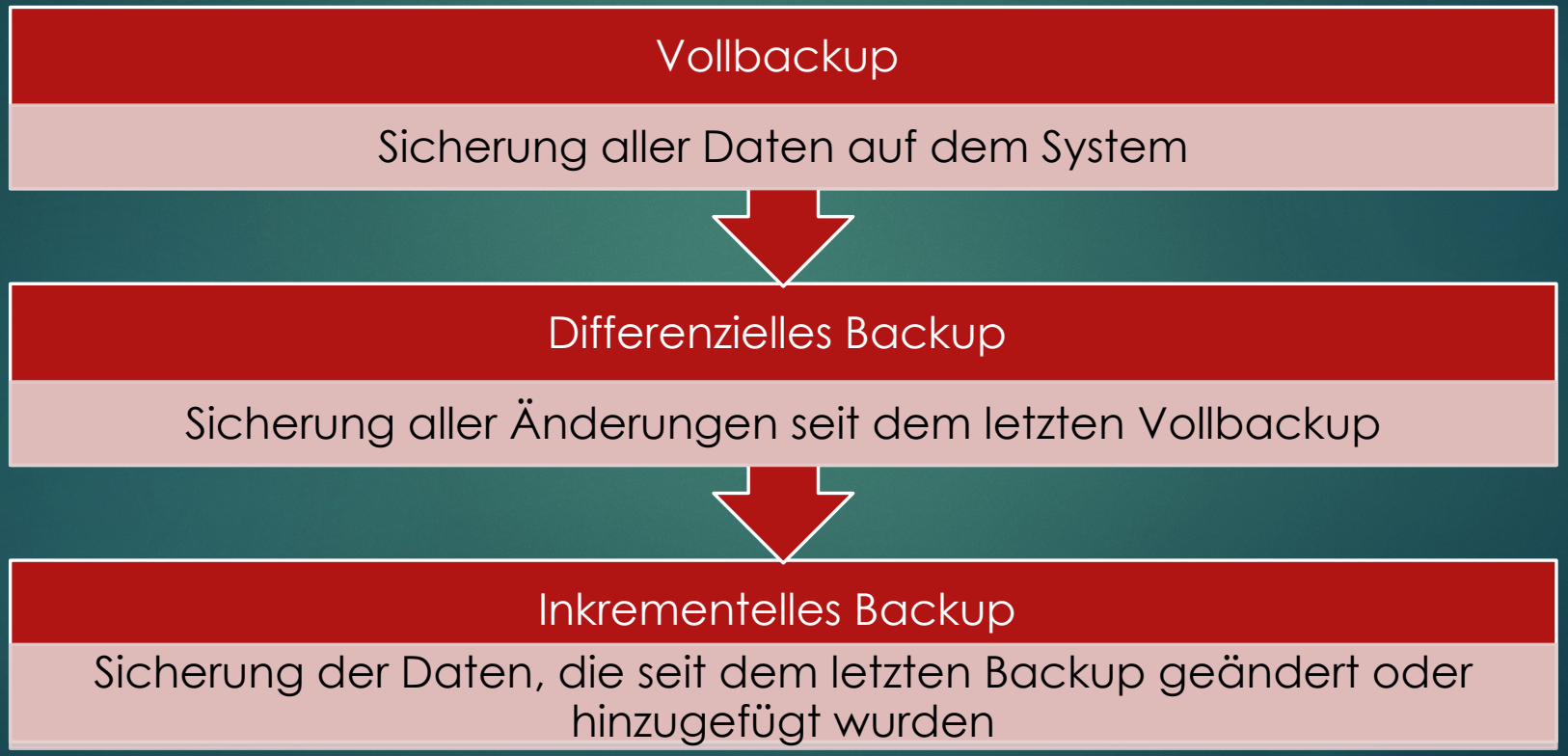
- Wie erkennt die Software, welche Daten zu sichern sind?
  - Einsatz eines Backup-Jobs, der festlegt, welche Dateien und Ordner gesichert werden sollen
  - Filtern oder Regeln helfen bestimmte Dateitypen oder Dateinamen zu erkennen

Was sind sicherungswürdige Daten?

- Daten, die für ein Unternehmen von hohem Wert und kritischer Bedeutung sind.

Kundendaten	Finanzdaten	Unternehmens-geheimnisse
E-Mail-Korrespondenz	Verträge	interne Dokumente

Inkrementelles, differenzielles und Vollbackup



Generationenprinzip bzw. Großvater/Vater/Sohn

- Backup-Strategie, bei der mehrere Generationen von Backups aufbewahrt werden
- Kombination von täglichen, wöchentlichen und monatlichen Back-ups
- Geringere Wahrscheinlichkeit von Datenverlusten aufgrund von Problemen bei einem bestimmten Backup

Backup Medien 1/2

Auswahl ist abhängig von verschiedenen Faktoren:

- Intervall
- Datenvolumen
- Vorhaltezeit
- Verfügbare Zeit der Datensicherung
- Kosten

Backup Medien 2/2

	Zugriffs-zeiten	Störanfälligkeit	Kosten	Speicher-kapazität	Lebens-dauer
Cloud	mittel	Cyberangriff, Internetverbindung notwendig	hoch	Theoretisch unbegrenzt	Theoretisch unbegrenzt
Blue-Ray	hoch	Kratzer und UV-Strahlung	niedrig	In der Theorie bis zu 500 GB	50 – 100 Jahre
SSD	gering	Stöße (deutlich geringer als HDD) und Hitze	mittel	bis zu 5 TB	10 Jahre
HDD	gering	Stöße und Feuchtigkeit	mittel	bis zu 15 TB	10 Jahre
Magnet-band	hoch	Magnetismus und physische Schäden	niedrig	bis zu 6 TB	10 - 30 Jahre

Hot vs. Cold

Hot Backup

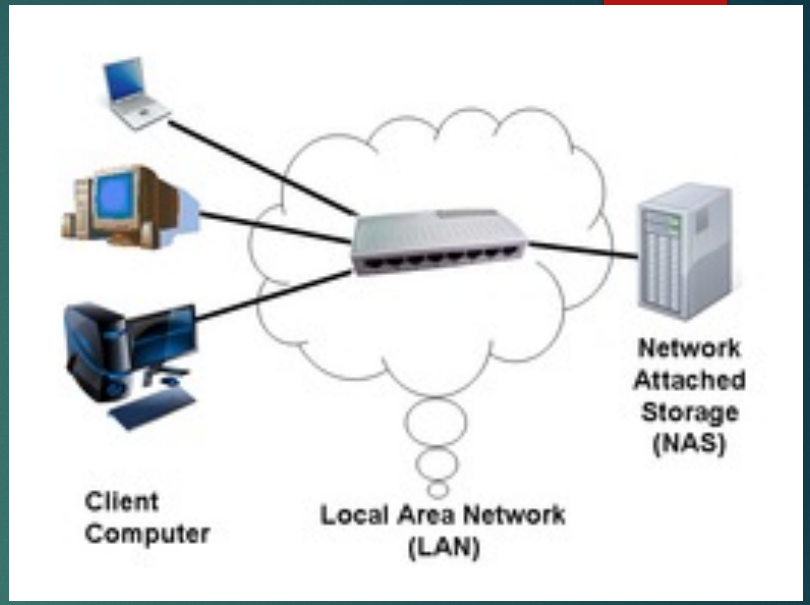
- Methode, bei der das System während des Backup-Vorgangs weiterläuft

Cold Backup

- System wird heruntergefahren, bevor das Backup durchgeführt wird

NAS

- einfach zu verwaltender Dateiserver
- Bereitstellung einer unabhängigen Speicherkapazität in einem Rechnernetz ohne hohem Aufwand
- Steht netzweit zur Verfügung
- Vorteile
  - Deutlich geringerer Stromverbrauch im Vergleich zu herkömmlichen PC-Systemen
  - Bewältigung großer Datenmengen
  - Gleichzeitiger Zugriff mehrerer Benutzer

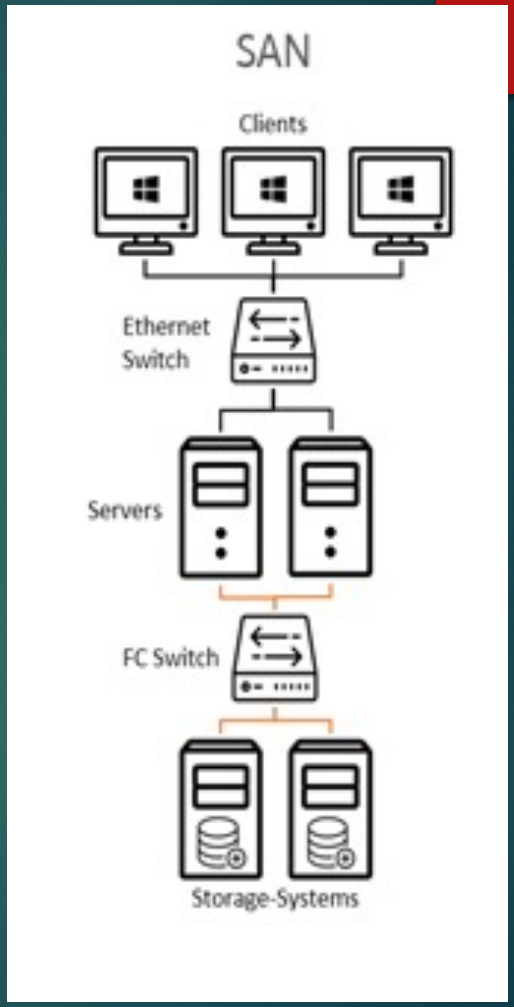


Quelle

SAN

Storage Area Network

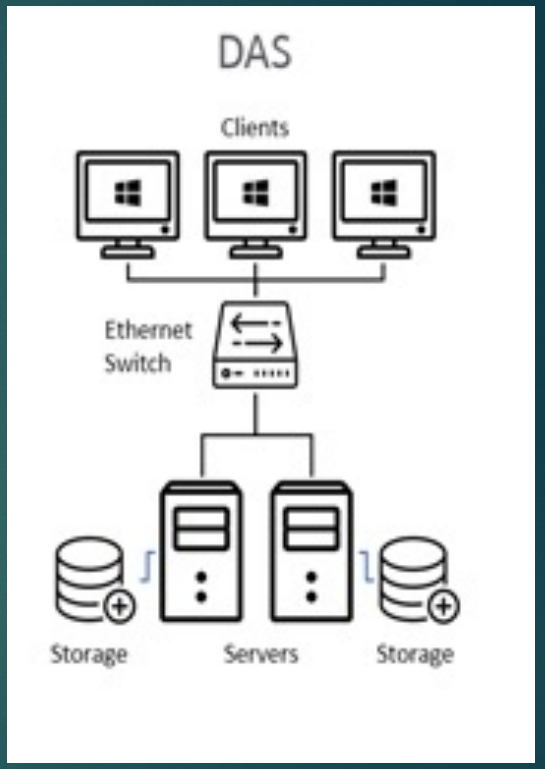
- spezialisiertes Speichernetzwerk, das blockbasierten Zugriff auf Speicher über ein dediziertes Netzwerk ermöglicht
- Server sehen den Speicher so, als wären es lokale Festplatten – trotz physischer Trennung
- Vorteile
  - Extrem leistungsfähig und ausfallsicher
  - Ideal für Datenbanken, VMs, Clusterlösungen
  - Sehr hohe Skalierbarkeit und Kontrolle



DAS

Direct Attached Storage

- Speichergeräte, die direkt an einen Computer oder Server angeschlossen sind – ohne Netzwerkverbindung
- einfachste Form von Speicher
- Vorteile
  - Günstig und leicht einsetzbar
  - Keine Netzwerkkonfiguration nötig
  - Sehr hohe Geschwindigkeit bei Direktanschluss



07 Kryptografie

- Zugangs- und Zugriffskontrolle
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Hashverfahren
- Blockchain
- Authentifizierung vs. Autorisierung
- Passwörter
- Zertifikate, Digitale Signaturen
- CA
- TPM
- Bitlocker

Zugangs- und Zugriffskontrolle

Zutrittskontrolle

- Kontrolle des physischen Zuganges zu beispielsweise einem bestimmten Raum, Gebäude oder Gelände, in denen die Datenverarbeitung stattfindet bzw. Akten, Computer oder Server stehen

Zugangskontrolle

- Festlegung, welcher Nutzer Zugang zu einem IT-System, Laufwerk, Dateiordner etc. erhält

Zugriffskontrolle

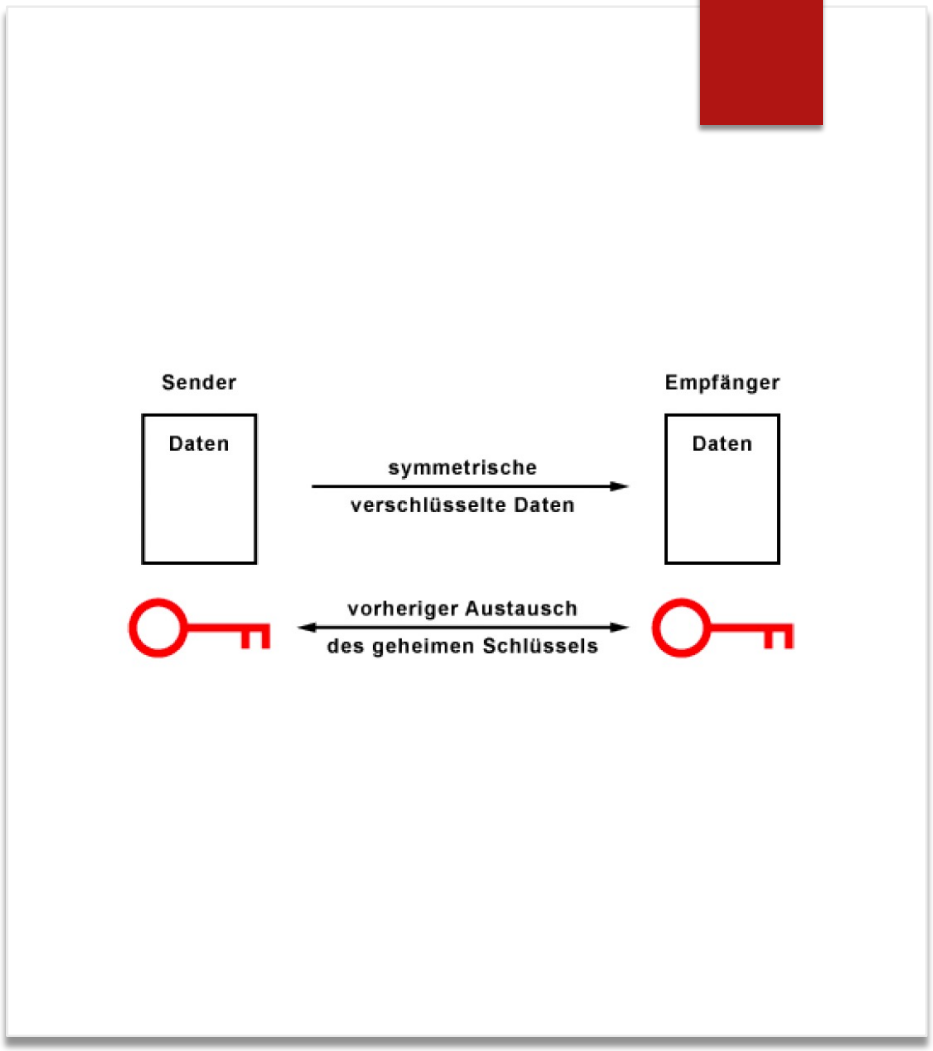
- Kontrolle dessen, welcher Nutzer bestimmte Daten verarbeiten darf
- Dazu gehört:
  - Erhebung, eigentliche Verarbeitung, Speicherung, Übermittlung, Einblick gewähren, Veränderung, Löschen bzw. Vernichten

Zugangskontrollen

- **Mechanische Zutrittskontrollen**
  - Schlüssel
- **Elektronische Zugangssysteme**
  - PIN-Code, RFID, Magnetleser, Bluetooth-Leser, Biometrische Sensoren
- **Verhaltensbasierte/Adaptive Systeme (High-End)**
  - Analyse von Nutzerverhalten wie z. B. ungewöhnliche Zeiten, doppelte Zugänge etc.

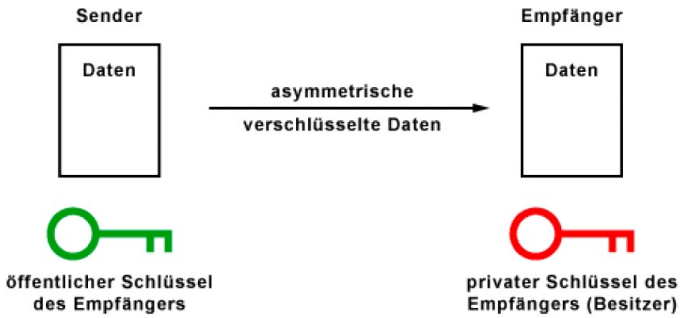
Symmetrische Verschlüsselung

- Verwendung von ein und desselben Schlüssels zum Verschlüsseln und zum Entschlüsseln der Daten
- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)



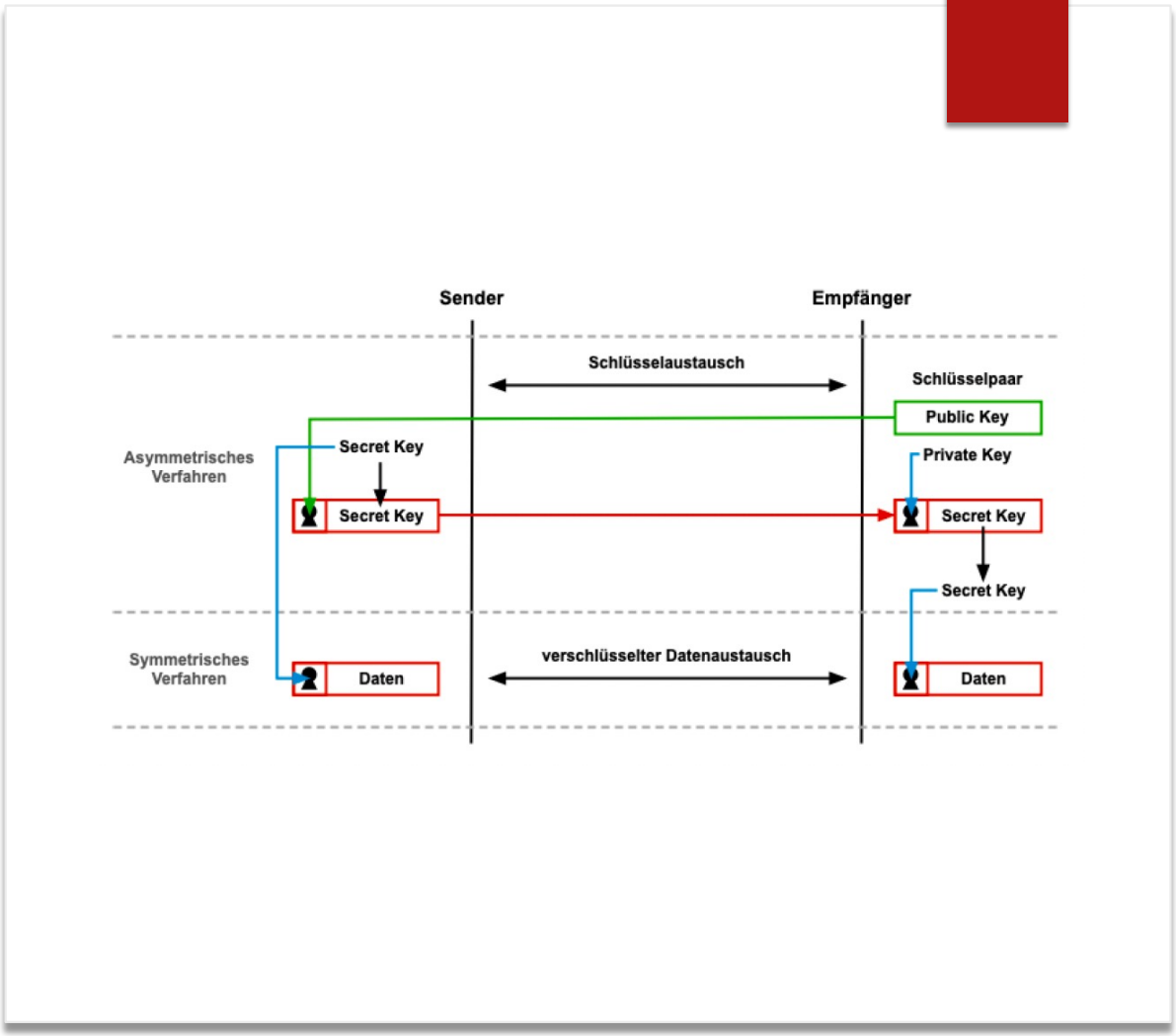
Asymmetrische Verschlüsselung

- Verwendung von zwei unterschiedlichen Schlüsseln
- Öffentlicher Schlüssel zum Verschlüsseln
- Privater Schlüssel zum Entschlüsseln
- RSA (Rivest-Shamir-Adleman)



Hybride Verschlüsselung

- Verschlüsselung der Daten mit dem symmetrischen Verfahren
- Das asymmetrische Verfahren wird nur für den Sitzungsschlüssel verwendet
- Einsatz in Netzwerkprotokollen z. B. bei E-Mail-Verschlüsselung



Hashverfahren

- Mathematische Einwegfunktionen
- Berechnung einer Prüfsumme oder eines Hashs aus einer großen Menge von Daten
- Dient der Überprüfung der Integrität
- SHA (Secure Hash Algorithm)
- MD (Message Digest)

Blockchain

- dezentrale digitale Datenbank bzw. verteiltes Register, das Transaktionen sicher, transparent und fälschungssicher in einem Netzwerk von Computern speichert

Blöcke mit Daten

- Informationen in einzelnen Blöcken gesammelt

Chronologische Kette

- durch Verknüpfung neuer Blöcke mit dem jeweils vorherigen Block

Kryptografische Verschlüsselung

- ermöglichen fälschungssichere Verknüpfung der Blöcke

Dezentrales Netzwerk

Konsensmechanismus

- **Einigung a**ller Computer im Netzwerk auf den Inhalt neuer Blöcke

Unveränderlichkeit

- keine nachträgliche Veränderungen möglich

Authentifizierung vs. Autorisierung

Authentifizierung:

- Prozess der Überprüfung der Identität eines Benutzers, bevor er Zugang zu einem System oder einer Anwendung erhält

Autorisierung:

- Prozess der Bestimmung, welche Aktionen ein authentifizierter Benutzer ausführen darf
- Gesteuert durch eine Kombination aus Rollen, Gruppen und individuellen Benutzerrechten

Passwörter 1/2

Zwei-Authentifizierung (2FA)

- Konzept, bei dem ein Benutzer zwei Authentifizierungsmethoden verwenden muss, um sich bei einem System anzumelden
- Z. B.:
  - Passwort + Einmalcode
  - Passwort + biometrische Authentifizierung

Passwort-Policy

- Sammlung von Regeln, die festlegen, welche Arten von Passwörtern Benutzer verwenden dürfen
- Z. B.:
  - Passwörter benötigen mindestens eine bestimmte Länge
  - Passwörter enthalten bestimmte Arten von Zeichen
  - Passwörter müssen in regelmäßigen Abständen geändert werden

Passwörter 2/2

OAuth2 (Open Authorization 2.0)

- Protokoll für zugriffsbasierte Autorisierung, bei dem eine Anwendung im Namen eines Benutzers Zugriff auf Ressourcen bei einem anderen Dienst erhält
- ohne das Passwort des Benutzers zu kennen oder zu speichern
- Einsatzgebiete
  - APIs
  - Cloud-Zugriffe

Single Sign-On (SSO)

- Verfahren, bei dem sich ein Benutzer nur einmal authentifizieren muss, um anschließend auf mehrere Systeme oder Anwendungen zugreifen zu können, ohne sich erneut anzumelden
- Einsatzgebiete:
  - MS 365
  - Active Directory
  - Campus-SSO

Zertifikate und Digitale Signaturen

Zertifikat

- Digitales Dokument, das die Identität einer Person, eines Unternehmens oder einer Organisation bestätigt
- Ausgestellt durch Zertifizierungsstellen (CAs)
- Enthalten Informationen wie den Namen des Inhabers, die Gültigkeitsdauer des Zertifikats und den öffentlichen Schlüssel des Inhabers

Digitale Signaturen

- Gewährleistung der Integrität von Daten
- Sicherzustellen, dass sie von einer vertrauenswürdigen Quelle stammen

Certificate Authority (CA)

- vertrauenswürdiger Dritter, der digitale Zertifikate ausstellt, um die Identität von Personen, Servern oder Organisationen zu bestätigen
- „digitaler Notar“ des Internets:
  - beglaubigt, dass ein öffentlicher Schlüssel wirklich zu dem angegebenen Inhaber gehört
- Ein digitales Zertifikat enthält u. a.:
  - Den öffentlichen Schlüssel
  - Den Namen / die Domain des Zertifikatsinhabers
  - Die gültige Zeitspanne
  - Die digitale Signatur der CA

Name	Besonderheiten
Let's Encrypt	Kostenlos, automatisiert, sehr verbreitet
DigiCert	Kommerziell, hoher Vertrauenslevel
GlobalSign	Große internationale CA
Sectigo (ehem. Comodo)	Häufig in Hostingpaketen enthalten

TPM

Trusted Platform Module

- Hardware-Chip auf dem Mainboard, der kryptografische Funktionen bietet und sensible Schlüssel sicher speichert – isoliert vom Betriebssystem
- **Funktionen**:
  - Absicherung von Bootvorgängen (Secure Boot)
  - Unterstützung von Plattenschutzsystemen wie BitLocker
  - Manipulationsschutz durch Trusted Computing
- **Vorteile**:
  - Schlüssel sind nicht auslesbar, selbst bei physischem Zugriff
  - Hardware-gebunden → Schutz gegen Kopieren/Clonen von Datenträgern
  - Ermöglicht transparentes Entsperren ohne Passworteingabe (z. B. bei Windows-Start)

Bitlocker

- Tool zur vollständigen Laufwerksverschlüsselung
- integriert in Windows ab Pro/Enterprise-Versionen

- **Vorteile**:
  - Nahtlose Integration in Windows
  - Kompatibel mit TPM für hohen Schutz
  - Automatisierte Verwaltung in Unternehmensnetzwerken
  - Transparente Verschlüsselung im Hintergrund

08 WLAN Sicherheit

- Begriffe
- Aktuelle Verschlüsselungen
- WPA2/3-PSK und WPA2/3-EAP
- RASIUS versus Kerberos

Begriffe

SSID (Service Set Identifier):	Mac-Filter:	WPS (Wi-Fi Protected Setup):	Wi-Fi Easy Connect:
• Name des WLAN-Netzwerks, Standardbezeichnungen sollten zum Schutz vor Hackern geändert werden	• Ausschluss bestimmter MAC-Adressen vom WLAN-Netzwerk	• Standard zum einfachen Aufbau eines drahtlosen lokalen Netzwerkes mit Verschlüsselung • Anfällig für Brute-Force-Angriffen, sollte deshalb deaktiviert werden	• Neuerer Standard als von WPS • Geräte können per QR-Code, NFC-Tags oder PINS eine einfache Verbindung ins WLAN herstellen

Aktuelle Verschlüsselungen

WPA2 - Wi-Fi Protected Access Version 2

- Weiterentwicklung von WPA
- Unterscheidet zwischen WPA2-Personal (WPA2-PSK) und WPA2-Enterprise (WPA2-EAP) zur Authentisierung
- Für Geräte, die WPA3 nicht unterstützen

WPA3 - Wi-Fi Protected Access Version 2

- Derzeit aktuell sicherster Verschlüsselungsstandard
- Seit 2020 verlangt die Wi-Fi Alliance für eine Zertifizierung von Geräten die WPA3-Unterstützung

WPA2/3-PSK und WPA2/3-EAP

WPA2/3-Personal (WPA2/3-PSK)

- Verwendet wird ein gemeinsames WLAN-Passwort (Pre-Shared Key)
- Für Heimnetzwerke geeignet

WPA2/3-Enterprise (WPA2/3-EAP)

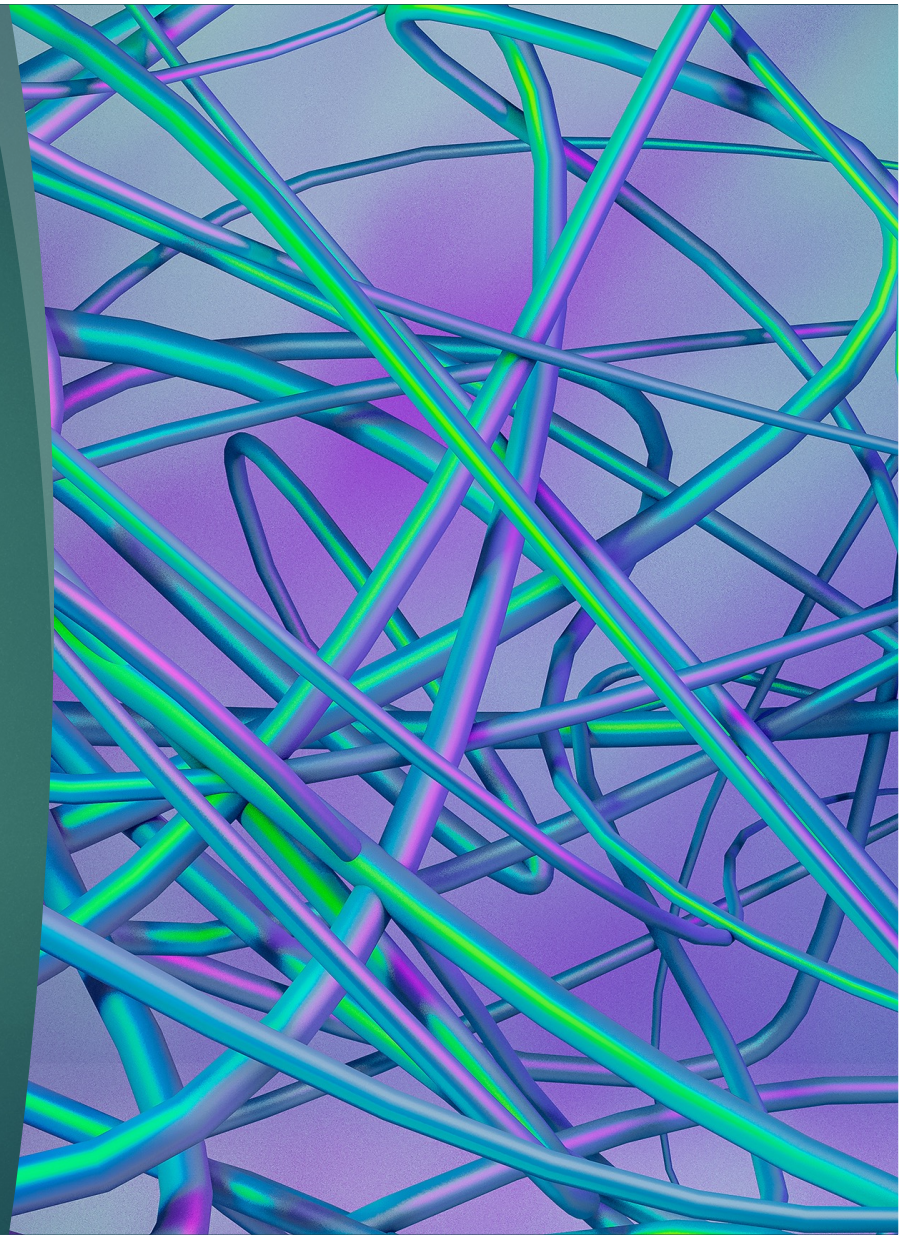
- Benötigt einen eigenen Authentifizierungsserver (RADIUS-Server)
- Jeder Benutzer hat einen eigenen Benutzernamen und Passwort
- Ermöglicht zentrale Verwaltung der WLAN-Zugriffe
- Für Unternehmen empfohlen

RADIUS versus Kerberos

Merkmal	RADIUS	Kerberos
Typ	Netzwerkprotokoll	Authentifizierungsprotokoll
Beschreibung	• Verwaltung der Authentifizierung, Autorisierung und Abrechnung (AAA) von Remotebenutzern, die über DFÜ-, VPN- oder drahtlose Verbindungen auf ein Netzwerk zugreifen • RADIUS-Server prüft die Anmeldeinformationen des Benutzers und weist Richtlinien und Parameter zu	• Überprüfung der Identität von Benutzern und Diensten in einem Netzwerk • Verwendung von Tickets (verschlüsselte Token), die die Identität des Benutzers, die Identität des Dienstes und einen Sitzungsschlüssel enthalten • Tickets vom Key Distribution Center (KDC) ausgestellt • KDC besteht aus: Authentifizierungsserver (AS), Ticket Granting Server (TGS).
Einsatzgebiet	VPN, WLAN, 802.1X	Active Directory, Fileserver
Sicherheit	• Gut (mit TLS/SSL) • Verschlüsselt nur PW, nicht das gesamte Datenpaket • Anfällig für Abfangen und Ändern	• Sehr hoch • Bietet gegenseitige Authentifizierung und SSO-Funktionalität

09 VPN

- Begriffsklärung
- Funktionsweise
- VPN-Arten
- Begriffsklärung: Tunneling
- Tunneling-Protokolle



Begriffsklärung

Virtual Private Network

- Herstellen einer verschlüsselten Verbindung zwischen Client und einem entfernten Server
- Internetverkehr wird vor Dritten geschützt

Funktionsweise

- Verschlüsselte Verbindung zu einem VPN-Server aufbauen
- Übertragung aller gesendeten und empfangenen Daten werden durch starke Verschlüsselung gesichert
- Verbindung wird über eine andere IP-Adresse vom VPN-Server geleitet und verbirgt so die tatsächliche Client-IP-Adresse

Arten 1/3

- End-to-Site-VPN
  - Unternehmen setzen VPNs ein, um Mitarbeitern einen sicheren Fernzugriff auf Firmendaten zu ermöglichen
  - Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her

Arten 1/3

- Site-to-Site-VPN
  - Mehrere lokale Netzwerke von Außenstellen oder Niederlassungen (Filialen) werden zu einem virtuellen Netzwerk über ein öffentliches Netz zusammengeschaltet

Arten 1/3

- End-to-End-VPN
  - Ein Client greift auf einen anderen Client in einem entfernten Netzwerk zugreift
  - Der VPN-Tunnel deckt die gesamte Verbindung zwischen zwei Hosts ab

Begriffsklärung: Tunneling

- Verfahren, bei dem ein Protokoll in ein VPN-Protokoll (z. B. L2TP) **verkapselt** wird, um Daten durch einen **sicheren, logischen Kanal (Tunnel)** über ein unsicheres Netzwerk – meist das Internet –zu übertragen
- Ziel:
  - **Schutz** der übertragenen Daten (Vertraulichkeit)
  - **Virtuelle Verbindung** über ein öffentliches Netz
  - **Transport von Protokollen**, die sonst nicht über das Internet gehen (z. B. NetBIOS, IPX)

Merkmal	Erklärung
Kapselung	Datenpakete werden verschachtelt übertragen
Transparenz	Nutzer bemerkt die Tunnelung nicht – funktioniert wie LAN
Sicherheit	Bei VPN fast immer mit Verschlüsselung kombiniert
Kompatibilität	Auch alte oder inkompatible Protokolle können transportiert werden

Tunneling-Protokolle

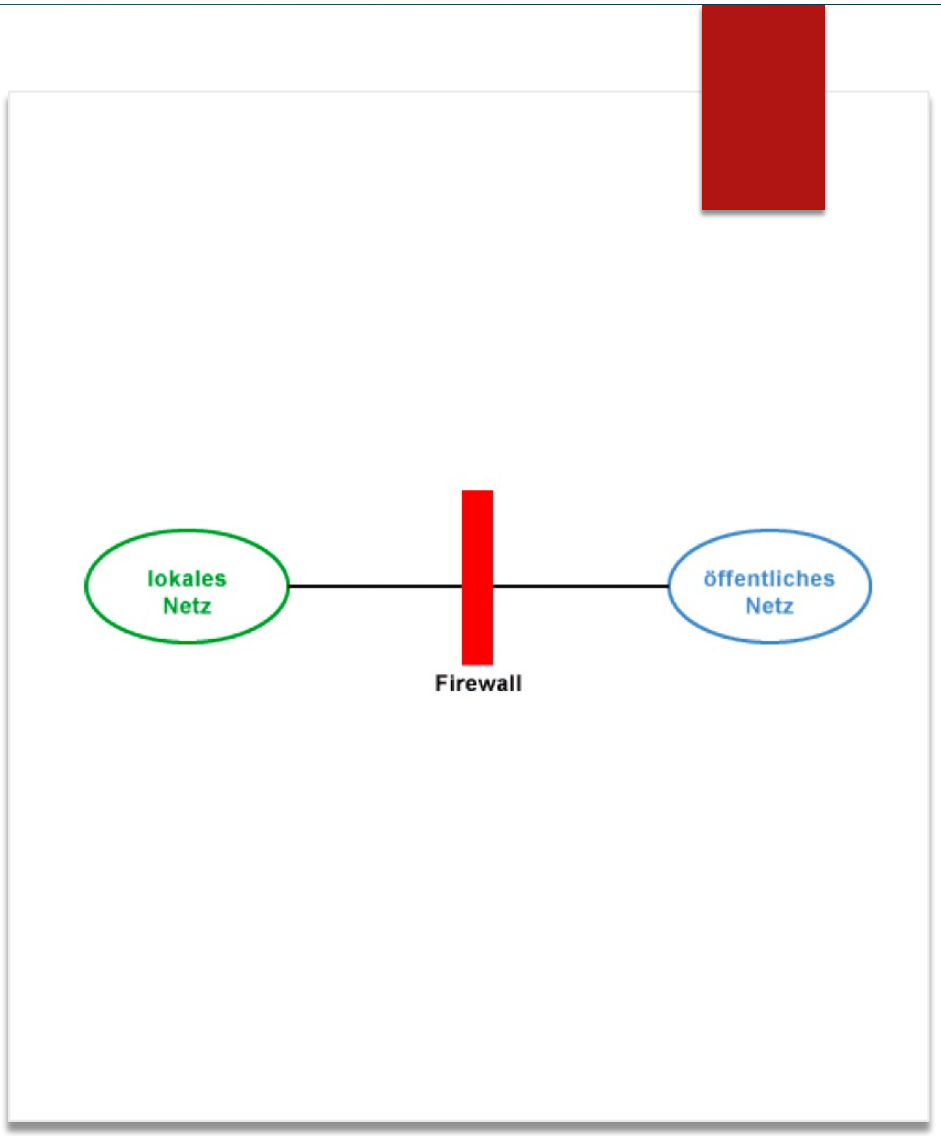
Protokoll	Sicherheit & Authentifizierung	Transport	Aktuelle Verbreitung / Support	Vorteile	Nachteile
OpenVPN	Sehr sicher: AES-256, TLS/SSL, PFS, Open Source	UDP oder TCP	Sehr weit verbreitet, plattformübergreifend	• Sehr flexibel (Portwahl, NAT) • OpenSource • hohe Sicherheit	• Etwas langsamer • komplexere Konfiguration
WireGuard	Modern, kryptogestützt (ChaCha20, Curve25519, BLAKE2s)	Nur UDP	Zunehmende Unterstützung	• Extrem schnell • schlanker Code • gute Mobile-Performance • OpenSource	• Noch weniger verbreitet • kein TCP-Support • potenzieller IP-Log
IKEv2/IPsec	Sehr sicher: IPsec mit Certs oder PSK, PFS	UDP (Ports 500 & 4500)	Gute nativen Unterstützung; empfohlen für mobile Nutzung	• Schnell, stabil bei Netzwerkwechseln • einfach einzurichten	• Weniger flexibel • schwieriger durch Firewalls/NAT
L2TP/IPsec	Tunnel ohne Ende-zu-Ende-Schutz, IPsec liefert Verschlüsselung	UDP 1701 + IPsec Ports	Alte Technologie, nur noch selten empfohlen	• Einfache Einrichtung • standardmäßig in OS	• Langsamer (Doppeltunneling) • Probleme hinter restriktiven Netzwerken
PPTP	Sehr unsicher: MPPE verschlüsselung, CHAP-Auth zerbrechlich	TCP + GRE	Obsolet, kaum noch genutzt	• Extrem einfach eingerichtet	• Veraltet • leicht angreifbar
SSTP	SSL/TLS-basierter Tunnel, PPP-Auth (MS-CHAPv2 etc.)	TCP 443	Nur Microsoft/Windows-Ökosystem stark unterstützt	• Funktioniert durch fast alle Firewalls (HTTPS-Port)	• Leistungseinbuße durch TCP-over-TC • Proprietär • weniger auditierbar

10 Firewall

- Begriffsklärung
- Sicherheitsstrategien
- Elemente einer Firewall
- Arten und Funktionsweise
- Proxy

Begriffsklärung

- Netzwerksicherheitsvorrichtung, die eingehenden und ausgehenden Netzwerkverkehr überwacht
- Entscheidet auf Grundlage einer Reihe von definierten Sicherheitsregeln, ob bestimmter Datenverkehr zugelassen oder blockiert wird
- Meist Teil eines Routers oder als externe Komponente einem Router vor- oder nachgeschaltet
- Firewall kann ein einzelner Computer oder eine Kombination aus Proxy und einem Router sein



Sicherheitsstrategien

Alles sperren

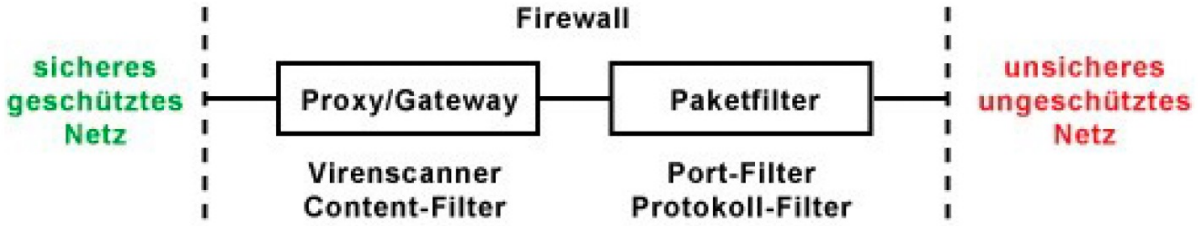
- Alles ist gesperrt
- Bekannte sichere und erwünschte Vorgänge werden freigegeben
- + Sehr sicher
- - Aufwendige Konfiguration erforderlich

Alles freigeben

- Alles ist freigegeben
- Bekannte unsichere und unerwünschte Vorgänge werden gesperrt
- + Komfortabel
- - Nur so sicher, wie Gefahren und Sicherheitslöcher bekannt sind und gesperrt werden

Elemente einer Firewall

- Passiver Paketfilter mit Port- und Protokoll-Filter
- Aktives Gateway (Proxy) mit Virenscanner und Content-Filter
- Optimaler Schutz:
  - Durch Kombination aus Paketfilter und Proxy
  - Paketfilter sollte dem Proxy vorgeschaltet sein, um unnötigen Datenverkehr über den Proxy zu vermeiden



Arten und Funktionsweise 1/2

Packet Filter/Stateless Firewall:

- Arbeitet auf OSI-Schicht 3
- Kontrolle des Datenverkehrs basierend auf bestimmten Regeln
- Regeln und Filter basieren u. a. auf Eigenschaften des Datenpakets, wie z.B. Quell-IP-Adresse, Ziel-IP-Adresse und Port

Stateful Packet Inspection/Stateful Firewall:

- Arbeitet auf OSI-Schicht 3
- Zusätzliche Überwachung des Zustands einer Verbindung zwischen einem Client und einem Server sowie Zuordnung der Datenpakete zu einer Session

Application Firewall/Proxy Firewall/Gateway Firewall:

- Arbeitet auf OSI-Schicht 7
- Kontrolle des Datenverkehrs anhand der Protokolle, Ports und Anwendungsdaten

Web Application Firewall (WAF):

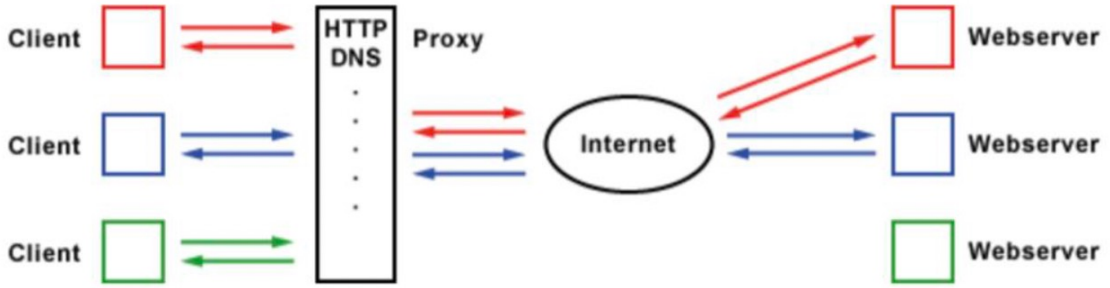
- Spezielle Art von der Application Firewall, die für Webanwendungen entwickelt wurde
- Filterung des Datenverkehrs für eine Webanwendung anhand der HTTP-Protokolldaten, der GET- oder POST-Parameter und anderer Anwendungsdaten

Arten und Funktionsweise 2/2

- Next-Generation Firewall (NGFW)
  - bieten zusätzliche Funktionen, wie zum Beispiel:
    - Intrusion Prevention Systeme (IPS): Überwachen den Datenverkehr auf verdächtige Aktivitäten und blockieren Angriffsversuche in Echtzeit.
    - Application Awareness: Erkennt und kontrolliert den Datenverkehr auf Anwendungsebene, z. B. durch das Blockieren bestimmter Anwendungen oder Dienste.
    - Deep Packet Inspection (DPI): Analysiert den Inhalt der Datenpakete auf Schadsoftware oder unerwünschte Daten.
    - Identitätsmanagement: Kontrolliert den Datenverkehr basierend auf Benutzeridentitäten und -rollen, z. B. durch das Zulassen oder Blockieren bestimmter Aktivitäten für bestimmte Benutzergruppen

Proxy

- Filtert und beeinflusst den Datenverkehr zwischen Client und Webserver
- Kann bestimmte Webseiten sperren oder den Zugriff auf bestimmte Inhalte beschränken
- Kann Datenverkehr beschleunigen, indem er die Webseiten zwischenspeichert (Cache) und bei wiederholtem Aufruf schneller an den Client übermittelt



11 DMZ

- Begriffsklärung
- Port Forwarding

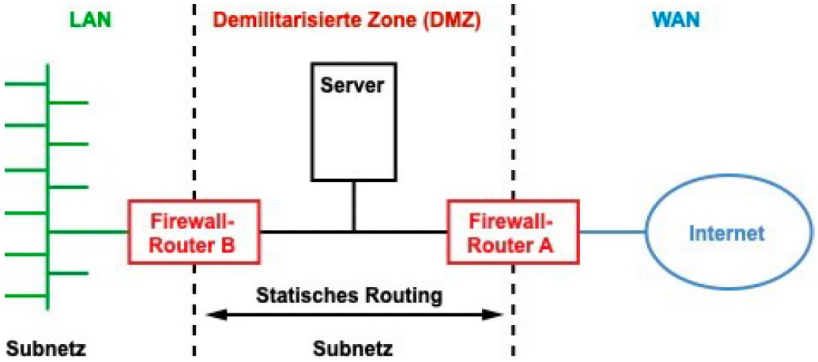
Begriffsklärung

Demilitarisierte Zone

- Netzwerkarchitektur zum Schutz kritischer Systeme im internen Netzwerk vor potenziellen Bedrohungen von außen
- Eigenständiges Subnetz, welches das lokale Netzwerk (LAN) durch Firewall-Router (A und B) vom Internet trennt
- Systeme in der DMZ haben begrenzte Verbindung zum internen Netzwerk und können nur auf bestimmte Ports und Protokolle zugreifen

Port Forwarding

- Benutzer haben Zugriff auf die in der DMZ platzierten Systeme, ohne dass sie direkt auf das interne Netzwerk zugreifen können
- Weiterleitung des Datenverkehrs eines bestimmten Ports auf dem Router an einen bestimmten Computer oder eine bestimmte Anwendung in der DMZ
- Zugriff auf Webserver in der DMZ möglich, ohne direkten Zugriff auf das interne Netzwerk



12 Leitlinien für Software-Entwicklung

- Sichere Entwicklung
- 4 zentrale Sicherheitsziele („CIAA“) in der Softwareentwicklung
- Secure SDLC
- Best Practices
- OWASP Top 10
- Eingabevalidierung als zentrales Schutzprinzip
- Begriffsklärung: CORS

Sichere Entwicklung

- **Frühzeitig einplanen:** Security gehört **ins Design**, nicht nur ins Testing
- **Risiken kennen:** OWASP Top 10 als Checkliste für Code Reviews und Schulungen
- **Validierung durchziehen:** Alle Eingaben strikt prüfen, nicht nur im Frontend
- **CORS richtig konfigurieren:** APIs nur für bekannte Clients freischalten
- **Regelmäßig testen:** Automatisierte Sicherheitsscans in CI/CD integrieren

4 zentrale Sicherheitsziele („CIAA“) in der Softwareentwicklung

Kriterium	Beschreibung	Entwicklungsrelevante Maßnahmen
C – Vertraulichkeit (Confidentiality)	Schutz vor unbefugtem Zugriff auf Daten	Zugriffskontrolle, Verschlüsselung, Geheimhaltung sensibler Daten
I – Integrität (Integrity)	Schutz vor unerlaubter oder unbeabsichtigter Veränderung von Daten	Input-Validierung, Hashing, Signaturen
A – Verfügbarkeit (Availability)	Systeme und Daten sind zum richtigen Zeitpunkt für berechtigte Nutzer verfügbar	Redundanz, Lastverteilung, Schutz vor DoS-Angriffen
A – Authentizität / Nachvollziehbarkeit (Accountability)	Nachweis über Aktionen und Identitäten	Logging, Auditing, Authentifizierung, Rechtemanagement

Secure SDLC

Secure Software Development Lifecycle

- Sicherheits-anforderungen im Softwareentwicklungs-prozess

Phase	Sicherheitsmaßnahme
Anforderungsanalyse	Sicherheitsziele definieren, Schutzbedarf analysieren
Design	Threat Modeling, Prinzipien wie „Least Privilege“
Implementierung	Secure Coding Practices (z. B. keine Hardcoded Secrets)
Testing	Penetrationstests, Fuzzing, automatisierte Sicherheitsscans
Deployment	Härtung der Umgebung, sichere Konfiguration
Betrieb/Wartung	Monitoring, Patch-Management, Log-Analyse

Best Practices

Prinzip	Beispiel
Security by Design	Sicherheitsaspekte von Anfang an einplanen
Least Privilege	Nutzende und Komponenten erhalten nur nötige Rechte
Fail Secure	Fehlerzustände dürfen keine neuen Schwachstellen schaffen
Defense in Depth	Mehrere Schutzschichten einbauen
Secure Defaults	Software sollte im „sicheren Zustand“ ausgeliefert werden
Keine Sicherheitslücken „verstecken“	„Security through obscurity“ gilt als unsicher
Sensitive Data nicht loggen	Passwörter oder Tokens gehören nie in Logs

OWASP Top 10

Open Web Application Security Project

- internationale Non-Profit-Organisation, die sich der Sicherheit von Webanwendungen widmet
- Erstellt international anerkannte Liste der häufigsten Sicherheitsrisiken für Webanwendungen
- dient als praktische Leitlinie für Entwickelnde, Architekten und Sicherheitsverantwortliche
- wird regelmäßig aktualisiert

- Eine detaillierte Übersicht aller 10 Risiken, inkl. Gegenmaßnahmen finden Sie in dem Dokument „**OWASP Top 10**“.

Eingabevalidierung als zentrales Schutzprinzip

Querschnittsmaßnahme, die essenziell in allen sicherheitskritischen Eingabepfaden ist – egal ob Webformular, API, URL-Parameter oder Upload-Funktion

Art	Zweck
Clientseitige Validierung	Nutzererfahrung verbessern
Serverseitige Validierung	Sicherheit gewährleisten (zwingend!)
Whitelist-Validierung	Nur erlaubte Formate/Zeichen zulassen
Blacklist-Validierung	Verbieten gefährlicher Zeichen (unsicher)

Was wird validiert?

Kontext	Was validieren?	Beispiel
Textfelder	Länge, erlaubte Zeichen, Format	Nur ASCII, keine <script>-Tags
Zahlenwerte	Wertebereich, Ganzzahlen	1 ≤ Alter ≤ 120
IDs und Parameter	Existenz in DB, Format (UUID, int)	Nur gültige user_id verwenden
Dateiuploads	Dateityp, MIME-Type, Größe	Kein .exe, .php bei Bild-Upload
URLs (SSRF-Prävention)	Nur erlaubte Domains und Protokolle	Kein Zugriff auf localhost, 169.254.*.*
CORS-Header	Nur zulässige Origins akzeptieren	Kein Access-Control-Allow-Origin: *

Risiken, bei denen Validierung notwendig oder empfohlen ist

OWASP-Risiko	Rolle der Validierung
A03 – Injection	🔥 Zentrale Gegenmaßnahme!Validierung verhindert Einschleusung von z. B. SQL-/XSS-Code
A01 – Broken Access Control	Validierung von Rollen- und Rechteparametern (z. B. user_id, role)
A02 – Cryptographic Failures	Eingabevalidierung schützt z. B. Schlüsselparameter, Passwörter, Dateiformate
A04 – Insecure Design	Validierung ist ein Bestandteil sicherer Architektur (z. B. Input Contracts)
A05 – Security Misconfiguration	Validierung kann Header- und Konfigurationseingaben auf Richtigkeit prüfen
A07 – Identification & Authentication Failures	Validierung von Login-Daten, Passwortstärke, 2FA-Codes
A09 – Security Logging & Monitoring Failures	Validierung hilft beim Schutz von Logfeldern vor Log-Injection (z. B. über manipulierte Eingaben)
A10 – SSRF (Server-Side Request Forgery)	Validierung von Ziel-URLs/IPs, um interne Netzwerke zu schützen

Begriffsklärung: CORS

Cross-Origin Resource Sharing

- Mechanismus im Browser, der kontrolliert, ob und welche externen Webseiten auf Ressourcen eines Servers zugreifen dürfen
  - insbesondere bei API-Zugriffen über Domains hinweg
- Teil von A05 – Security Misconfiguration der OWASP Top 10
- Falsch konfigurierte CORS-Header können es Angreifern ermöglichen, Anfragen im Namen eines angemeldeten Nutzers auszuführen