Kapitel 6. Netzwerke

Inhaltsverzeichnis

6.1 Netzwerktechnik

Fachbegriff Netzwerk

Definition

Ein Netzwerk ist ein Zusammenschluss von mindestens zwei Computern oder digitalen Geräten, die miteinander verbunden sind, um Daten, Ressourcen (z.B. Drucker, Internet, Dateien) oder Dienste auszutauschen. Netzwerke ermöglichen eine effiziente Kommunikation und zentrale Verwaltung in IT-Infrastrukturen.

Grundfunktionen eines Netzwerks

- Datenübertragung zwischen Geräten
- Zugriff auf zentrale Ressourcen (z.B. Server, Drucker, Datenbanken)
- Verbindung ins Internet
- Zentrale Benutzerverwaltung (z.B. über Active Directory)
- Kommunikation (z.B. E-Mail, Chats, IP-Telefonie)

Typische Netzwerkarten

NETZWERKTYP	BESCHREIBUNG	BEISPIEL
LAN (LOCAL AREA NETWORK)	Lokales Netzwerk innerhalb eines Gebäudes oder Raumes	Schulnetzwerk, Heimnetzwerk, Firmennetzwerk
WLAN (WIDE AREA NETWORK)	Drahtlose Variante des LAN	Wi-Fi-Netz zu Hause, Hotspots, mobile Geräte
WAN (WIDE AREA NETWORK)	Weltumspannendes Netzwerk	Internet
MAN (METROPOLITAN AREA NETWORK)	Netzwerk über mehrere Standorte in einer Stadt	Uni-Netzwerk, Stadtverwaltung
VPN (VIRTUAL PRIVATE NETWORK)	Virtuelles Netzwerk, über öffentliche Netze, aber verschlüsselt	Sicherer Fernzugriff auf Firmennetz
PAN (PERSONAL AREA NETWORK)	Sehr kleines Netzwerk rund um eine Person	Bluetooth-Verbindung zwischen Handy-Kopfhörer

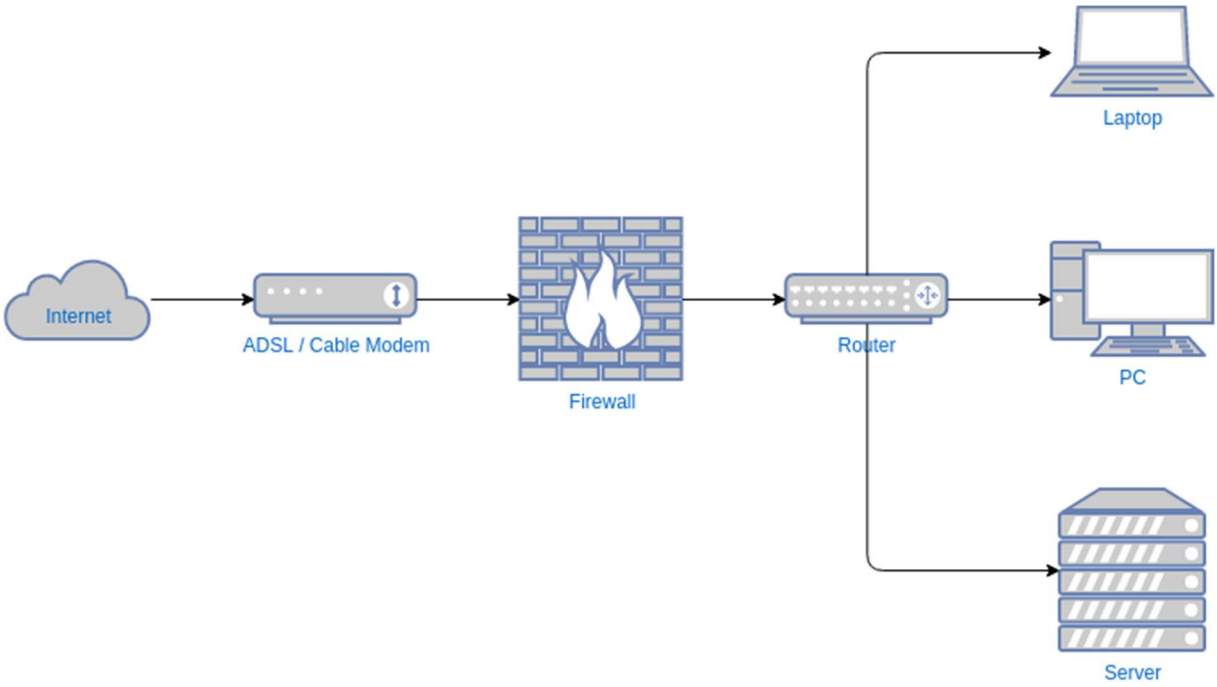
Bestandteile eines Netzwerks

- Endgeräte: PC, Laptop, Drucker, Smartphone
- Netzwerkgeräte: Router, Switch, Access Point, Modem, Firewall
- Übertragungsmedien: Netzwerkkabel /Twisted Pair, Glasfaser), Funk (Wi-Fi, BT)
- Protokolle: Regeln für die Kommunikation (z.B. TCP/IP, DHCP, DNS)

Wichtige Begriffe im Zusammenhang

- IP-Adresse: Eindeutige Adressen im Netzwerk zur Geräteidentifikation
- MAC-Adresse: Physikalische Hardwareadresse
- Subnetzmaske: Strukturierung eines Netzwerks in kleinere Segmente
- Gateway: Übergangspunkt zwischen eigenem Netzwerk und Internet

Grafische Darstellung eines Netzwerks



Netzwerktopologien: Stern, Ring, Bus, Baum, Masche

Definition

Eine Netzwerktopologie beschreibt die Anordnung und Verbindung der Geräte (Knoten) in einem Netzwerk – entweder physisch (tatsächliche Verkabelung) oder logisch (Datenfluss). Die Topologie beeinflusst Leistung, Ausfallsicherheit, Skalierbarkeit und Wartbarkeit des Netzwerks.

Übersicht der Netzwerktopologien

Stern:

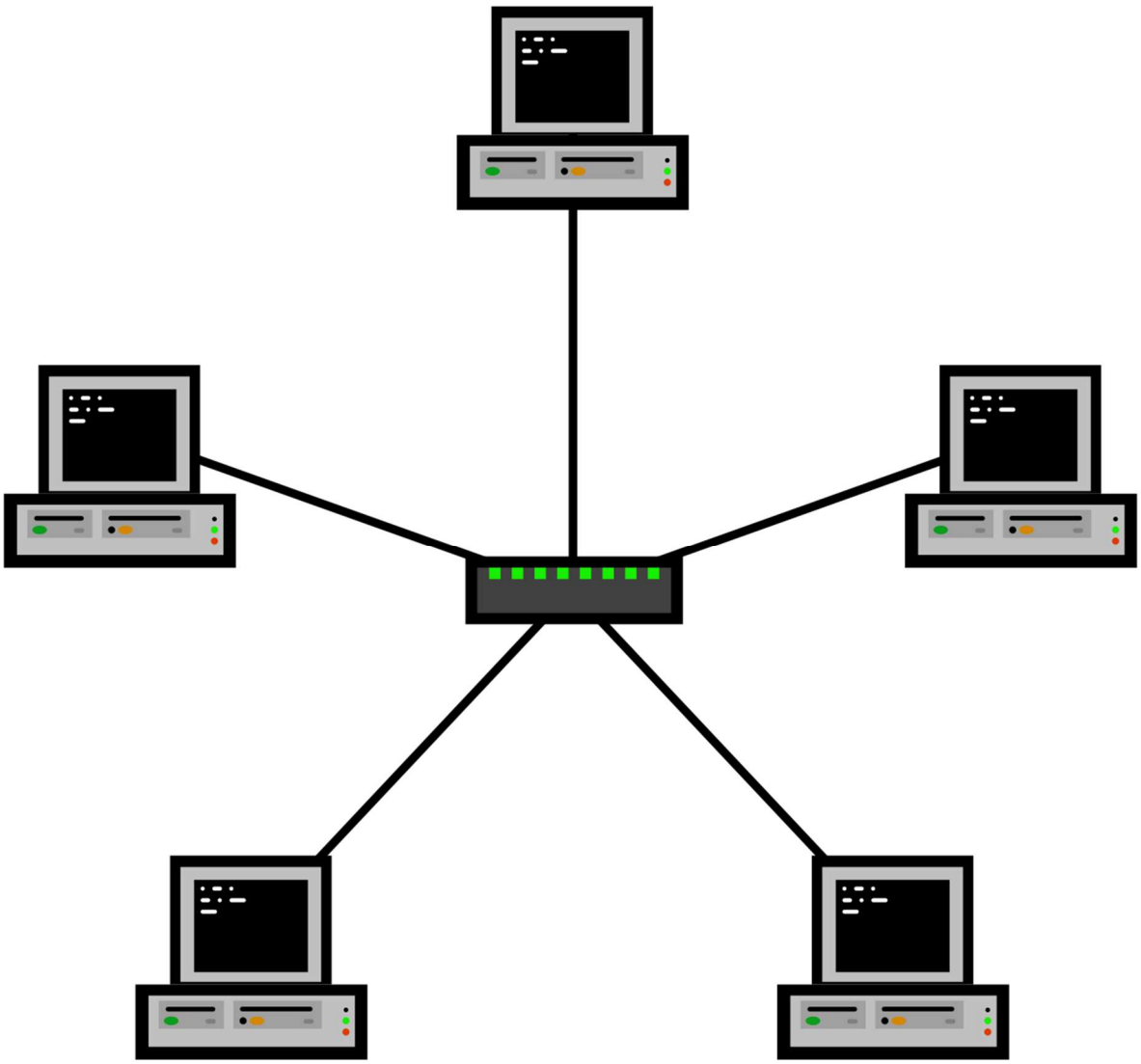
Alle Geräte sind mit einem zentralen Knoten wie einem Switch oder Hub verbunden. Wird für klassische LANs verwendet.

Vorteile:

- Einfach zu verwalten
- Leicht erweiterbar
- Ausfall eines Endgeräts hat keine Auswirkungen auf das Gesamtnetz

Nachteile:

- Zentrale Einheit ist Schwachpunkt – fällt sie aus fällt das ganze Netz aus



Ring:

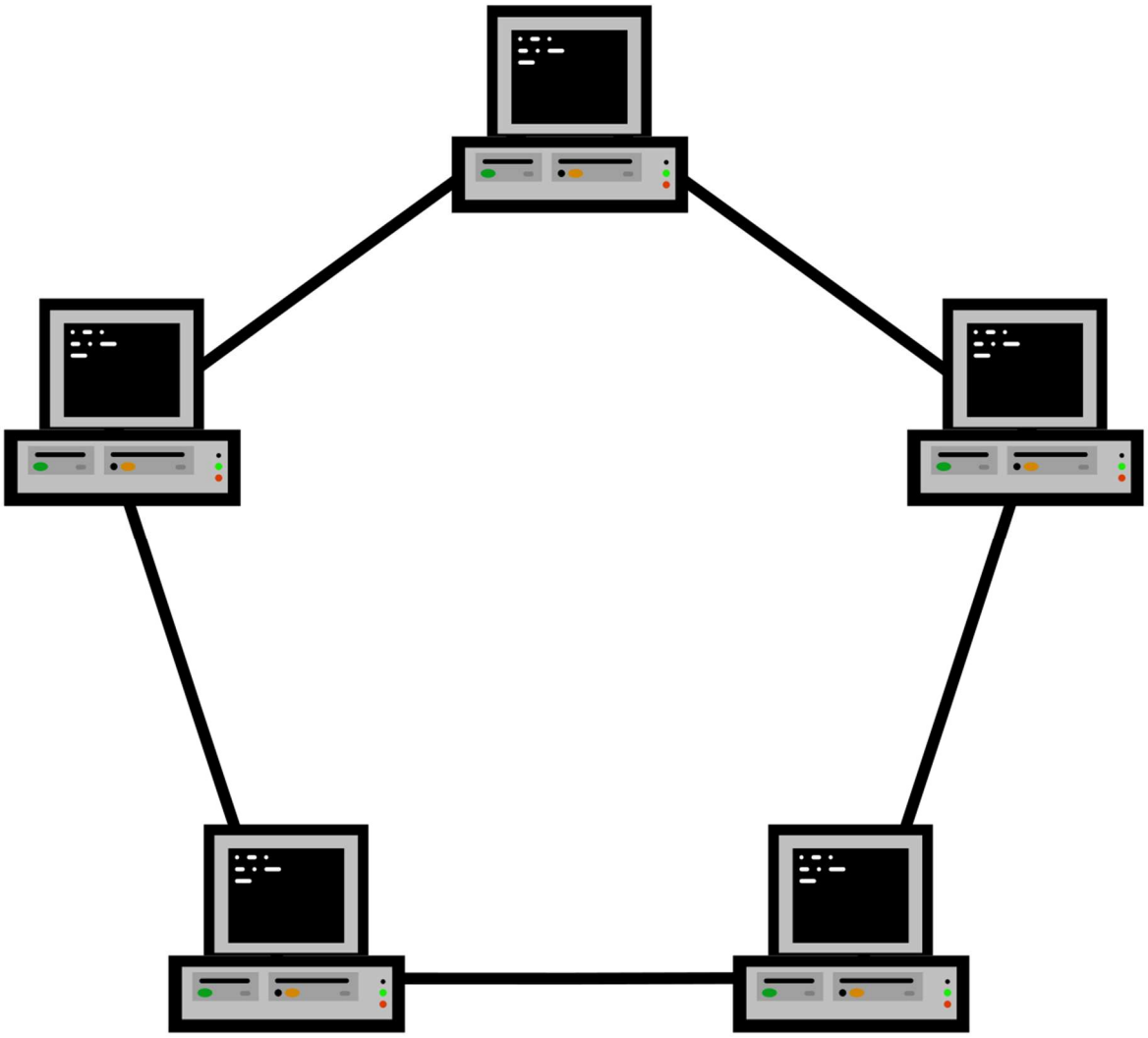
Geräte sind in einem geschlossenen Kreis verbunden – Daten wandern im Kreis. Früher Token Ring, FDDI-Netze

Vorteile:

- Gleichmäßige Auslastung
- Vorhersehbarer Datenfluss

Nachteile:

- Ausfall eines Geräts unterbricht das gesamte Netzwerk (ohne Protection-Umschaltung)



Bus:

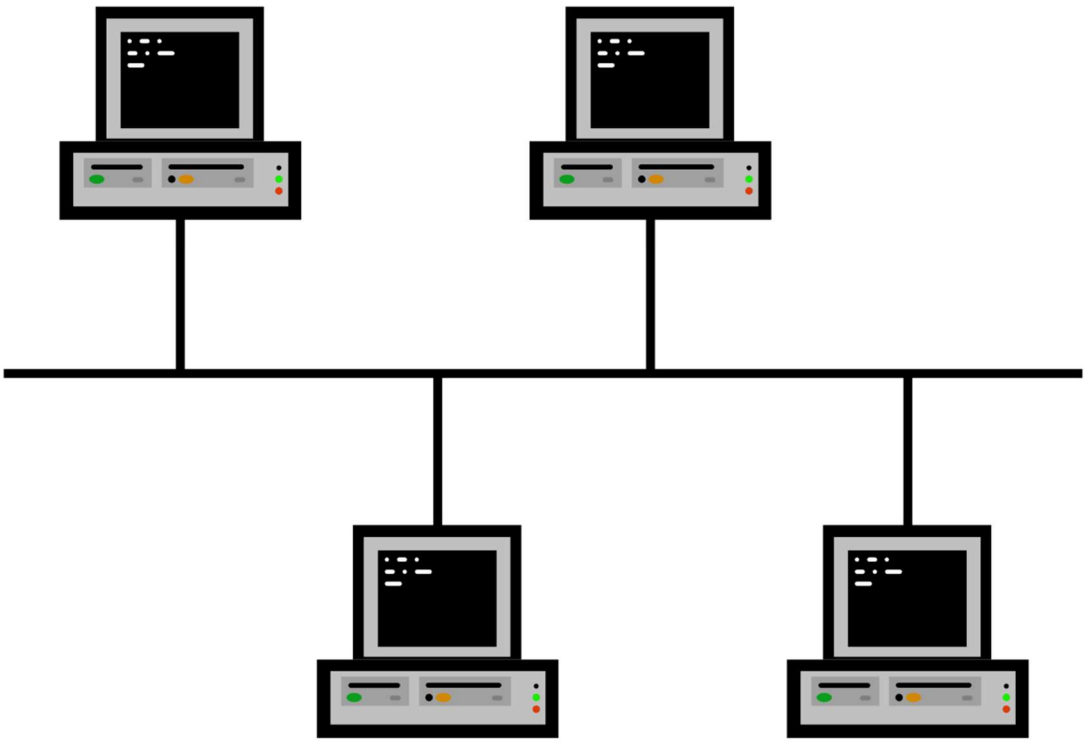
Alle Geräte hängen an einer gemeinsamen Leitung dem Buskabel.

Vorteile:

- Einfach und günstig bei wenigen Geräten

Nachteile:

- Datenkollisionen
- Schwer erweiterbar
- Niedrige Leistung bei hoher Teilnehmeranzahl



Baum:

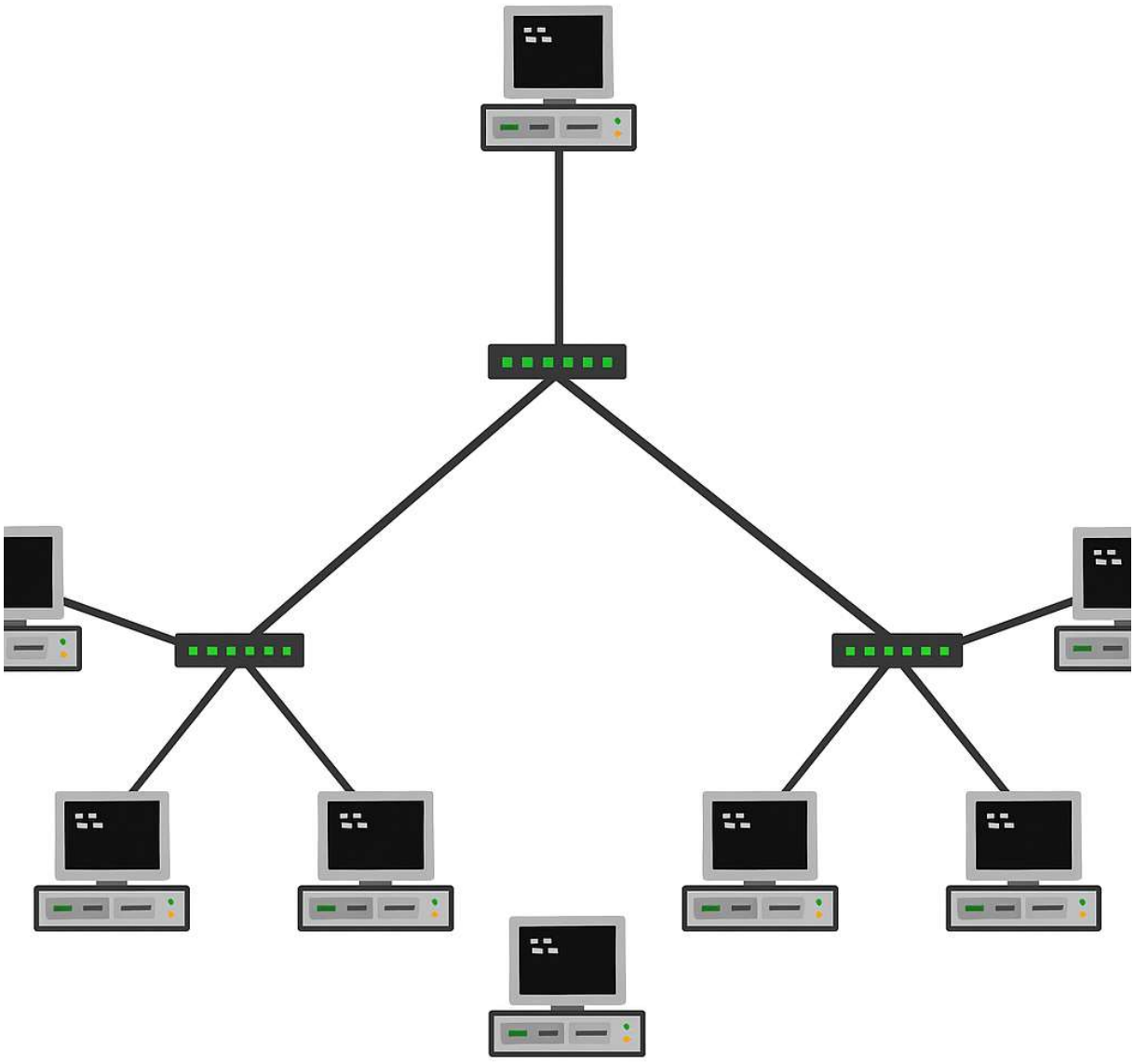
Hierarchische Sternstruktur, bei der mehrere Sternnetzwerke an einen Backbone angeschlossen sind.

Vorteile:

- Gut strukturiert
- Erweiterbar
- Übersichtlich

Nachteile:

- Ausfall des Backbones oder zentraler Knoten gefährdet gesamte Struktur



Masche:

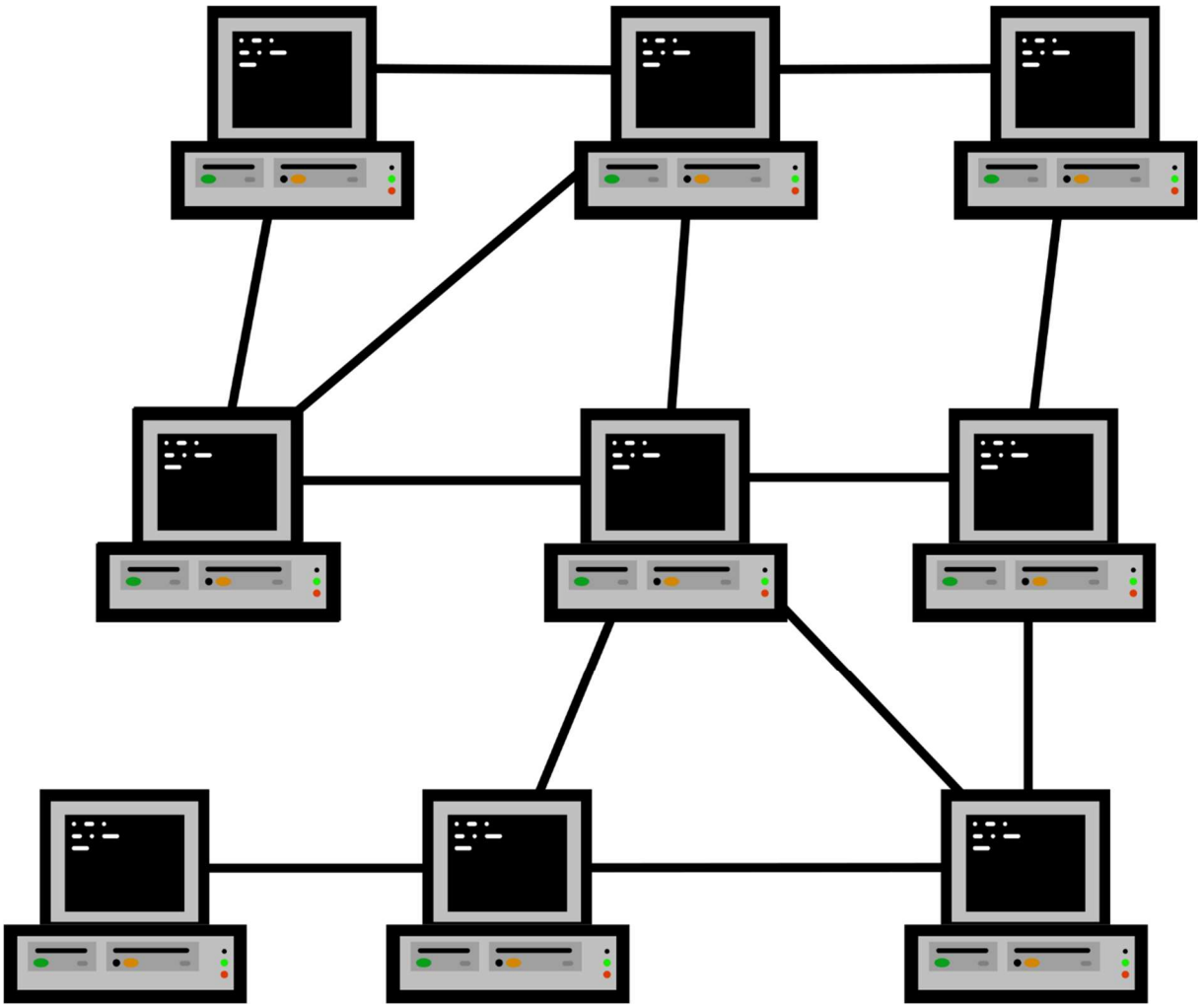
Jeder Knoten ist mit mehreren anderen direkt verbunden.

Vorteile:

- Höchste Ausfallsicherheit
- Direkte Datenwege

Nachteile:

- Sehr teuer und aufwendig zu verkabeln
- Komplex zu konfigurieren



Kenntnis der Vor- und Nachteile der jeweils eingesetzten Netzwerktopologien

Sterntopologie

Vorteile:

- Einfache Installation und Erweiterung
- Fehler in Endgeräten beeinträchtigen das Netzwerk nicht
- Übersichtliche Struktur
- Leichte Fehlersuche
- Gute Performance bei vielen Teilnehmern

Nachteile:

- Zentrale Komponente ist ein Single Point of Failure
- Höherer Kabelbedarf als bei Bus
- Abhängig von zentralem Switch/Hub

Ringtopologie

Vorteile:

- Gleichmäßige Auslastung
- Keine Kollisionen (besonders bei Token-Ring)
- Vorhersehbare Übertragungszeiten

Nachteile:

- Ausfall eines Geräts kann das Netz lahmlegen
- Erweiterung nur schwer möglich
- Störungsanfälliger Datenfluss
- Fehlersuche aufwendig

Bustopologie

Vorteile:

- Sehr einfacher Aufbau
- Geringer Kabelaufwand
- Günstige Kostenstruktur

Nachteile:

- Datenkollisionen möglich (insbesondere bei CSMA/CD)
- Bei vielen Teilnehmern stark abnehmende Performance
- Begrenzte Länge und Teilnehmeranzahl
- Fehleranfällig – Kabelbruch = Netzdefekt

Baumtopologie

Vorteile:

- Gut strukturiert und skalierbar
- Kombination aus Stern- und Busvorteilen
- Ideal für große, strukturierte Netzwerke
- Verwaltung von Teilsegmenten möglich

Nachteile:

- Abhängigkeit vom Backbone – bei Ausfall teilweise Totalausfall
- Hoher Verkabelungsaufwand
- Komplexere Administration

Maschentopologie

Vorteile:

- Höchste Ausfallsicherheit und Redundanz
- Direkte Datenwege
- Selbstheilende Routen bei Störung
- Höchste Verfügbarkeit

Nachteile:

- Sehr teuer und komplex
- Hoher Verkabelungs- und Wartungsaufwand
- Nicht wirtschaftlich bei kleinen Netzen

Funktionsprinzip eines Routers, Switches

Switch – Funktionsprinzip

Ein Switch (Layer-2-Gerät) verbindet Geräte innerhalb eines lokalen Netzwerks (LAN) und leitet Datenpakete gezielt an den richtigen Empfänger weiter – basierend auf MAC-Adressen.

Typischer Einsatz ist die Verbindung mehrerer PCs in einem Büro oder als Backbone-Komponente in Stern- oder Baumtopologie.

Funktionsweise:

- Arbeitet auf OSI-Schicht 2 (Data Link Layer)
- Lernt MAC-Adressen anhand der empfangenen Frames
- Führt eine MAC-Adresstabelle (Forwarding Table)
- Wenn ein Frame eingeht, prüft der Switch:
    - Ist die Zieladresse bekannt? → Nur an diesen Port weiterleiten
    - Ist sie unbekannt? → An alle Ports senden (außer dem Empfangsport)

Vorteile:

- Reduziert Broadcast-Verkehr
- Verbessert Netzwerkauslastung
- Hohe Übertragungsgeschwindigkeit
- Vollduplex möglich (senden + empfangen gleichzeitig)

Router – Funktionsprinzip

Ein Router (Layer-3-Gerät) verbindet mehrere Netzwerke miteinander (z.B. LAN mit dem Internet) und leitet Datenpakete anhand von IP-Adressen weiter.

Funktionsweise:

- Arbeitet auf OSI-Schicht 3 (Network Layer)
- Nutzt Routing-Tabellen zur Pfadfindung
- Prüft Ziel-IP-Adresse → Leitet das Paket an den nächsten Hop
- Führt oft auch NAT (Network Address Translation) durch:
    - Wandelt interne IP-Adressen in eine öffentliche um
- Kann mit Firewall- und QoS-Funktionen erweitert sein

Vorteile:

- Ermöglicht Kommunikation zwischen verschiedenen Netzwerken
- Notwendig für Internetzugang
- Unterstützt Subnetting und IP-Routing
- Sicherheit durch NAT, Firewall-Integration

Kenntnis des Fachbegriffes Subnetzmaske und deren technischen Zusammenhänge

Definition

Die Subnetzmaske trennt bei einer IP-Adresse den Netzwerkanteil vom Hostanteil. Sie definiert, welche IP-Adressen zu einem Subnetz gehören. Dies ist entscheidend für Routing, Adressierung und IP-Management. Eine IP-Adresse besteht aus zwei Teilen, den Netzanteil und den Hostanteil welche sich durch die logische „UND“ Verknüpfung von IP-Adresse und Subnetzmaske ergeben.

Beispiel

	Dezimalschreibweise	Bitschreibweise
IP-Adresse	192.168.1.10	11000000.10101000.00000001.00001010
Subnetzmaske	255.255.255.0	11111111.11111111.11111111.00000000
Netzadresse	192.168.1.0	11000000.10101000.00000001.00000000

Durch die Subnetzmaske herrscht eine Trennung von Netzanteil und Hostanteil. In der Bitschreibweise stehen die 1en für den Netzanteil und die 0en für den Hostanteil. Korrekte Subnetzmasken sind immer eine Folge aus 1en und 0en.

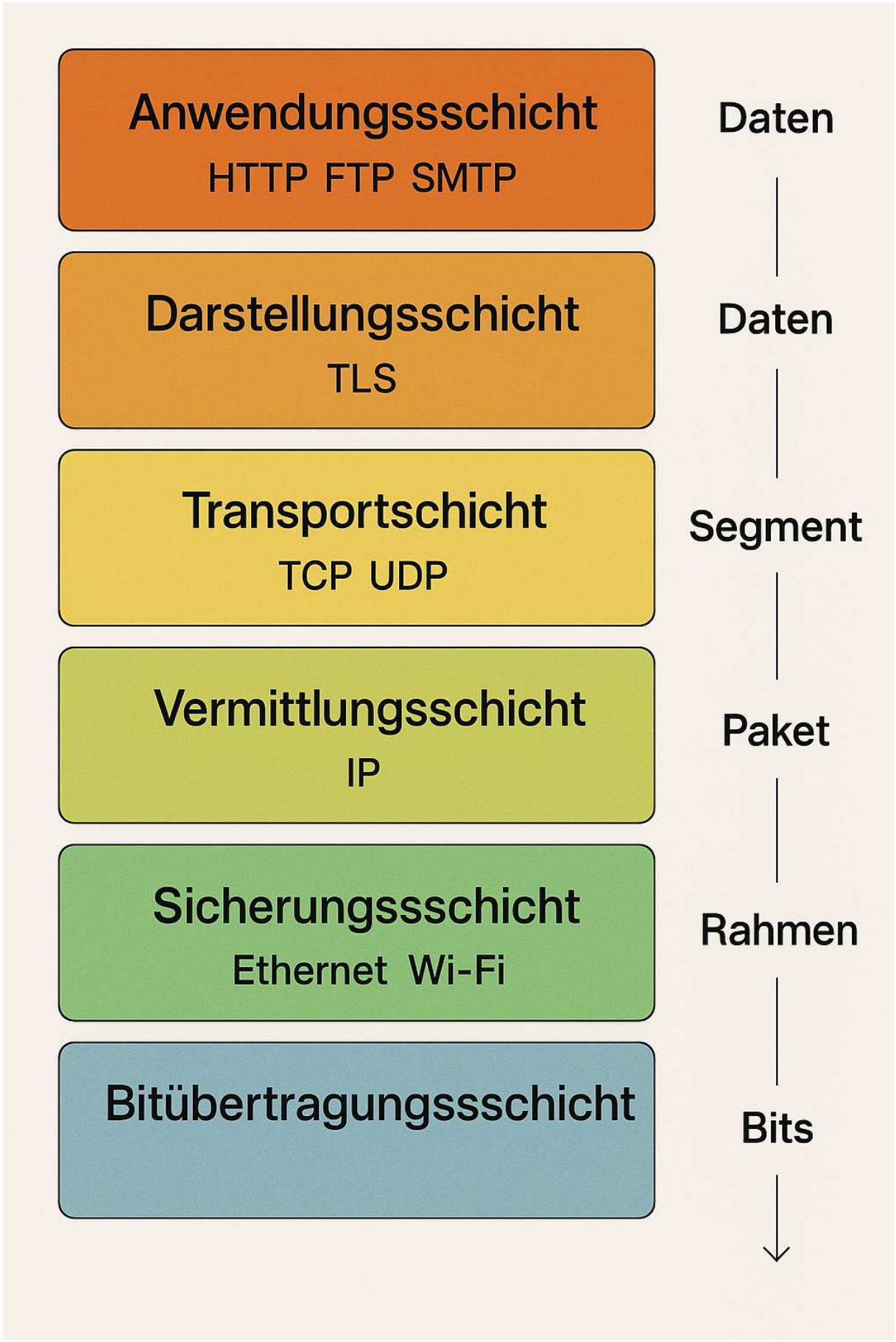
Seit CIDR (Classless Inter-Domain Routing) werden für die Subnetzmaske Notationen wie /24 verwendet um anzugeben, wie viele Bits für das Netzwerk verwendet werden. Je mehr Bits für das Netz, desto weniger Hosts pro Subnetz dafür mehr Subnetze.

Kenntnisse über das OSI-Modell

Das OSI-Modell (Open Systems Interconnection Model) ist ein konzeptionelles Schichtenmodell, das beschreibt, wie Daten in einem Netzwerk von einer Anwendung auf einem Computer zu einer Anwendung auf einem anderen übertragen werden. Es dient als Referenzmodell zur Standardisierung von Netzwerkprotokollen und -kommunikation.

Datentransport durch das OSI-Modell

Beim Senden von Daten fügt jede Schicht einen Header (und ggf. Trailer) hinzu, dies nennt man Encapsulation. Beim Empfänger werden diese Header durch die jeweilige Schicht Decapsuliert.


Anwendungsschicht
HTTP FTP SMTP
Daten
Darstellungsschicht
TLS
Daten
Transportschicht
TCP UDP
Segment
Vermittlungsschicht
IP
Paket
Sicherungsschicht
Ethernet Wi-Fi
Rahmen
Bitübertragungsschicht
Bits

Die einzelnen Schichten im Überblick

Jede Schicht nutzt die Dienste der darunterliegenden Schicht und stellt Funktionen für die darüberliegende bereit. Die Modularität erlaubt Austausch und Kombination verschiedener Protokolle.

Schicht 1 – Bitübertragungsschicht (Physical Layer)

Funktion: Übertragung roher Bits über ein physikalisches Medium (0 und 1 als elektrische, optische oder Funk-Signale).

Beispiele:

- Ethernet-Kabel, Glasfaser, WLAN (802.11), Bluetooth
- Stecker (RJ45), Spannungsspezifikationen
- Geräte: Netzwerkkarten, Hubs, Repeater, Medienkonverter
- Wichtig: Keine Protokollinformationen, rein physikalisch.

Schicht 2 – Sicherungsschicht (Data Link Layer)

Funktion: Stellt eine fehlerfreie Verbindung zwischen zwei direkt verbundenen Geräten her.
Aufgaben:

- MAC-Adressen, Frame-Erstellung
- Fehlererkennung (z. B. CRC)
- Flusskontrolle auf Layer-2
  Protokolle: Ethernet, PPP, ARP, VLAN (802.1Q), HDLC
  Geräte: Switches, Bridges

Schicht 3 – Vermittlungsschicht (Network Layer)

Funktion: Routing von Paketen über mehrere Netzwerke hinweg.
Aufgaben:

- Logische Adressierung (z. B. IP-Adressen)
- Fragmentierung
- Weiterleitung durch Router
  Protokolle: IPv4, IPv6, ICMP, IPsec, OSPF, BGP
  Geräte: Router, Layer-3-Switches
  Wichtig: Erster Layer, der „netzwerkübergreifend“ denkt.

Schicht 4 – Transportschicht (Transport Layer)

Funktion: End-to-End-Kommunikation, Zuverlässigkeit und Flusskontrolle
Aufgaben:

- Segmentierung der Daten
- Fehlerkorrektur, Wiederholung bei Paketverlust
- Multiplexing (Ports)

Protokolle:

- TCP: Verbindungsorientiert, zuverlässig
- UDP: Verbindungslos, schnell
  Geräte: Endsysteme (Clients, Server)
  Beispiel: TCP-Port 80 für HTTP, 443 für HTTPS

Schicht 5 – Sitzungsschicht (Session Layer)

Funktion: Aufbau, Verwaltung und Beendigung von Kommunikationssitzungen
Aufgaben:

- Synchronisation
- Wiederaufnahme nach Unterbrechung
  Protokolle: NetBIOS, RPC, PPTP, SMB
  Wichtig: Meist in modernen TCP/IP-Netzen in höheren Schichten integriert

Schicht 6 – Darstellungsschicht (Presentation Layer)

Funktion: Übersetzung der Daten in ein standardisiertes Format
Aufgaben:

- Verschlüsselung/Entschlüsselung
- Komprimierung/Dekomprimierung
- Formatkonvertierung (ASCII, EBCDIC, JPEG, MPEG)
  Beispiele: SSL/TLS, MIME-Encoding
  Praxis: Webbrowser dekodiert HTTPS über TLS hier.

Schicht 7 – Anwendungsschicht (Application Layer)

Funktion: Schnittstelle zwischen Netzwerk und Nutzeranwendung
Aufgaben:

- Datenbereitstellung für Nutzer
- Endnutzer-Authentifizierung, Protokollfunktionen
  Protokolle: HTTP(S), FTP, SMTP, DNS, SNMP, Telnet
  Praxis: Alles, was für den Benutzer sichtbar ist – z. B. der Inhalt einer Webseite

Einordnung von Protokollen in das OSI-Modell

Die **Einordnung von Protokollen in das OSI-Modell** ist essenziell, um Netzwerke strukturiert zu verstehen und zu analysieren. Jedes Protokoll gehört zu einer bestimmten Schicht (manche auch überlappend) und erfüllt dort spezifische Aufgaben.

Schicht 1 – Bitübertragungsschicht (Physical Layer)

Übertragung elektrischer/optischer Signale.

- **RJ45, Glasfaser, Koax, WLAN (802.11)** – Medienstandards
- **DSL, ISDN, Bluetooth, USB** – Übertragungstechnologien

Schicht 2 – Sicherungsschicht (Data Link Layer)

Fehlererkennung, MAC-Adressen, Frames.

- **Ethernet (IEEE 802.3)** – LAN-Standard
- **ARP** – IP-zu-MAC-Auflösung
- **PPP** – Punkt-zu-Punkt-Verbindungen
- **STP/RSTP** – Schleifenerkennung bei Switches
- **VLAN (802.1Q)** – virtuelle LANs

Schicht 3 – Vermittlungsschicht (Network Layer)

Routing und logische Adressierung.

- **IPv4/IPv6** – Adressierung
- **ICMP** – Fehler- und Diagnosenachrichten (z. B. bei Ping)
- **OSPF, BGP, RIP** – Routing-Protokolle
- **IPsec** – Verschlüsselung auf IP-Ebene

Schicht 4 – Transportschicht (Transport Layer)

Zuverlässiger oder schneller Transport zwischen Endpunkten.

- **TCP** – Zuverlässige, verbindungsorientierte Kommunikation
- **UDP** – Schnelle, verbindungslose Kommunikation
- **SCTP** – Multistreaming, Multi-Homing

Schicht 5 – Sitzungsschicht (Session Layer)

Sitzungsverwaltung und Synchronisation.

- **NetBIOS** – Netzwerkkommunikation in Windows-Umgebungen
- **RPC** – Remote-Prozeduren
- **PPTP** – VPN-Protokoll

Schicht 6 – Darstellungsschicht (Presentation Layer)

Datenformatierung, Kodierung, Verschlüsselung.

- **SSL/TLS** – Verschlüsselung von Verbindungen
- **MIME** – E-Mail-Formatierung
- **ASCII, JPEG, MPEG** – Datenformate

Schicht 7 – Anwendungsschicht (Application Layer)

Stellt Dienste für Endanwender bereit, z. B. Webzugriffe oder E-Mail.

- **HTTP/HTTPS** – Webseiten (Port 80/443)
- **FTP/SFTP** – Dateitransfer
- **SMTP/POP3/IMAP** – E-Mail
- **DNS** – Namensauflösung
- **Telnet, SSH** – Remote Access
- **SNMP** – Netzwerkmanagement
- **DHCP** – IP-Adressvergabe

Einordnung von Netzwerk- und Hardwaregeräten in das OSI-Modell

OSI-Schicht	Gerätebeispiele
Schicht 1	Netzwerkkarte, Repeater, Hub, Modem, Access Point
Schicht 2	Switch, Bridge, Netzwerkkarte, Access Point, VLAN-fähige Geräte
Schicht 3	Router, Layer-3-Switch, Firewall
Schicht 4-7	Application Firewalls, Gateways, Proxys, Load Balancer

Kenntnisse über die Protokollfamilie TCP/IP

Was ist TCP/IP?

TCP/IP (Transmission Control Protocol / Internet Protocol) ist eine Sammlung von standardisierten Nerzwerkprotokollen, di die Kommunikation zwischen Computern und Geräten im Internet oder lokalen Netzwerken ermöglichen.

- Entwickelt: 1970er-Jahre (für ARPANET, Vorgänger des Internets)
- Einsatzgebiet: Grundprotokoll des Internets und nahezu aller modernen Netzwerke
- Architektur: Mehrschichtig – ähnlich wie OSI, aber einfacher (4Schichten)

Schichtenmodell von TCP/IP im Vergleich zum OSI-Modell

TCP/IP-SCHICHT	IM OSI-MODELL	FUNKTION
ANWENDUNGSSCHICHT	OSI-Schichten 5-7	Nutzernahe Kommunikation (HTTP, HTTPS, FTP, DNS…)
TRANSPORTSCHICHT	OSI-Schicht 4	Zuverlässiger Datentransport (TCP/UDP)
INTERNETSCHICHT	OSI-Schicht 3	Routing, IP-Adressen (IP, ICMP)
NETZZUGANGSSCHICHT	OSI-Schichten 1-2	Physische Übertragung (Ethernet, WLAN, PPP)

Wichtige Protokolle der TCP/IP-Familie

Anwendungsschicht:

PROTOKOLL	FUNKTION
HTTP/HTTPS	Webseiten anzeigen (Browser)
FTP/SFTP	Dateiübertragung
DNS	Namensauflösung (Domain – IP)
SMTP/POP3/IMAP	E-Mail-Versand und -Abruf
DHCP	Automatische IP-Zuweisung

Transportschicht:

PROTOKOLL	FUNKTION
TCP (TRANSMISSION CONTROL PROTOCOL)	Verbindungsorientiert, zuverlässig, mit Fehlerkorrektur
UDP (USER DATAGRAM PROTOCOL)	Verbindungslos, schneller ohne Fehlerkorrektur (z.B. Streaming, DNS)

Internetschicht:

PROTOKOLL	FUNKTION
IPV4 / IPV6	Adressierung & Routing
ICMP	Diagnosedienste (z.B. Ping)
ARP	Zuordnung von IP- zu MAC-Adressen im LAN

Netzzugangsschicht:

TECHNIK/PROTOKOLL	FUNKTION
ETHERNET	Kabelgebundene Netzwerke
WLAN (IEEE 802.11)	Drahtlose Übertragung
PPP	Punkt-zu-Punkt-Verbindung (z.B. Modem)

Kommunikation in TCP/IP

1. Anwendung erzeugt Daten (z. B. HTTP-Request)
2. TCP/UDP segmentiert Daten in Pakete
3. IP versieht sie mit IP-Absender/Zieladresse
4. Netzwerkschicht überträgt sie physikalisch
5. Auf Empfängerseite wird das Ganze umgekehrt wieder zusammengesetzt

TCP vs. UDP – Vergleich

MERKMAL	TCP	UDP
VERBINDUNG	Verbindungsorientiert	Verbindungslos
ZUVERLÄSSIGKEIT	Ja (Bestätigungen, Wiederholung)	Nein
GESCHWINDIGKEIT	Langsamer	Schneller
ANWENDUNG	Web, E-Mail, Dateiübertragungen	VoIP, Streaming, DNS

Fachbegriff IPv4-Adresse und deren Aufbau

Definition

Eine IPv4-Adresse (Internet Protocol Version 4) ist eine 32-Bit lange Zahl, die jedem Gerät in einem IP-basierten Netzwerk eine eindeutige Identifikation zuweist. Sie ist notwendig, damit Datenpakete korrekt zwischen Sender und Empfänger vermittelt werden können.

Aufbau einer IPv4-Adresse:

- Besteht aus 4 Oktetten (je 8 Bit) → insgesamt 32 Bit
- Darstellung in Dezimalform, z. B.: 192.168.1.10
- Jedes Oktett: Wertebereich von 0 bis 255

Bitschreibweise:

BINÄR	DEZIMAL
11000000.10101000.00000001.00001010	192.168.1.10

Struktur: Netzwerk- und Hostanteil

Die IPv4-Adresse ist abhängig von der Subnetzmaske zweigeteilt:

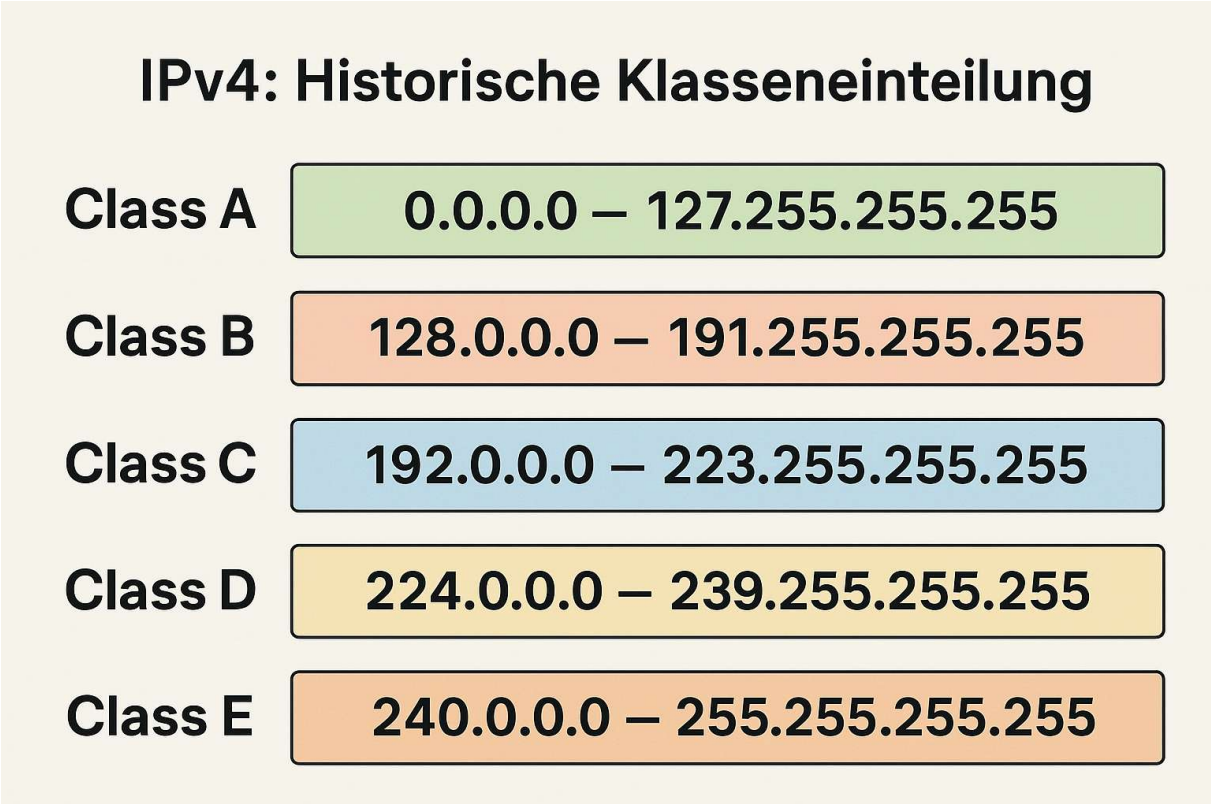
- **Netzanteil:** Gibt an, zu welchem Netzwerk die Adresse gehört.
- **Hostanteil:** Identifiziert das einzelne Gerät innerhalb des Netzwerks.

Adressproblematik und Lösungen

IPv4 wurde als Teil der Internetprotokollfamilie für das Arpanet entwickelt und kam darin ab 1983 zum Einsatz. Damals waren nur einige hundert Rechner an das Netz angeschlossen. Das Arpanet entwickelte sich zum Internet und überschritt 1989 die Grenze von 100.000 Rechnern.

Anfang der 1990er Jahre war erkennbar, dass IP-Adressen bald knapp würden, da die damals übliche Netzklassen-basierte Adressvergabe erheblichen Verschnitt verursachte. Als kurzfristige Lösung wurde 1993 Classless Inter-Domain Routing eingeführt, das eine deutlich effizientere Adressvergabe ermöglichte.

Klassenbasierte Einteilung:



CIDR - Classless Inter-Domain Routing

CIDR (Classless Inter-Domain Routing) ist trotz der Namensgebung kein Routing-Protokoll, sondern ein Verfahren, um den IPv4-Adressraum effizienter zu nutzen. CIDR wurde 1993 eingeführt, um das Konzept der Netzklassen abzulösen. Mit CIDR fällt die feste Zuordnung zwischen IPv4-Adresse und einer bestimmten Netzklasse weg. Vor CIDR hat die Netzklasse definiert, welcher Teil der Netzteil und welcher der Hostanteil einer IPv4-Adresse ist. Mit CIDR steckt diese Information in einem Suffix.

Vereinfacht ausgedrückt ist das Suffix eine Schreibweise, die die Subnetzmaske abkürzt. Das Suffix gibt die Anzahl der aufeinander folgenden 1er Bits in der Subnetzmaske an.

255.255.255.0 = 11111111.11111111.11111111.00000000 = /24

IPv4 Adressbereiche

Private Netzwerke (RFC1918)
Diese Adressbereiche sind für den internen Gebrauch in privaten Netzwerken vorgesehen und werden im öffentlichen Internet nicht geroutet.

CIDR-BLOCK	ADRESSBEREICH	BESCHREIBUNG
10.0.0.0/8	10.0.0.0 – 10.255.255.255	Große private Netzwerke
172.16.0.0/12	172.16.0.0 – 172.31.255.255	Mittlere private Netzwerke
192.168.0.0/16	192.168.0.0 – 192.168.255.255	Kleine private Netzwerke

Spezielle und reservierte Adressbereiche (RFC 5735, RFC 6890)
Diese Adressbereiche sind für spezielle Zwecke reserviert.

CIDR-BLOCK	ADRESSBEREICH	BESCHREIBUNG
0.0.0.0/8	0.0.0.0 – 0.255.255.255	Nur als Quelladresse gültig
127.0.0.0/8	127.0.0.0 – 127.255.255.255	Loopback-Adressen
169.254.0.0/16	169.254.0.0 – 169.254.255.255	Link-local-Adressen (APIPA)
192.0.2.0/24	192.0.2.0 – 192.0.2.255	TEST-NET-1 Dokumentation
198.51.100.0/24	198.51.100.0 – 198.51.100.255	TEST-NET-2 Dokumentation
203.0.113.0/24	203.0.113.0 - 203.0.113.255	TEST-NET-3 Dokumentation
224.0.0.0/4	224.0.0.0 – 239.255.255.255	Multicast-Adressen
240.0.0.0/4	240.0.0.0 – 255.255.255.254	Reserviert
255.255.255.255	255.255.255.255	Broadcast-Adresse

Aus den übrigen IPv4 Adressen ergeben sich die öffentlichen Adressbereiche. Da IPv4-Adressen begrenzt sind müssen dies offiziell beantragt und zugeteilt werden. Man kann also nicht irgendeine Adresse verwenden.
Die Adressvergabe folgte ursprünglich einer regionalen Hierarchie. Das heißt, der IPv4-Adressraum wurde in Regionen aufgeteilt. Man hat dazu Regional Internet Registries (RIR) mit der Aufgabe betraut IPv4-Adressen zu vergeben. In Europa und dem Mittleren Osten ist dafür das RIPE NCC zuständig. **Alle verfügbaren öffentlichen IPv4-Adressen sind ausgeschöpft!**

Kenntnisse über IPv6-Adressierung

Was ist IPv6?

IPv6 (Internet Protocol Version 6) ist der Nachfolger von IPv4 und wurde entwickelt, um die Adressenknappheit im Internet zu lösen. IPv6 bietet eine deutlich größere Adresskapazität sowie moderne Funktionen für Routing, Sicherheit und Autokonfiguration.

Unterschiede zu IPv4

MERKMAL	IPV4	IPV6
ADRESSLÄNGE	32 Bit – 4 Oktette	128 Bit – 8 Blöcke à 16 Bit
SCHREIBWEISE	Dezimal – 192.168.0.10	Hexadezimal – 2001:0db8:85a3::1
ADRESSANZAHL	~4,3 Milliarden	3,4 x 10^{38} - 340 Sextillionen
NAT NOTWENDIG?	Ja	Nein - direkte globale Adressen möglich
BROADCAST	Ja	Nein - stattdessen Multicast
SICHERHEITSFUNKTIONEN	Zusatzoption	Integriert - IPsec

Aufbau einer IPv6-Adresse

- IPv6-Adressen bestehen aus 8 Gruppen zu je 4 hexadezimalen Zeichen
- Wird durch **:** getrennt
- Beispiel:
  2001:0db8:0000:0000:0000:ff00:0042:8329

Vereinfachungsregeln

- Führende Nullen dürfen weggelassen werden:
  2001:0db8 → 2001:db8
- Längere Nullblöcke können durch **::** ersetzt werden (nur einmal pro Adresse erlaubt):
  2001:db8:0:0:0:0:1 → 2001:db8::1

Adressbereiche und Typen

TYP	BEREICH (PRÄFIX)	VERWENDUNG
UNICAST	z.B. 2000::/3	Einzelner Host – wie IPv4 Adresse
MULTICAST	FF00::/8	Kommunikation mit mehreren Hosts gleichzeitig
ANYCAST	Je nach Konfiguration	Gleiche Adresse auf mehreren Geräten – nächstgelegenes wird verwendet
LINK-LOCAL	FE80::/10	Automatische Kommunikation im lokalen Netz – z.B. Router suchen
UNIQUE LOCAL	FC00::/7	Vergleichbar mit privaten IPv4-Adressen
LOOPBACK	::1	Entspricht 127.0.0.1 in IPv4

Zuweisung von IPv6-Adressen

- SLAAC – Stateless Address Autoconfiguration
- DHCPv6 – dynamisch wie IPv4
- Manuelle Konfiguration

Sicherheitsaspekte bei IPv6

- IPsec ist integraler Bestandteil
- Kein NAT notwendig, daher direkter Zugriff auf Geräte – Firewall ist Pflicht!
- Eindeutige globale Erreichbarkeit erleichtert Angriffe, aber auch Routing

Unterscheidung von public/private IP-Adressen

Private IP-Adressen (RFC 1918)

Diese Adressbereiche sind nicht im Internet geroutet, sondern nur für lokale Netzwerke vorgesehen. Sie sind beliebig oft verwendbar in unterschiedlichen privaten Netzen, müssen jedoch per NAT (Network Address Translation) umgesetzt werden um mit dem Internet kommunizieren zu können.

Public IP-Adressen

- Werden von Internetdienstanbietern (ISPs) zugewiesen
- Müssen weltweit eindeutig sein
- Beispiel: 142.251.37.3 (google.at)
- Nur Geräte mit Public IPs sind direkt über das Internet erreichbar
- Meist erhält der Router eine Public IP, die per NAT auf interne Geräte gemappt wird

Kenntnis der privaten IP-Adress-Bereiche

KLASSE	ADRESSBEREICH	CIDR-NOTATION	HOSTS
KLASSE A	10.0.0.0 – 10.255.255.255	/8	16.777.216
KLASSE B	172.16.0.0 – 172.31.255.255	/12	1.048.576
KLASSE C	192.168.0.0 – 192.168.255.255	/16	65.536

Fachbegriff MAC-Adresse und deren Aufbau

Die MAC-Adresse (Media Access Control Address) ist eine weltweit eindeutige Hardwareadresse einer Netzwerkschnittstelle (z. B. LAN, WLAN). Sie dient zur Identifikation eines Geräts im lokalen Netzwerk (Layer 2).
Jede Netzwerkkarte (NIC) hat ab Werk eine MAC-Adresse – vergleichbar mit einem "Fingerabdruck" des Geräts im Netzwerk.

Die MAC-Adresse arbeitet auf der OSI-Schicht 2 (Sicherungsschicht / Data Link) und wird von Switches genutzt zur zielgerichteten Weiterleitung von Frames. Durch das ARP-Protokoll (Address Resolution Protocol) wird zu einer IP-Adresse die zugehörige MAC-Adresse ermittelt. DHCP-Server nutzen ebenfalls die MAC-Adresse um gezielt IP-Adressen vergeben zu können.

Aufbau einer MAC-Adresse

- 48 Bit = 6 Byte
- Darstellung in Hexadezimaler Schreibweise
- Besteht aus 6 Gruppen zu je 2 Zeichen, getrennt durch **:** oder **-**
  Beispiel: 00:1A:2B:3C:4D:5E
- Die ersten drei Gruppen sind zur Herstellererkennung (OUI – Organizationally Unique Identifier)
- Die letzten drei Gruppen sind die Gerätespezifische Seriennummer (eindeutig innerhalb des Herstellers)
- Beispiel: 00:1B:44:11:3A:B7
  - 00:1B:44 → OUI
  - 11:3A:B7 → Seriennummer

Fachbegriff Ethernet

Definition

Ethernet ist ein standardisiertes Verfahren für die Verkabelung, Datenübertragung und Zugriffssteuerung in lokalen Netzwerken (LANs). Es legt fest, wie Geräte Daten austauschen, und ist heute die am weitesten verbreitete LAN-Technologie weltweit.

Ethernet definiert physikalische Verbindungen (Kabel, Stecker) und logische Übertragung (z. B. Paketstruktur, Zugriffsverfahren).

Technischer Aufbau

KOMPONENTE	BESCHREIBUNG
OSI-SCHICHT	Layer 1 (Physikalisch) & Layer 2 (Data Link)
STANDARD	IEEE 802.3
ADRESSIERUNG	Verwendet MAC-Adressen
ZUGRIFFSVERFAHREN	CSMA/CD (nur bei Hubs, Halbduplex)
ÜBERTRAGUNGSMEDIEN	Twisted Pair (Cat6, Cat7, Cat8), Glasfaser

Übertragungsgeschwindigkeiten – Ethernet-Standards

STANDARD	BEZEICHNUNG	DATENRATE	MEDIUM
10BASE-T	Ethernet	10 Mbit/s	Twisted Pair Cat3
100BASE-TX	Fast Ethernet	100 Mbit/s	Twisted Pair Cat5
1000BASE-T	Gigabit Ethernet	1 Gbit/s	Twisted Pair Cat5e/6
10GBASE-T	10-Gigabit	10 Gbit/s	Twisted Pair Cat6a/7
1000BASE-LX	Gigabit Ethernet	1Gbit/s	Glasfaser

Wichtige Eigenschaften

- **Vollduplexbetrieb:** Daten können gleichzeitig gesendet und empfangen werden
- **Nicht routingfähig:** funktioniert innerhalb eines lokalen Segments
- **Switched Ethernet:** ersetzt ältere Hubs – keine Kollisionen mehr
- **Broadcast-basiert:** z.B. für ARP oder DHCP-Requests

Typische Komponenten

- Netzwerkkarten (NICs)
- Twisted Pair-Kabel mit RJ45 Stecker
- Switches (Layer 2)
- Access Points (bei Wireless Ethernet / IEEE 802.11)

Fachbegriff xDSL

Definition

xDSL steht für „Digital Subscriber Line“ und bezeichnet eine Familie von Technologien, die digitale Datenübertragung über bestehende Kupfertelefonleitungen ermöglichen.

Das „x“ steht dabei als Platzhalter für verschiedene DSL-Varianten wie ADSL, VDSL, SDSL usw.

Grundprinzip

- DSL nutzt Frequenzbereiche oberhalb der analogen Telefonie, sodass gleichzeitiges Telefonieren und Internetsurfen möglich ist (Split-Technologie).
- Es handelt sich um eine punkt-zu-punkt Verbindung vom Modem zum DSLAM (Digital Subscriber Line Access Multiplexer) beim Anbieter.

Wichtige DSL-Varianten im Überblick

VARIANTE	BEZEICHNUNG	EIGENSCHAFT	VERWENDUNG
ADSL	Asymmetric DSL	Download schneller als Upload	Heimanwender, Standard-DSL
SDSL	Symmetric DSL	Gleich hohe Up-/Downloadraten	Firmen mit Upload-Bedarf
VDSL	Very High Bitrate DSL	Höhere Geschwindigkeiten, kürzere Leitungslänge	FTTC (Fibre to the Curb)
VDSL2	Erweiterung von VDSL	Bis zu 100 Mbit/s	Moderne Breitbandanschlüsse
G.FAST	Nachfolger von VDSL2	Gigabit-Übertragung über kurze Kupferleitungen	Hochgeschwindigkeitszugänge

Typische Eigenschaften

- Nutzt bestehende Infrastruktur (Telefonnetz)
- Störanfällig bei langen Kupferleitungen (> 1 km)
- Begrenzt in Geschwindigkeit gegenüber Glasfaser
- Upload meist deutlich geringer als Download (außer bei SDSL)

Unterscheidung der Fachbegriffe Upload, Download

Definitionen

Download:
Übertragung von Daten aus dem Internet bzw. einem entfernten Server zum eigenen Gerät. Beispiel: Datei aus dem Internet laden.

Upload:
Übertragung von Daten vom eigenen Gerät ins Internet bzw. zu einem Server. Beispiel: Datei in die Cloud oder auf YouTube hochladen.

Vergleichstabelle: Download vs. Upload

KRITERIUM	DOWNLOAD	UPLOAD
DATENRICHTUNG	Vom Server zum lokalen Gerät	Vom lokalen Gerät zum Server
TYPISCHE NUTZUNG	Webseiten ansehen, Filme streamen, Softwaredownload	E-Mails versenden, Dateien teilen, Video-Uploads
GESCHWINDIGKEIT	Meist schneller als Upload (asymmetrisch)	Oft langsamer, besonders bei ADSL
BEISPIEL	YouTube-Video schauen	YouTube-Video hochladen
MESSUNG	Mbit/s oder Kbit/s	Mbit/s oder Kbit/s

Fachbegriff WLAN

Definition

WLAN steht für Wireless Local Area Network und bezeichnet ein drahtloses lokales Netzwerk, bei dem Endgeräte wie Notebooks, Smartphones, Drucker oder IoT-Geräte ohne Kabelverbindung über Funk kommunizieren.

WLAN ist die drahtlose Variante eines LANs und basiert auf dem IEEE-Standard 802.11.

Grundlagen und Eigenschaften

MERKMAL	BESCHREIBUNG
STANDARD	IEEE 802.11 (a/b/g/n/ac/ax)
FREQUENZBEREICHE	2,4 GHz und 5 GHz (neu: 6 GHz bei Wi-Fi 6E)
ÜBERTRAGUNGSMEDIEN	Funkwellen (Funknetz)
GESCHWINDIGKEIT	Bis 600 Mbit/s (WiFi 4), 1300 Mbit/s (WiFi 5), >1000 Mbit/s (WiFi 6)
TYPISCHES GERÄT	Access Point / WLAN-Router
ADRESSIERUNG	Verwendet MAC- und IP-Adressen
TOPOLOGIE	Stern (logisch – alle Geräte verbinden sich mit dem Access Point)

Wichtige WLAN-Standards im Vergleich

STANDARD	MAX. DATENRATE	FREQUENZ	BEMERKUNG
802.11B	11 Mbit/s	2,4 GHz	Veraltet
802.11G	54 Mbit/s	2,4 GHz	Ältere Geräte
802.11N (WIFI 4)	600 Mbit/s	2,4 + 5 GHz	Weit verbreitet
802.11AC (WIFI 5)	1,3 Gbit/s	5 GHz	Sehr schnell, aktuelle Geräte
802.11AX (WIFI 6)	>9 Gbit/s	2,4/5/6 GHz	Neuester Standard, effizient

Komponenten eines WLANs

- **Access Point (AP):** Zentrale Funkstation, über die Clients kommunizieren
- **WLAN-Router:** Meist Kombination aus AP, Switch und Router
- **Endgeräte:** Notebooks, Smartphones, Smart-Home-Geräte etc.
- **Repeater:** Verstärken das Signal, um größere Flächen abzudecken

Sicherheit im WLAN

MAßNAHME	BESCHREIBUNG
WPA2 / WPA3	Verschlüsselung des Datenverkehrs
SSID-HIDING	Verstecken des Netzwerknamens
MAC-FILTER	Nur erlaubte Geräte dürfen sich verbinden
FIREWALL & ISOLATION	Schützt vor fremden Zugriffen innerhalb des Netzes

Fachbegriff Access-Point

Definition

Ein Access Point (AP) ist ein Gerät, das drahtlose Endgeräte (z. B. Smartphones, Laptops, Drucker) mit einem verkabelten LAN-Netzwerk verbindet. Er stellt die zentrale Funkzelle eines WLANs dar.

Der Access Point funktioniert wie eine drahtlose "Steckdose" fürs Netzwerk – alle WLAN-Geräte verbinden sich über ihn mit dem Netzwerk und ggf. dem Internet.

Funktion und Aufbau

EIGENSCHAFT	BESCHREIBUNG
OSI-SCHICHT	Schicht 2 (Data Link) + teilweise Layer 1
VERBINDUNG	Funk (WLAN) zu Clients + LAN-Kabel zu Switch/Router
ADRESSIERUNG	MAC-Adressen (für Frame-Weiterleitung)
NETZSEGMENT	Schafft eine eigene Funkzelle (WLAN)
VERWALTUNG	Entweder standalone oder zentral per WLAN-Controller

Typen von Access Points

TYP	BESCHREIBUNG
STANDALONE-AP	Einzelgerät, direkt konfigurierbar
INTEGRIERT IM ROUTER	WLAN-Router (Heimnetz) enthält AP, Switch & Routerfunktionen
CONTROLLER-BASIERTER AP	In großen WLANs zentral verwaltet über WLAN-Controller
REPEATER-MODUS	Einige APs können als Signalverstärker (WLAN-Repeater) fungieren

Sicherheitsfunktionen (je nach Gerät)

- SSID-Konfiguration (Netzwerkname sichtbar/versteckt)
- WPA2/WPA3-Verschlüsselung
- MAC-Filterung
- Client-Isolation (Gäste voneinander trennen)
- Band Steering (optimiert 2,4 GHz vs. 5GHz-Verbindung)

6.2 Netzwerkdienste

Aufbau eines Active-Directorys

Definition

Active Directory (AD) ist ein von Microsoft entwickter Verzeichnisdienst, der in Netzwerken mit Windows-Servern zur zentralen Verwaltung von Benutzern, Computern, Gruppen, Rechten und Ressourcen dient.

Active Directory ist das „Gehirn“ eines Windows-Netzwerks – alle Benutzer- und Geräteinformationen werden dort gespeichert und verwaltet. Active Directory ist hierarchisch organisiert – vom kleinsten Objekt bis zur Gesamtstruktur.

1. Objekte

Die kleinste Einheit – jedes Element im AD ist ein Objekt.

OBJEKT-TYP	BEISPIEL
BENUTZER	Max Mustermann
COMPUTER	CLIENT-01
GRUPPE	IT-Abteilung, Schüler
DRUCKER	Drucker-01
FREIGABE	\SERVER\Daten

2. Organisationseinheiten (OU)

OUs dienen der logischen Gruppierung von Objekten, z.B. nach Abteilung oder Standort.

- Beispiel: OU=Schule, OU=Lehrer, OU=Schüler
- Ermöglicht delegierte Verwaltung und Gruppenrichtlinien (GPOs)

3. Domäne (Domain)

Eine Domäne ist die zentrale Verwaltungseinheit im AD mit gemeinsamer Benutzer-Datenbank.

- Beispiel: schule.local, firma.at
- Alle Benutzer und Geräte werden in der Domäne authentifiziert
- Wird von einem Domain Controller (DC) verwaltet

4. Baum (Tree)

Mehrere Domänen mit gemeinsamen Namensraum.
Beispiel:

- firma.local
    - it.firma.local

5. Gesamtstruktur (Forest)

Größte Einheit – mehrere Bäume mit unterschiedlichen Namensräumen, aber gemeinsamer Vertrauensstellung.

- Wird durch die erste Domäne installiert
- Enthält das globale Katalogverzeichnis

Wichtige Rollen im AD

- **Domain Controller (DC):** Führt Authentifizierung und Verwaltung durch
- **Globaler Katalogserver:** Hält Teilinformationen aller Objekte
- **FSMO-Rollen:** Verantwortlich für spezielle AD-Funktionen (z. B. Schema-Master, RID-Master)

Wichtige Funktionen von AD

- **Benutzerauthentifizierung:** Anmeldung an Domäne durch Benutzername & Passwort
- **Gruppenrichtlinien (GPO):** Steuerung von Benutzer- und Rechnerverhalten zentral
- **Zugriffssteuerung (ACL):** Verwaltung von Rechten auf Dateien, Ordner, Drucker
- **LDAP (Protokoll):** Zugriff und Suche innerhalb des Verzeichnisses

Funktionsprinzip eines Domain-Controllers

Definition

Ein Domain Controller ist ein Windows-Server, der innerhalb einer Active Directory (AD)-Domäne die zentrale Rolle übernimmt. Er ist verantwortlich für die Benutzerauthentifizierung, Verzeichnisverwaltung und die Durchsetzung von Gruppenrichtlinien (GPOs).

Kurz gesagt: Der DC ist das Herzstück der Domäne. Ohne ihn ist keine zentrale Anmeldung, keine Benutzerverwaltung und keine sichere Ressourcenfreigabe möglich.

Hauptaufgaben eines Domain Controllers

- **Authentifizierung:** Benutzer melden sich zentral am Netzwerk an – der DC prüft Benutzername, Passwort, Gruppenmitgliedschaften
- **Benutzer- & Computerverwaltung:** Verwalten von Benutzern, Gruppen, Computern, Druckern usw. im Active Directory
- **Gruppenrichtlinien anwenden:** Verteilen von Regeln und Einstellungen auf Benutzer und Geräte (z. B. Druckerzuweisung, Softwareverteilung)
- **Rechte- und Zugriffssteuerung:** Zentrale Vergabe von Dateiberechtigungen, Anmelderechten usw.
- **DNS-Integration:** Meist als interner DNS-Server im Einsatz – löst Namen zu IP-Adressen auf
- **Replikation bei mehreren DCs:** Synchronisation zwischen mehreren Domain Controllern (z. B. in großen Netzen)

Technische Komponenten

- **Active Directory Domain Services (AD DS):** Zentrale Rolle auf dem DC – stellt den Verzeichnisdienst bereit
- **NTDS.dit:** AD-Datenbankdatei mit allen Informationen über Benutzer, Gruppen etc.
- **SYSVOL:** Freigabe mit Skripten und Gruppenrichtlinien
- **Kerberos:** Standard-Authentifizierungsprotokoll in der Domäne
- **LDAP:** Zugriff auf das Verzeichnis (z. B. Suchanfragen von Programmen)

Ablauf einer Anmeldung (vereinfacht)

1. Benutzer gibt Benutzername + Passwort ein
2. Der Client kontaktiert den Domain Controller
3. Der DC prüft die Zugangsdaten über Kerberos
4. Bei Erfolg wird ein Token mit Gruppenmitgliedschaften übermittelt
5. Zugriff auf Ressourcen wird auf Basis dieses Tokens geprüft

Sicherheitsfunktionen

- Zentralisierte Anmeldung = einheitliches Rechte- und Benutzerkonzept
- Absicherung durch GPOs (z. B. Passwortregeln, Desktop-Richtlinien)
- Mehrere DCs erhöhen Verfügbarkeit (Redundanz durch Replikation)
- Möglichkeit zur Delegierung von Verwaltungsrechten (z. B. Admin für nur eine OU)

Kenntnisse über den Netzwerkdienst DHCP

Definition

DHCP ist ein Netzwerkdienst, der Geräten in einem IP-Netzwerk automatisch Konfigurationsdaten zuweist – insbesondere eine IP-Adresse, Subnetzmaske, Gateway und DNS-Server. Ohne DHCP müsste jeder Rechner im Netzwerk manuell konfiguriert werden – DHCP automatisiert diesen Prozess.

DHCP liefert dem Client automatisch:

- IP-Adresse
- Subnetzmaske
- Standard-Gateway (Routeradresse)
- DNS-Server-Adresse
- (Optional: WINS-Server, Lease-Zeit etc.)

Ablauf der DHCP-Adressvergabe (DORA)

1. **DHCPDISCOVER:** Client sendet Broadcast: „Wer kann mir eine IP geben?“
2. **DHCPOFFER:** DHCP-Server bietet eine IP-Adresse an
3. **DHCPREQUEST:** Client fordert die angebotene IP-Adresse offiziell an
4. **DHCPACK:** Server bestätigt und stellt Konfigurationsdaten bereit

DHCP-Konfigurationsbegriffe:

- **Scope / Bereich:** Definiert den IP-Adressbereich, aus dem Adressen vergeben werden (z. B. 192.168.0.100–192.168.0.200)
- **Lease-Zeit:** Zeitraum, wie lange eine IP-Adresse gültig ist
- **Reservation:** Statische Zuweisung einer bestimmten IP zu einer bestimmten MAC-Adresse
- **Exclusion Range:** Adressen, die nicht automatisch vergeben werden dürfen (z. B. für Drucker, Server)

Sicherheitsaspekte

- DHCP ist nicht authentifiziert – jeder Client im Netz könnte Anfragen senden.
- In Firmennetzwerken: DHCP-Snooping auf Switches aktiviert → blockiert gefälschte Server.
- Rogue DHCP Server = Sicherheitsrisiko (z. B. im WLAN)

Funktionsprinzip eines Proxy-Servers

Definition

Ein Proxy-Server (auch Zwischenspeicher- oder Vermittlungsserver) ist ein vermittelnder Server zwischen einem Client (z. B. PC) und einem Zielserver (z. B. Webseite). Er nimmt Anfragen des Clients entgegen, verarbeitet sie weiter und gibt die Antworten zurück – teils verändert oder gefiltert.

Der Proxy „vertritt" den Client gegenüber dem Internet und kann dabei Zugriffe steuern, beschleunigen oder protokollieren.

Funktionsweise eines Proxy-Servers (vereinfacht)

1. Client sendet eine Anfrage an den Proxy (z. B. Öffne www.beispiel.at)
2. Proxy prüft:
    a. Ist die Seite erlaubt? (Filter)
    b. Ist sie im Cache gespeichert? (Beschleunigung)
3. Proxy ruft ggf. die Webseite ab, speichert sie (Caching), filtert ggf. Inhalte
4. Gibt die Antwort zurück an den Client

Arten von Proxy-Servern

- **Forward Proxy:** Vermittelt Client - Internet (häufig in Schulen, Firmen)
- **Reverse Proxy:** Vermittelt Internet - interner Server (z. B. bei Webservern)
- **Transparenter Proxy:** Funktioniert ohne Client-Konfiguration, im Hintergrund aktiv
- **Caching Proxy:** Speichert Webinhalte lokal zwischen, um Ladezeiten zu verkürzen
- **Filter-Proxy:** Blockiert z. B. bestimmte Webseiten, Inhalte oder Dateitypen

Typische Einsatzgebiete

- **Unternehmen:** Zugangskontrolle & Protokollierung von Internetzugriffen
- **Schulen:** Jugendschutz durch Inhaltsfilter
- **Provider:** Caching zur Lastreduzierung
- **Webserver:** Lastverteilung durch Reverse Proxies

Sicherheits- & Datenschutzfunktionen:

Anonymisierung: Die Zielseite sieht nur die IP des Proxyservers

Zugriffskontrolle: Nur berechtigte Nutzer dürfen auf bestimmte Seiten zugreifen

Inhaltsfilterung: Sperrung von Websites nach Kategorie, Adresse, Inhalt

Protokollierung (Logging): Nachvollziehbarkeit von Nutzeranfragen

Funktionsprinzip eines Webservers

Definition

Ein Webserver ist ein Gerät (oder Software), welches Webseiteninhalte (HTML, CSS, Bilder, Skripte etc.) auf Anfrage an Clients (meist Webbrowser) über das Internet oder Intranet bereitstellt – typischerweise über das HTTP- oder HTTPS-Protokoll.

Ein Webserver reagiert auf Anfragen von Webbrowsern und liefert Inhalte für Webseiten aus.

Funktionsweise eines Webservers (vereinfacht)

1. Client (Browser) sendet eine HTTP/HTTPS-Anfrage an den Webserver
2. Webserver verarbeitet die Anfrage
    a. Prüft Pfad, Datei, Berechtigungen
    b. Startet ggf. Skripte (PHP, ASP.NET, usw.)
3. Antwort wird als HTTP(S)-Response zurückgegeben

Typische Webserver-Software

NAME	PLATTFORM	BESCHREIBUNG
APACHE	Windows/Linux	Meistverbreitete Open-Source-Lösung
NGINX	Linux	Leistungsstark, auch als Reverse Proxy
MICROSOFT IIS	Windows Server	Integriert in Windows Server OS
LIGHTTPD	Linux	Leichtgewichtiger Server für kleinere Sites

Erweiterte Funktionen eines Webservers

- Unterstützung dynamischer Inhalte: z. B. durch PHP, Python, .NET
- Session-Verwaltung
- SSL-Zertifikate (für HTTPS)
- Zugriffsprotokollierung (Access Logs)
- Authentifizierung und Zugriffsschutz

Kenntnis des DNS-Dienstes und dessen hierarchischen Aufbaues

Definition

Das DNS (Domain Name System) ist ein hierarchisches Namensauflösungssystem, das menschenlesbare Domainnamen (z. B. www.schule.at) in maschinenlesbare IP-Adressen (z. B. 213.33.98.1) übersetzt – und umgekehrt.

DNS ist quasi das „Telefonbuch des Internets“ – es sorgt dafür, dass dein Browser weiß, welche IP-Adresse zu einem Webserver gehört.

Eine komplette Adresse wie www.schule.at wird als Fully Qualified Domain Name **(FQDN)** bezeichnet.

Funktionsweise von DNS (vereinfacht)

1. Der Benutzer gibt www.schule.at im Browser ein.
2. Der Rechner fragt beim lokalen DNS-Resolver (z. B. Router, Provider).
3. Falls unbekannt, wird die Anfrage rekursiv bis zum zuständigen Nameserver weitergeleitet.
4. Der DNS-Server antwortet mit der IP-Adresse.
5. Der Browser verbindet sich mit dem Webserver.

Hierarchischer Aufbau des DNS-Systems

DNS ist bauförmig aufgebaut – jede Ebene im Namen entspricht einer Hierarchieebene im System.
Aufbau von rechts nach links:

EBENE	BEISPIEL	FUNKTION
ROOT-ZONE	.	Ausgangspunkt aller Domains („leere“ Ebene)
TOP-LEVEL-DOMAIN	.com, .org, .at	Länder- oder generische Domains
SECOND-LEVEL-DOMAIN	Google, wko, orf	Eigentliche Domain des Anbieters
SUBDOMAIN	www, mail, dns	Unterstruktur, z.B. Dienste oder Abteilungen
REKURSIVE ADRESSE	www.google.com	Vollständiger Domainname (FQDN)

Arten von DNS-Servern

TYP	AUFGABE
ROOT-NAMESERVER	Verweisen auf TLD-Nameserver
TLD-SERVER	Verweisen auf autoritative Nameserver
AUTHORITATIVER NAMESERVER	Enthält die echten Zuweisungen für Domains
CACHING RESOLVER	Zwischenspeichert Anfragen zur Beschleunigung
LOKALER DNS-SERVER	Meist am Router oder im Firmen-LAN

Wichtige DNS-Einträge (Resource Records)

TYP	BEDEUTUNG	BEISPIEL
A	IPv4-Adresse einer Domain	example.com – 93.184.216.34
AAAA	IPv6-Adresse einer Domain	example.com – 2606:2800::…
CNAME	Alias für eine andere Domain	mail.example.com – google.com
MX	Mailserver-Zuordnung	E-Mail an @example.com – Server X
NS	Delegation an Nameserver	Example.com wird verwaltet von ns1.xyz.net
PTR	Rückwärtsauflösung (IP-Name)	93.184.216.34 – example.com

Sicherheitsaspekte

- DNS-Antworten sind nicht verschlüsselt (Risiko: DNS-Spoofing)
- DNSSEC sichert DNS-Einträge kryptografisch ab
- Moderne Erweiterungen wie DoH (DNS over HTTPS) und DoT (DNS over TLS) verschlüsseln DNS-Anfragen

Fachbegriffe Domain, Sub-Domain und Top-Level-Domain

Top-Level-Domain (TDL)

Die TDL ist der oberste Teil einer Domain – sie steht ganz rechts in einem Domainnamen und bezeichnet die Hauptkategorie oder Region, zu der eine Domain gehört.

Arten von TDLs:

TYP	BEISPIELE	BESCHREIBUNG
GENERISCHE	.com, .org, .net, .info	Allgemeine Domains, weltweit nutzbar
LÄNDERSPEZIFISCH	.at, .de, .us, ….	Für nationale Domains
NEUE TDL	.shop, .tech, .berlin	Seit 2014 möglich, themenspezifisch

Subdomain

Eine Subdomain ist ein Teilbereich einer bestehenden Domain und wird vor der Hauptdomain gesetzt. Sie dient dazu, Dienste oder Abteilungen logisch zu trennen – etwa mail.google.com oder www.bmvit.gv.at.

DOMAINNAME	SUBDOMAIN	DOMAIN	TDL
WWW.GOOGLE.COM	www	Google	.com
MAIL.SCHULE.WIEN.GV.AT	mail.schule	wien.gv	.at
FTP.UNI-GRAZ.AC.AT	ftp	uni-graz	.ac.at

Kenntnis der Web-Protokolle HTTP und HTTPS

Was ist HTTP?

HTTP (HyperText Transfer Protocol) ist ein Anwendungsprotokoll, das verwendet wird, um Webseiten, Bilder, Videos und andere Webinhalte zwischen Webserver und Webbrowser zu übertragen.

- Es arbeitet nach dem Client-Server-Prinzip
- Der Client (Browser) sendet eine Anfrage (Request), der Server antwortet mit einer Antwort (Response)

Beispiel: Man gibt www.wko.at in einem Browser ein → der Browser stellt eine HTTP-Anfrage an den Webserver → dieser sendet die Website als HTML-Daten zurück.

Was ist HTTPS?

HTTPS (HyperText Transfer Protocol Secure) ist die verschlüsselte Version von HTTP. Es schützt die übertragenen Daten durch eine TLS/SSL-Verschlüsselung, damit sie nicht abgehört oder manipuliert werden können. Die meisten Webseiten werden über HTTPS abgerufen.

HTTP/HTTPS-Vergleichstabelle

MERKMAL	HTTP	HTTPS
VERSCHLÜSSELUNG	Keine	TLS/SSL
SICHERHEIT	Niedrig (anfällig für Abhören)	Hoch (vertraulich & authentisch)
STANDARD-PORT	80	443
URL-BEGINN	http://	https://
ZERTIFIKAT NÖTIG	Nein	Ja – X.509-Zertifikat vom CA
VERWENDUNG	Öffentlich zugängliche Seiten	Login-Formulare, Bezahldienste

Wie funktioniert HTTPS?

1. Browser verbindet sich mit Webserver auf Port 443.
2. Server sendet SSL-Zertifikat zur Identifikation.
3. Browser prüft das Zertifikat (Gültigkeit, Herausgeber).
4. Gemeinsamer Sitzungsschlüssel wird ausgehandelt (TLS-Handshake).
5. Danach erfolgt die verschlüsselte Kommunikation.

Wichtige Begriffe:

- **TLS/SSL:** Verschlüsselungsprotokoll für sichere Kommunikation
- **CA (Certificate Authority):** Zertifizierungsstelle, stellt HTTPS-Zertifikate aus
- **Zertifikat:** Digitale Ausweisdatei mit Serveridentität & Schlüssel

Funktionsprinzip eines Mail-Servers

Ein Mail-Server ist ein Server, der E-Mails entgegennimmt, speichert, weiterleitet und zustellt. Es gibt:

- Postausgangsserver (SMTP-Server) → versendet E-Mails
- Posteingangsserver (IMAP/POP3-Server) → stellt empfangene E-Mails bereit

Ein Mailserver besteht aus mehreren Diensten und Protokollen, die zusammenarbeiten, um den reibungslosen E-Mail-Verkehr zwischen Absendern und Empfängern zu ermöglichen – sowohl innerhalb eines lokalen Netzwerks als auch im Internet.

Ablauf des E-Mail-Versands (vereinfacht)

1. Benutzer schreibt E-Mail im E-Mail-Client (z. B. Outlook, Thunderbird)
2. Der Client sendet die Nachricht über SMTP an den Mailserver des Absenders
3. Der Mailserver sucht per DNS (MX-Eintrag) den Mailserver des Empfängers
4. Die Nachricht wird über SMTP zum Empfänger-Mailserver übertragen
5. Der Empfänger ruft die Mail via IMAP oder POP3 ab

Protokolle und ihre Aufgaben

PROTOKOLL	FUNKTION
SMTP (SIMPLE MAIL TRANSFER PROTOCOL)	Überträgt E-Mails vom Absender zum Mailserver und zwischen Servern
IMAP (INTERNET MESSAGE ACCESS PROTOCOL)	E-Mails bleiben auf dem Server, Client greift online darauf zu.
POP3	E-Mails werden vom Server heruntergeladen und lokal gespeichert

Mailserver-Komponenten

KOMPONENTE	FUNKTION
SMTP-DIENST	Versand & Weiterleitung von Mails
IMAP-/POP3-DIENST	Empfang der Nachrichten durch Benutzer
MAIL TRANSFER AGENT (MTA)	Verantwortlich für Routing von Mails
MAIL DELIVERY AGENT (MDA)	Legt Mails im Postfach des Empfängers ab
MAIL USER AGENT (MUA)	Der Mailclient (z.B. Outlook)

Sicherheitsaspekte

- **Authentifizierungspflicht** bei SMTP (SMTP-AUTH)
- **TLS-Verschlüsselung** für SMTP, IMAP & POP3 - schützt Inhalte vor Mitlesen
- **Spam-Filter** und **Virenscanner** direkt am Mailserver
- **DNS-Einträge (MX, SPF, DKIM, DMARC)** - schützen vor Spam und Spoofing

Kenntnis der Mailprotokolle POP3/POP3S, IMAP/IMAPS und SMTP/SMTPS

POP3 – Post Office Protocol v3

POP3 wird verwendet, um E-Mails vom Mailserver auf ein Endgerät herunterzuladen. Danach werden die Mails auf dem Server meist gelöscht (Standardverhalten).

Merkmale:

- Einfaches Protokoll, offline-orientiert
- Kein zentraler Mail-Sync über mehrere Geräte
- Lokale Speicherung der Nachrichten
- Port: 110

POP3S (verschlüsselt):

- Nutzung von TLS/SSL-Verschlüsselung
- Port: 995

IMAP – Internet Message Access Protocol

IMAP erlaubt es, E-Mails direkt auf dem Server zu verwalten, ohne sie herunterzuladen. Ideal für den Zugriff über mehrere Geräte (z. B. Laptop, Smartphone).

Merkmale:

- Serverbasierte Mailverwaltung
- E-Mails und Ordnerstruktur bleiben auf dem Server
- Änderungen werden synchronisiert (z. B. „Gelesen“-Status)
- Port: 143

IMAPS (verschlüsselt):

- Nutzung von TLS/SSL-Verschlüsselung
- Port: 993

SMTP – Simple Mail Transfer Protocol

SMTP wird für den Versand von E-Mails verwendet – vom Mailclient zum Server und zwischen Mailservern.

Merkmale:

- Einfache Weiterleitung von Mails
- Keine Abfrage-Funktion (nur Versand!)
- Unterstützt Authentifizierung (SMTP AUTH)
- Port: 25

SMTPS (verschlüsselt):

- Verschlüsselte Übertragung über TLS
- Ports: SMTPS - 465 oder SMTP-AUTH – 587

Kenntnisse über FTP/FTPS

Was ist FTP?

FTP (File Transfer Protocol) ist ein standardisiertes Protokoll, mit dem Dateien zwischen einem Client und einem Server übertragen werden. Es basiert auf dem Client-Server-Modell.

Funktionen:

- Dateien hoch- und herunterladen
- Verzeichnisse auflisten
- Umbenennen, löschen, verschieben von Dateien

Ports:

FUNKTION	PORT
STEUERVERBINDUNG	21
DATENVERBINDUNG	Dynamisch/Port 20 bei aktivem Modus

FTP ist unverschlüsselt! → Passwörter & Dateien werden **im Klartext** übertragen!

Was ist FTPS (FTP Secure)?

FTPS ist eine erweiterte, verschlüsselte Version von FTP, bei der die Kommunikation mit TLS/SSL gesichert wird.

Varianten:

- **Explicit FTPS:** Verbindung beginnt unverschlüsselt, dann Wechsel auf TLS
- **Implicit FTPS:** Verbindung startet direkt verschlüsselt (veraltet, aber noch im Einsatz)

Ports:

VARIANTE	PORT
EXPLICIT FTPS	21
IMPLICIT FTPS	990

Wie funktioniert eine FTP/FTPS-Verbindung?

1. Verbindungsaufbau: Der Client stellt eine Verbindung zum Server her (Port 21).
2. Authentifizierung: Benutzername und Passwort werden gesendet.
3. Übertragung: Dateien werden über die Datenverbindung ausgetauscht.
4. Bei FTPS: TLS wird aktiviert → Daten & Anmeldedaten werden verschlüsselt.

Kenntnisse über SSL

Definition:

SSL (Secure Sockets Layer) ist ein Kryptoprotokoll, dass die verschlüsselte Kommunikation zwischen zwei Geräten (meist Client und Server) über ein Netzwerk ermöglicht – insbesondere im Internet.

Hauptzweck: Schutz vor Mitlesen, Manipulation und Identitätsdiebstahl bei der Datenübertragung.

Wie funktioniert SSL (vereinfacht)?

Die Verschlüsselung basiert auf asymmetrischer Kryptographie für den Austausch, und symmetrischer Verschlüsselung für die Datennachrichten.

1. Client stellt Verbindung zum Server her (z. B. über HTTPS auf Port 443)
2. Server sendet sein SSL-Zertifikat
3. Client prüft das Zertifikat (Echtheit, Gültigkeit, Signatur durch CA)
4. Schlüsselaustausch - Sitzungsschlüssel für die Verschlüsselung wird ausgehandelt
5. Ab jetzt verschlüsselte Kommunikation

Was schützt SSL konkret?

SCHUTZFUNKTION	BEDEUTUNG
VERTRAULICHKEIT	Daten werden verschlüsselt – niemand kann sie lesen
INTEGRITÄT	Daten werden auf Veränderung geprüft (Hash-Wert)
AUTHENTIZITÄT	SSL-Zertifikat bestätigt Identität des Servers

SSL wird verwendet bei:

DIENST	PROTOKOLL MIT SSL/TLS	PORT
WEBSERVER	HTTPS	443
MAILVERSAND	SMTPS	564 / 587
MAILABRUF	POP3S, IMAPS	995 / 993
DATEIÜBERTRAGUNGEN	FTPS	990
VPN-VERBINDUNGEN	SSL-VPN (OpenVPN etc.)	Je nach Konfiguration

Fachbegriff Cloud-Computing und Beispiele für marktbekannte Cloud-Dienste

Definition

Cloud-Computing bezeichnet die Bereitstellung von IT-Ressourcen über das Internet (die „Cloud“), anstatt lokal auf physischen Geräten. Dazu gehören Speicherplatz, Rechenleistung, Anwendungen und Netzwerke, die flexibel und skalierbar nutzbar sind – meist on demand und kostenbasiert nach Nutzung. Der Nutzer muss sich nicht um Hardware, Wartung oder physische Infrastruktur kümmern.

Grundmodelle des Cloud-Computing

MODELL	BESCHREIBUNG
IAAS – INFRASTRUCTURE AS A SERVICE	Bereitstellung von virtueller Hardware (z.B. Server, Speicher, Netzwerk)
PAAS – PLATFORM AS A SERVICE	Bereitstellung von Entwicklungsplattformen (z.B. Datenbankdienste, Laufzeitumgebungen)
SAAS – SOFTWARE AS A SERVICE	Fertige Softwarelösungen über den Browser nutzbar (z.B. MS365, Gmail, Dropbox)

Cloud-Bereitstellungsmodelle

TYP	BESCHREIBUNG
PUBLIC CLOUD	Öffentliche Cloud-Angebote – z.B. Google Cloud
PRIVATE CLOUD	Nur für eine Organisation – intern oder extern gehostet
HYBRID CLOUD	Kombination aus Public + Private Cloud
COMMUNITY CLOUD	Für bestimmte Gruppen oder Sektoren (z.B. Schulen)

Beispiele für marktbekannte Cloud-Dienste

DIENST	TYP / MODELL	ANBIETER
GOOGLE DRIVE	SaaS – Dateispeicherung	Google
MS365 / ONEDRIVE	Saas + IaaS	Microsoft
DROPBOX	SaaS – File Hosting	Dropbox Inc.
AMAZON WEB SERVICES (AWS)	IaaS + PaaS + SaaS	Amazon
GOOGLE CLOUD PLATFORM (GCP)	IaaS + PaaS	Google
MICROSOFT AZURE	IaaS + PaaS + SaaS	Microsoft
ZOOM, GMAIL, SALESFORCE	SaaS	Diverse Anbieter
NEXTCLOUD	Private Cloud (Open Source)	Selbstgehostet

Vorteile von Cloud-Computing

- Kosteneffizienz (Nutzung nach Bedarf, keine Hardware-Investition)
- Hohe Skalierbarkeit
- Orts- und geräteunabhängig
- Automatische Updates & Wartung
- Schnelle Bereitstellung

Risiken / Nachteile

- Abhängigkeit vom Anbieter (Vendor Lock-in)
- Datenschutz & DSGVO – Standort der Daten wichtig!
- Internetverfügbarkeit erforderlich
- Mögliche Sicherheitslücken bei falscher Konfiguration

Kenntnisse über Private/Public/Hybrid Cloud

Public Cloud

Eine Public Cloud ist eine öffentlich zugängliche Cloud-Infrastruktur, die von einem externen Anbieter betrieben wird und mehreren Kunden gleichzeitig (Mandanten) zur Verfügung steht.

Nutzer teilen sich die physische Infrastruktur – jeder hat isolierten Zugriff auf seine Daten.

Vorteile:

- Geringe Kosten (Nutzung nach Bedarf)
- Keine eigene Hardware notwendig
- Hohe Skalierbarkeit
- Wartung durch den Anbieter

Nachteile:

- Weniger Kontrolle über Infrastruktur
- Datenschutzprobleme (z. B. Serverstandort USA)
- Abhängigkeit vom Anbieter (Vendor Lock-in)

Beispiele:

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

Private Cloud

Eine Private Cloud ist eine dedizierte Cloud-Infrastruktur, die ausschließlich für eine einzelne Organisation betrieben wird – entweder intern (im eigenen Rechenzentrum) oder extern (z. B. gehostet von einem Dienstleister).

Mehr Kontrolle, eigene Regeln – Sicherheit und Compliance stehen im Vordergrund.

Vorteile:

- Volle Kontrolle über Infrastruktur & Sicherheit
- Individuelle Anpassung möglich
- Besserer Datenschutz (z. B. DSGVO-konform)

Nachteile:

- Hoher Einrichtungs- und Wartungsaufwand
- Höhere Kosten (Hardware, Personal)
- Weniger flexibel als Public Cloud

Beispiele:

- OpenStack im eigenen Rechenzentrum
- Private Azure- oder VMware-Cloud für Unternehmen
- Kleiner Heimserver für private Nutzung

Hybrid Cloud

Eine Hybrid Cloud kombiniert Private und Public Clouds, um flexibel auf Anforderungen reagieren zu können. Sensible Daten verbleiben in der Private Cloud, während skalierbare Dienste in der Public Cloud laufen.

Typisches Szenario: lokale Infrastruktur + Cloud-Erweiterung bei hoher Last („Cloud-Bursting“)

Vorteile:

- Flexible Auslagerung je nach Bedarf
- Kosteneinsparung durch Cloud-Nutzung
- Sicherheit & Datenschutz durch selektive Trennung

Nachteile:

- Komplexe Verwaltung & Integration
- Erhöhte Sicherheitsanforderungen (Schnittstellen)
- Abhängigkeit von mehreren Anbietern

Beispiel:

- SAP-System lokal + Cloud-Backup auf Azure
- Datenbank lokal + Analyseplattform in AWS

Fachbegriffe IaaS, PaaS, SaaS

IaaS – Infrastructure as a Service

IaaS stellt virtuelle IT-Ressourcen wie Server, Speicher, Netzwerke und Firewalls zur Verfügung. Der Nutzer verwaltet selbst das Betriebssystem, Anwendungen und Daten.

Ideal für Admins, Entwickler und Unternehmen, die Kontrolle über ihre Systeme brauchen, aber keine eigene Hardware anschaffen wollen.

Beispielhafte Dienste:

- Amazon EC2 (virtuelle Server)
- Microsoft Azure Virtual Machines
- Google Compute Engine

Nutzer kümmert sich um:

- Betriebssystem
- Anwendungen
- Sicherheit & Updates

PaaS – Platform as a Service

PaaS bietet eine fertige Plattform zum Entwickeln, Testen und Bereitstellen von Software. Der Anbieter kümmert sich um Infrastruktur, Betriebssystem und Laufzeitumgebung.

Ideal für Entwickler, die sich nicht mit Servern oder Updates beschäftigen möchten.

Beispielhafte Dienste:

- Google App Engine
- Microsoft Azure App Services
- Heroku
- SAP Business Technology Platform

Nutzer kümmert sich um:

- Eigene Anwendungen
- Business-Logik
- Daten

SaaS – Software as a Service

SaaS liefert fertige Software-Anwendungen, die über den Browser oder eine App genutzt werden. Der Anbieter übernimmt alles – von Server bis Benutzeroberfläche.

Ideal für Endnutzer, die einfach nur mit der Software arbeiten möchten.

Beispielhafte Dienste:

- Microsoft 365
- Google Workspace (Gmail, Docs)
- Dropbox
- Salesforce
- Zoom

Nutzer kümmert sich um:

- Die Nutzung der Software (ohne Technik dahinter)

Kriterien und Voraussetzungen für den Einsatz von Cloud-Diensten

Bevor ein Unternehmen oder eine Organisation Cloud-Dienste einsetzt, müssen verschiedene Bedingungen erfüllt sein und Entscheidungsfaktoren berücksichtigt werden – sowohl aus Sicht der IT-Infrastruktur als auch der Datensicherheit, Gesetzgebung und Betriebsanforderungen.

Wichtige Kriterien für die Auswahl und Nutzung von Cloud-Diensten

Datenschutz & Sicherheit

- DSGVO-Konformität (z. B. bei Verarbeitung personenbezogener Daten)
- Standort der Datenzentren (z. B. EU vs. USA)
- Verschlüsselung bei Speicherung und Übertragung
- Zugriffsschutz und Identitätsmanagement (z. B. 2FA)

Verfügbarkeit & Zuverlässigkeit

- Hohe Verfügbarkeit (SLA: Service Level Agreements mit z. B. 99,9 %)
- Redundanz, Backup und Notfallwiederherstellung (Disaster Recovery)
- Stabiler Internetzugang als Voraussetzung!

Kosten & Wirtschaftlichkeit

- Kostenstruktur (Abomodell, Pay-as-you-go, Lizenzen)
- Einsparungen durch reduzierte Wartung/Hardware
- Gesamtkosten über die Laufzeit (TCO: Total Cost of Ownership)

Technische Voraussetzungen

- Kompatibilität mit vorhandener IT-Infrastruktur
- Bandbreite / Netzwerkanbindung
- Interoperabilität mit bestehenden Systemen
- Fähigkeit zur Integration in lokale Systeme (z. B. Active Directory)

Rechtliche Rahmenbedingungen

- Vertragsgestaltung & AGBs prüfen
- Klarheit über Zugriffsrechte, Datenhoheit und Vertragskündigung
- Compliance-Anforderungen (z. B. ISO 27001, TISAX, BSI)

Flexibilität & Skalierbarkeit

- Möglichkeit, Ressourcen schnell zu erweitern oder zu reduzieren
- Modularität der Services
- Anpassung an wachsende Nutzerzahlen / Anforderungen

Benutzerfreundlichkeit und Support

- Intuitive Bedienung für Endnutzer
- Verfügbarkeit von technischem Support & Schulungsangeboten
- Dokumentation & Self-Service-Portale

Voraussetzungen für den Einsatz (technisch & organisatorisch)

BEREICH	VORAUSSETZUNG
IT-INFRASTRUKTUR	Schnelle Internetverbindung, Firewall-Konfiguration
RECHTSABTEILUNG / DSB	Prüfung von Datenschutzkonformität
IT-ABTEILUNG	Know-how für Cloud-Verwaltung / Migration
ORGANISATIORISCH	Verantwortlichkeiten, Schulung der Nutzer
TECHNISCH	VPN, Backupkonzepte, Netzwerksegmentierung

6.3 IT-Security und Betriebssicherheit

Kenntnisse über Gefahren von Viren, Würmern, Trojanern, Spyware, Hackern, Phishing

Virus

Ein Virus ist ein Schadprogramm, das sich an andere Dateien oder Programme anhängt und sich beim Öffnen selbst vervielfältigt.

Gefahr:

- Datenmanipulation oder -löschung
- Verlangsamung des Systems
- Kann andere Schadsoftware nachladen

Merksatz: „Viren brauchen Wirte“ – sie verbreiten sich nur durch Benutzeraktionen (z. B. Dateianhang öffnen).

Wurm (Worm)

Ein Wurm ist ein selbstständiges Programm, das sich automatisch über Netzwerke verbreitet, ohne Benutzerinteraktion.

Gefahr:

- Hohe Netzwerklast (z. B. durch massenhafte Verbreitung)
- Schlägt Sicherheitslücken aus
- Kann sich sehr schnell ausbreiten (z. B. „ILOVEYOU“, „Blaster“)

Merksatz: „Würmer wandern von selbst“ – kein Klick nötig!

Trojaner (Trojan Horse)

Ein Trojaner tarnt sich als nützliches oder harmloses Programm, enthält aber schädlichen Code, der unbemerkt im Hintergrund ausgeführt wird.

Gefahr:

- Öffnet Hintertüren (Backdoors) für Hacker
- Kann Passwörter ausspionieren oder Fernzugriff ermöglichen
- Wird häufig mit Downloads verbreitet

Merksatz: „Der Trojaner täuscht und schleicht sich ein“ – scheinbar nützlich, in Wahrheit gefährlich.

Spyware

Spyware ist Software, die ohne Wissen des Nutzers Informationen über dessen Verhalten sammelt und weitergibt.

Gefahr:

- Überwachung von Tastatureingaben (Keylogger)
- Datendiebstahl (z. B. Kreditkarten, Logins)
- Verletzung der Privatsphäre

Merksatz: „Spyware spioniert“ – erkennt man kaum, aber sie sammelt alles.

Hacker (Angreifer)

Ein Hacker versucht, unerlaubt Zugriff auf Systeme oder Netzwerke zu erhalten – oft durch Ausnutzung von Sicherheitslücken.

Gefahr:

- Datendiebstahl
- Sabotage von Systemen
- Übernahme ganzer Netzwerke (z. B. über Ransomware)
- Achtung: Nicht alle Hacker sind kriminell – „White Hats“ testen Systeme legal zur Sicherheit.

Merksatz: „Hacker brechen ein – mit oder ohne Erlaubnis“

Phishing

Phishing bezeichnet den Versuch, durch gefälschte E-Mails oder Webseiten an vertrauliche Informationen wie Passwörter oder Bankdaten zu gelangen.

Gefahr:

- Identitätsdiebstahl
- Finanzbetrug (z. B. Fake-Bankseiten)
- Gefahr für ganze Unternehmen durch CEO-Fraud

Merksatz: „Phishing fischt nach Daten“ – über gefälschte Kommunikation.

Schutzmaßnahmen:

- Antivirenprogramme & Firewalls
- Betriebssystem- & Software-Updates
- Keine unbekannten Anhänge öffnen
- Multi-Faktor-Authentifizierung
- Nutzeraufklärung & Schulungen
- SPAM-Filter und sichere Mailgateways

Fachbegriff Zero-Day-Exploit

Ein Zero-Day-Exploit ist ein Angriff, der eine Sicherheitslücke ausnutzt, die dem Hersteller oder der Öffentlichkeit noch nicht bekannt ist – und für die es deshalb noch keinen Patch oder Schutz gibt.

Solche Angriffe sind besonders gefährlich, weil es noch keine Updates, Virensignaturen oder Firewall-Regeln gibt, um sie zu blockieren.

Technischer Zusammenhang

- Jede Software hat potenzielle Sicherheitslücken (Vulnerabilities).
- Ein Zero-Day-Exploit nutzt eine neu entdeckte, nicht dokumentierte Schwachstelle aus.
- Der Angreifer kann dadurch z. B.:
    - Code ausführen
    - Rechte ausweiten
    - Daten stehlen oder löschen
    - Zugriff auf Systeme übernehmen

Kenntnisse über Einschränkungsmöglichkeiten bei Benutzerkonten

Was bedeutet das?

Benutzerkonten erhalten in einem IT-System Rollen, Rechte und Einschränkungen, um genau zu definieren:

- Was sie sehen, verändern, installieren oder ausführen dürfen.
- Welche Systembereiche oder Netzlaufwerke sie nutzen können.
- Ob sie lokal oder remote zugreifen dürfen.

Ziel: Sicherheit, Ordnung, Nachvollziehbarkeit und Schutz vor Missbrauch.

Wichtige Einschränkungsmöglichkeiten im Überblick

EINSCHRÄNKUNG	BESCHREIBUNG UND ZWECK
BENUTZERROLLE / GRUPPENZUGEHÖRIGKEIT	Zuweisung zu Gruppen wie Benutzer, Administrator, Gast
RECHTEVERGABE (Z. B. NTFS-RECHTE)	Kontrolle über Lesen, Schreiben, Ändern von Dateien & Ordnern
ZUGRIFF AUF LAUFWERKE / FREIGABEN	Nur bestimmte Netzlaufwerke oder Ordner sichtbar
ANMELDEZEITEN	Zugriff nur in bestimmten Zeitfenstern (z. B. Mo–Fr, 8–18 Uhr)
GERÄTEZUGRIFFSSTEUERUNG	Kein Zugriff auf USB-Sticks, Drucker, CD/DVD-Laufwerke
SOFTWAREEINSCHRÄNKUNGEN / AUSFÜHRUNGSRICHTLINIEN	Nur erlaubte Programme starten (z. B. per GPO)
INTERNET- ODER NETZWERKEINSCHRÄNKUNG	Kein Zugriff auf Internetseiten oder bestimmte IPs
SPEICHER- UND POSTFACHKONTINGENTE	Beschränkung der Speichergröße (z. B. bei E-Mails)
REMOTEZUGRIFF VERBIETEN/ERLAUBEN	Zugriff nur vom Büro oder VPN, nicht von außen
SPERRUNG VON SYSTEMTOOLS ODER EINSTELLUNGEN	Keine Rechte zum Installieren oder Systemverändern

Beispiele in der Praxis (Windows)

In Unternehmen werden oft Active Directory Gruppenrichtlinien (GPOs) eingesetzt, um Benutzer zentral zu steuern.

BENUTZERKONTO	EINSCHRÄNKUNGEN
STANDARDBENUTZER	Kann Programme starten, aber nicht installieren oder Systemeinstellungen ändern
GAST	Sehr eingeschränkter Zugriff – kein dauerhaftes Speichern
ADMINISTRATOR	Vollzugriff auf System, darf alles – nur für IT-Personal empfohlen

Warum sind Einschränkungen wichtig?

- Sicherheit: Verhindert Installation von Schadsoftware
- Stabilität: Schutz vor falschen Änderungen im System
- Nachvollziehbarkeit: Jeder darf nur das, was er wirklich braucht
- Compliance: Datenschutz und Zugriffskontrolle werden eingehalten

Fachbegriff Multifaktor-Authentifizierung

Definition:

Multifaktor-Authentifizierung (MFA) ist ein Sicherheitsverfahren, bei dem der Zugriff auf ein System, Konto oder Netzwerk nicht nur durch ein einziges Authentifizierungsmerkmal (z. B. Passwort), sondern durch mindestens zwei unterschiedliche, unabhängige Faktoren abgesichert wird.

Ziel: Erhöhung der Zugriffssicherheit – auch bei gestohlenen Passwörtern bleibt das System geschützt.

Die drei Authentifizierungsfaktoren

FAKTOR-KATEGORIE	BEISPIEL	BESCHREIBUNG
WISSEN	Passwort, PIN	Etwas das der Benutzer weiß
BESITZ	Smartphone-App, Token, Chipkarte	Etwas das der Benutzer hat
BIOMETRIE	Fingerabdruck, Gesicht, Iris	Der Benutzer selbst

MFA = Kombination aus mindestens zwei dieser Kategorien

2FA = Zwei-Faktor-Authentifizierung (eine Unterform von MFA)

Typische MFA-Methoden im Einsatz

METHODE	TYPISCHER EINSATZBEREICH
TOTP (TIME-BASED-ONE-TIME-PASSWORD)	Login bei Microsoft, Amazon, Uni-Portale
SMS-CODE ODER E-MAIL LINK	Web-Logins, Bankdienste
SMARTCARD ODER YUBIKEY	Unternehmensnetzwerke, VPNs
BIOMETRIE (FINGERABDRUCK, GESICHT)	Windows Hello, Smartphones

Warum ist MFA so wichtig?

- Passwörter allein sind unsicher (Phishing, Brute Force, Datenlecks)
- MFA schützt auch bei gestohlenem Passwort – ohne zweiten Faktor kein Zugriff
- Pflicht in vielen Unternehmen, Behörden und nach DSGVO-Bestimmungen

Kenntnis der Sicherheits-Unterschiede zw. Hardware- und Software-Firewall

Was ist eine Firewall?

Eine Firewall ist ein Sicherheitsmechanismus, der den Datenverkehr zwischen zwei Netzwerken (z. B. Internet und LAN) überwacht und kontrolliert. Sie entscheidet, welche Verbindungen erlaubt oder blockiert werden – basierend auf Regeln, Ports, Protokollen und Adressen.

Software-Firewall

Eine Software-Firewall ist ein Programm, das auf einem Computer oder Server installiert wird und den Datenverkehr dieses Systems filtert.

Merkmale:

- Läuft auf dem Betriebssystem selbst
- Filtert ein- und ausgehende Verbindungen
- Kann pro Anwendung, Port oder IP-Adresse Regeln setzen

Vorteile:

- Genaue Kontrolle einzelner Anwendungen
- Benutzerfreundlich und flexibel konfigurierbar
- Oft bereits im Betriebssystem enthalten (z. B. Windows Defender Firewall)

Nachteile:

- Abhängig vom Betriebssystem – kann umgangen oder deaktiviert werden
- Nicht systemunabhängig → nur Schutz für den eigenen Rechner
- Braucht Systemressourcen

Hardware-Firewall

Eine Hardware-Firewall ist ein eigenständiges physisches Gerät, das zwischen Netzwerkkomponenten geschaltet wird (z. B. zwischen Router und Switch) und den gesamten Datenverkehr im Netzwerk filtert.

Merkmale:

- Gerät mit eigenem Betriebssystem (embedded OS)
- Arbeitet unabhängig von Endgeräten
- Unterstützt Deep Packet Inspection, VPN, IDS/IPS etc.

Vorteile:

- Zentraler Schutz für das ganze Netzwerk
- Keine Beeinflussung durch lokale Betriebssysteme
- Sehr leistungsfähig, besonders für Unternehmen
- Meist stabiler & sicherer gegen Manipulation

Nachteile:

- Kostenintensiver (Anschaffung + Wartung)
- Komplexere Konfiguration
- Kein Schutz, wenn Angriffe bereits innerhalb des LANs erfolgen

Vergleichstabelle: Hardware- vs. Software-Firewall

MERKMAL	SOFTWARE-FIREWALL	HARDWARE-FIREWALL
POITION	Auf dem Endgerät	Zwischen Internet und internem Netzwerk
SCHUTZBEREICH	Nur für den jeweiligen PC	Für das gesamte Netzwerk
KOSTEN	Günstig / oft kostenlos	Höher (Anschaffung + Wartung)
KONFIGURATION	Benutzerfreundlich	Komplex, professionell
PERFORMANCE	Belastet das Endgerät	Eigene Hardware – höhere Leistung
MANIPULATIONSSICHERHEIT	Kann deaktiviert oder umgangen werden	Schutz durch isoliertes System

Funktion einer Hardware-Firewall

Definition

Eine Hardware-Firewall ist ein physisches Netzwerkgerät, das den Datenverkehr zwischen verschiedenen Netzwerken (z. B. Internet und internes LAN) überwacht, filtert und kontrolliert. Sie dient als erste Verteidigungslinie gegen unautorisierten Zugriff und Cyberangriffe.

Eine Hardware-Firewall ist Teil eines umfassenden Defense-in-Depth-Konzepts, bei dem mehrere Sicherheitsmaßnahmen (z. B. Firewall, Virenschutz, Netzwerksegmentierung) auf verschiedenen Ebenen zusammenspielen.

Hauptfunktionen einer Hardware-Firewall

Paketfilterung (Packet Filtering)
Überprüfung von Header-Informationen in IP-Paketen (z. B. Quell-/Ziel-IP, Port, Protokoll). Pakete, die nicht den Regeln entsprechen, werden verworfen.

Stateful Packet Inspection (SPI)
Verfolgt den Zustand aktiver Verbindungen und entscheidet basierend auf dem Kontext, ob Daten durchgelassen werden. Ist sicherer als reines Paketfiltern.

Zugriffskontrolle (Access Control)
Regeln zur Steuerung, welche Dienste, IP-Adressen oder Netzwerke kommunizieren dürfen. Z. B.: "Nur interne Clients dürfen HTTP nach außen senden."

NAT (Network Address Translation)
Übersetzt private IP-Adressen zu öffentlichen, was zusätzliche Sicherheit bringt, da interne Systeme nicht direkt aus dem Internet erreichbar sind.

VPN-Unterstützung
Viele Hardware-Firewalls bieten integrierte VPN-Funktionen für sichere Remote-Verbindungen.

Intrusion Detection & Prevention (IDS/IPS) (bei Next-Gen Firewalls)
Erkennung und Blockierung von Angriffsmustern und ungewöhnlichem Verhalten in Echtzeit.

Content Filtering / Application Control
Blockierung bestimmter Webseiten oder Anwendungen (z. B. Social Media, P2P-Traffic), oft über Deep Packet Inspection.

Logging & Monitoring
Protokollierung von Verbindungsversuchen, Sicherheitsverstößen etc., oft mit syslog-Support oder SIEM-Integration.

Kenntnisse über notwendige Einstellungen bei Virenscanner

Ein Virenscanner (Antivirenprogramm) erkennt, blockiert und entfernt Schadsoftware (Malware) wie Viren, Trojaner, Würmer, Spyware und Ransomware. Damit der Virenscanner effektiv arbeitet, müssen bestimmte Einstellungen korrekt konfiguriert werden – sowohl für Endgeräte als auch auf Servern und in Netzwerken.

Wichtige Einstellungen im Überblick

EINSTELLUNG	FUNKTION
ECHTZEITSCHUTZ (ON-ACCESS SCAN)	Überwacht kontinuierlich alle Dateizugriffe und blockiert Bedrohungen sofort.
GEPLANTE SCANS (SCHEDULED SCANS)	Automatische, regelmäßige Systemüberprüfung zu festgelegten Zeiten.
SIGNATUR-UPDATE (DEFINITION UPDATE)	Automatische Aktualisierung der Malware-Datenbank, meist mehrmals täglich.
HEURISTISCHE ANALYSE	Erkennung neuer oder unbekannter Malware durch Analyse verdächtigen Verhaltens.
VERHALTENSÜBERWACHUNG	Analyse laufender Prozesse auf verdächtige Aktivitäten (z. B. Zugriff auf Systemdateien).
QUARANTÄNEFUNKTION	Infizierte Dateien werden isoliert, ohne sofort gelöscht zu werden.
E-MAIL- UND WEB-SCHUTZ	Scannt Anhänge, eingebettete Links und Webseiten auf Schadcode.
AUSNAHMEN (WHITELIST)	Vertrauenswürdige Programme/Ordner vom Scan ausnehmen, z. B. für Performance-Gründe.
USB-/WECHSELDATENTRÄGER-SCHUTZ	Automatische Prüfung bei Anschluss von externen Geräten (z. B. USB-Sticks).
FIREWALL-INTEGRATION (BEI SUITES)	Steuerung von Netzwerkzugriffen, optional durch den Virenscanner integriert.

Sicherheit vs. Performance: Feineinstellung

Virenscanner können Systemressourcen stark beanspruchen. Daher ist es wichtig, die Balance zwischen Sicherheit und Leistung zu finden:

- Geplante Scans am besten außerhalb der Arbeitszeiten.
- Ausnahmen nur gezielt und mit Begründung einrichten (z. B. bestimmte Entwicklerverzeichnisse).
- Archivdateien (z. B. ZIP, RAR): Tiefenscan nur bei Bedarf, da sehr ressourcenintensiv.

Zentrale Verwaltung (für Unternehmen)

In größeren IT-Umgebungen werden Virenscanner über eine zentrale Management-Konsole verwaltet:

- Richtlinien für Gruppen und Geräte
- Überwachung von Ereignissen, Infektionen, Updates
- Remote-Konfiguration und Fern-Scans
- Protokollierung & Reporting

Typische Fehler in der Konfiguration

FEHLER	FOLGE
DEAKTIVIERTER ECHTZEITSCHUTZ	Malware kann sich ungehindert ausführen
KEINE AUTOMATISCHEN UPDATES	Neue Bedrohungen werden nicht erkannt
ZU VIELE AUSNAHMEN	Malware kann sich in Whitelist-Verzeichnissen verstecken
IGNORIEREN VON E-MAIL-SCHUTZ	Gefährliche Anhänge oder Phishing-Mails werden nicht abgewehrt
KEIN SCAN VON EXTERNEN DATENTRÄGERN	USB-Infektionen bleiben unentdeckt

Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

Client-PCs sind oft das schwächste Glied in der Sicherheitskette. Ein wirksamer Schutz vor Missbrauch (z. B. durch unbefugte Nutzung, Malware, Datenklau) erfordert eine Kombination aus technischen Maßnahmen, organisatorischen Regeln und Benutzerschulung.

Technische Schutzmaßnahmen (Hardening des Clients)

MAßNAHME	BESCHREIBUNG
BENUTZERKONTENSTEUERUNG (UAC)	Verhindert unautorisierte Änderungen durch administrative Rechte.
GRUPPENRICHTLINIEN (GPO)	Zentral gesteuerte Einschränkungen und Sicherheitsvorgaben im Netzwerk.
EINSCHRÄNKUNG LOKALER ADMINRECHTE	Nur autorisierte Admins dürfen Systemeinstellungen ändern.
BIOS-/UEFI-PASSWORTSCHUTZ	Verhindert unautorisierten Zugriff auf Boot-Einstellungen.
VERSCHLÜSSELUNG (Z. B. BITLOCKER)	Schutz der Daten bei Diebstahl oder unbefugtem Zugriff auf das Speichermedium.
AUTORISIERTE SOFTWARE-WHITELIST	Nur genehmigte Programme dürfen installiert und ausgeführt werden.
PORTS UND SCHNITTSTELLEN SPERREN	Deaktivierung ungenutzter USB- oder Netzwerkschnittstellen.

Netzwerkbezogene Maßnahmen

MAßNAHME	BESCHREIBUNG
FIREWALL-REGELN	Kontrolliert ein- und ausgehenden Netzwerkverkehr.
NETZWERKSEGMENTIERUNG	Trennung sensibler Bereiche (z. B. Buchhaltung, HR) vom allgemeinen Netz.
VPN-ZUGANG NUR MIT AUTHENTIFIZIERUNG	Absicherung von Remote-Verbindungen.
INTRUSION DETECTION/PREVENTION (IDS/IPS)	Erkennung und Abwehr von Angriffen auf Netzwerkebene.

Software-Schutzmaßnahmen

MAßNAHME	BESCHREIBUNG
AKTUELLER VIRENSCANNER	Echtzeitschutz und regelmäßige Updates gegen Malware.
PATCH-MANAGEMENT	Automatisches Einspielen von Sicherheitsupdates für Betriebssysteme und Software.
APPLICATION CONTROL	Kontrolle, welche Anwendungen gestartet werden dürfen.
BROWSER-HARDENING	Blockieren von unsicheren Plugins, Pop-ups und Skripten.

Organisatorische & Benutzerbezogene Maßnahmen

MAßNAHME	BESCHREIBUNG
STARKE PASSWORTRICHTLINIEN	Komplexe, regelmäßig zu ändernde Passwörter mit MFA (Multi-Faktor-Authentifizierung).
BENUTZERSCHULUNGEN	Aufklärung über Phishing, Social Engineering und sichere Nutzung.
LOGGING UND MONITORING	Aufzeichnung und Auswertung von Benutzeraktivitäten zur Missbrauchserkennung.
SPERRUNG BEI INAKTIVITÄT	Automatische Bildschirmsperre nach definierter Zeit.

Beispielhafte Kombination in der Praxis

Ein sicher konfigurierter Client-PC in einem Unternehmen:

- Nutzer hat kein Admin-Recht
- BitLocker aktiviert
- Virenscanner mit Echtzeitschutz
- Zugriff nur über VPN mit MFA
- Nur genehmigte Software installierbar
- USB-Schnittstellen deaktiviert
- Sicherheits-Patches werden automatisch eingespielt

Kenntnisse über sichere Planung von Backups

Ein Backup schützt Daten vor Verlust durch Hardwarefehler, Malware (z. B. Ransomware), menschliches Versagen oder Naturkatastrophen. Eine sichere Backup-Planung ist essenziell für die Datenverfügbarkeit.

Grundprinzipien der Backup-Strategie

PRINZIP	BESCHREIBUNG
REGELMÄßIGKEIT	Backups müssen automatisiert und wiederholend (z. B. täglich, wöchentlich) erfolgen.
REDUNDANZ	Mehrere Backup-Kopien an verschiedenen Orten speichern.
TRENNUNG	Backups getrennt vom produktiven System aufbewahren (physisch/logisch).
SICHERHEITSPRÜFUNG (RECOVERY TEST)	Regelmäßige Wiederherstellungstests, um Datenintegrität und Verfügbarkeit zu prüfen.
ZUGRIFFSKONTROLLE	Backups verschlüsseln und vor unbefugtem Zugriff schützen.

Die 3-2-1-Regel (Best Practice)

REGEL	ERKLÄRUNG
3 KOPIEN	Mindestens drei Kopien der Daten: 1 original + 2 Backups
2 SPEICHERARTEN	Auf mindestens zwei unterschiedlichen Medien speichern (z. B. Festplatte & Cloud)
1 OFFSITE-KOPIE	Mindestens eine Kopie außerhalb des Standorts lagern

Arten von Backups

BACKUP-TYP	BESCHREIBUNG
VOLL-BACKUP	Komplettes Backup aller Daten – sehr sicher, aber speicherintensiv
INKREMENTELLES BACKUP	Nur Datenänderungen seit dem letzten Backup werden gespeichert – speicher- und zeiteffizient
DIFFERENTIELLES BACKUP	Änderungen seit dem letzten Voll-Backup – schneller wiederherstellbar als inkrementell

Backup-Ziele (RTO & RPO)

Diese Werte bestimmen Backup-Intervall und Wiederherstellungsstrategie.

BEGRIFF	BEDEUTUNG
RTO (RECOVERY TIME OBJECTIVE)	Wie schnell sollen Systeme nach einem Ausfall wieder laufen?
RPO (RECOVERY POINT OBJECTIVE)	Wie alt dürfen die Daten im Notfall maximal sein (z. B. 1 Tag)?

Sichere Speicherorte & Medien

SPEICHERLÖSUNG	VORTEILE	NACHTEILE
EXTERNE FESTPLATTEN	Kostengünstig, mobil	Risiko bei physischem Schaden
NAS/SAN-SYSTEME	Netzwerkbasierte Sicherung für mehrere Clients	Kann bei Malware-Befall mitverschlüsselt werden
BANDLAUFWERKE (TAPE)	Langlebig, offline-lagerfähig	Langsame Wiederherstellung
CLOUD-BACKUP	Ortsunabhängig, skalierbar	Abhängig von Internet und Datenschutzrisiken

Automatisierung & Monitoring

Backup-Software (z. B. Iperius, Veeam, Acronis, Windows Server Backup) ermöglicht:

- Zeitpläne und Versionierung
- Backup-Berichte und Warnmeldungen bei Fehlern
- Verschlüsselung und Benutzerrechteverwaltung

Backup-Sicherheit

MAßNAHME	BEGRÜNDUNG
VERSCHLÜSSELUNG DER BACKUPS	Schutz bei Verlust oder Diebstahl
ZUGRIFFSRECHTE BESCHRÄNKEN	Nur autorisierte Admins dürfen auf Backup-Daten zugreifen
BACKUP VOM NETZWERK TRENNEN	Schutz vor Ransomware (Air Gap)
LOGS & PROTOKOLLE ÜBERWACHEN	Verdächtige Aktivitäten erkennen, z. B. nicht autorisierte Löschungen

Kenntnisse über verschiedene Backup-Prinzipien

Backup-Prinzipien definieren die Art, wie und wann Daten gesichert werden. Die Auswahl eines geeigneten Backup-Prinzips ist entscheidend für Datensicherheit, Verfügbarkeit, Wiederherstellungsdauer und Ressourceneffizienz.

Haupt-Backup-Prinzipien im Vergleich

PRINZIP	BESCHREIBUNG	VORTEIL	NACHTEIL
VOLL-BACKUP	Es wird jedes Mal das gesamte System gesichert.	Einfache Wiederherstellung	Lange Dauer, viel Speicher
INKREMENTELLES BACKUP	Es werden nur Änderungen seit dem letzten Backup gesichert.	Spart Speicher und Zeit beim Backup	Abhängig von allen vorherigen Backups
DIFFERENZIELLES BACKUP	Es werden alle Änderungen seit dem letzten Voll-Backup gespeichert.	Schneller restore als inkrementell	Speicherbedarf steigt täglich
SPIEGELUNG (MIRRORING)	Daten werden in Echtzeit gespiegelt (1:1-Kopie).	Permanente Verfügbarkeit	Kein Schutz vor logischen Fehlern
SNAPSHOT (Z. B. BEI VM)	Momentaufnahme des Systemzustands zu einem Zeitpunkt.	Sehr effizient bei virtuellen Systemen	Kein Ersatz für langfristige Backups

Erweiterte Backup-Prinzipien und Konzepte^

PRINZIP / KONZEPT	BESCHREIBUNG
ROLLIERENDE BACKUPS	Backup-Sätze rotieren über Zeit, z. B. tägliche/wöchentliche Medienrotation.
BACKUP-GENERATIONEN (GROßVATER-VATER-SOHN)	3-Ebenen-Strategie (z. B. täglich, wöchentlich, monatlich) zur Datenversionierung
SNAPSHOT + EXPORT	Snapshot + spätere Konvertierung/exportierte Sicherung auf externes Medium
VERSIONIERTE BACKUPS	Mehrere Dateiversionen werden archiviert – wichtig bei versehentlichem Überschreiben
DIFFERENZIMAGES	Nur geänderte Datenblöcke im Vergleich zur vorherigen Version werden gespeichert

Kenntnisse über Backup-Medien und deren richtiger Lagerung

Backup-Medien sind physische oder digitale Speichermedien, auf denen Sicherungskopien gespeichert werden. Die Wahl des richtigen Mediums sowie dessen fachgerechte Lagerung ist entscheidend für Datensicherheit, Langlebigkeit und Wiederherstellbarkeit.

Überblick über Backup-Medien

MEDIUM	EIGENSCHAFTEN	HALTBARKEIT	ANWENDUNG
EXTERNE FESTPLATTE (HDD/SSD)	Mobil, schnell, große Kapazität, günstig	3–5 Jahre (HDD), >5 Jahre (SSD)	KMU, Home-Office, lokale Sicherung
BANDLAUFWERK (TAPE)	Geringe Kosten pro GB, langlebig, offline lagerbar	10–30 Jahre	Großunternehmen, Langzeitarchivierung
NAS (NETWORK ATTACHED STORAGE)	Mehrbenutzerfähig, im Netzwerk erreichbar	abhängig von Festplatten	Kleinunternehmen, automatische Backups
RDX (WECHSELDATENTRÄGER)	Robust, stoßfest, für Industrie geeignet	10–15 Jahre	Industrie, mobile Sicherung
DVD/BLU-RAY	Nur für kleinere Datenmengen, hohe Ausfallsicherheit	5–10 Jahre	Private Nutzung, Langzeitsicherung
CLOUD-SPEICHER	Ortsunabhängig, skalierbar, keine physische Lagerung	abhängig vom Anbieter	Unternehmen & Privat, Disaster Recovery

Sichere Lagerung von Backup-Medien

MAßNAHME	BESCHREIBUNG
KLIMATISCHE BEDINGUNGEN	Kühle, trockene und staubfreie Umgebung; ideal 10–20 °C, <60 % Luftfeuchtigkeit
PHYSISCHE SICHERHEIT	Aufbewahrung in abschließbaren Schränken/Safes
BRANDSCHUTZ	Brandschutzschränke oder Lager in anderen Brandabschnitten
OFFSITE-LAGERUNG	Mindestens eine Sicherung außerhalb des Betriebsstandorts lagern
LAGERUNG OFFLINE (AIR-GAP)	Backup nicht dauerhaft mit dem Netzwerk verbunden → Schutz vor Ransomware
KENNZEICHNUNG UND INVENTARISIERUNG	Eindeutige Beschriftung, Dokumentation von Speicherinhalt und Datum
ROTATION (Z. B. G-V-S)	Alte Medien regelmäßig durch neue ersetzen (z. B. Großvater-Vater-Sohn-Prinzip)

Spezielle Lagerung nach Medientyp

MEDIUM	HINWEISE ZUR LAGERUNG
BÄNDER (LTO, DDS)	Senkrecht lagern, nicht in der Nähe von Magnetfeldern
FESTPLATTEN (HDD)	Erschütterungsfrei, nicht im Betrieb transportieren
SSD	Kühl lagern, elektrostatisch schützen (ESD-Tasche)
DVD/BLU-RAY	Kratzfest aufbewahren, direkte Sonneneinstrahlung vermeiden
RDX	Robust, trotzdem stoßfrei lagern

Fachbegriff DMZ

Definition

Die DMZ (Demilitarisierte Zone) ist ein sicherheitskritischer Netzwerkbereich, der zwischen dem internen, vertrauenswürdigen LAN und dem externen, ungeschützten Internet liegt. Sie dient als Pufferzone, in der öffentlich zugängliche Server betrieben werden (z. B. Web-, Mail- oder DNS-Server), ohne direkten Zugriff auf das interne Firmennetz zu erlauben.

Ziel und Funktion der DMZ

ZWECK	BESCHREIBUNG
SICHERHEITSISOLATION	Trennung von Internet und internem Netz
ANGRIFFSBEGRENZUNG	Sollte ein Dienst in der DMZ kompromittiert werden, bleibt das LAN geschützt
ZUGRIFFSSTEUERUNG	Nur definierter Datenverkehr ist zwischen DMZ ↔ LAN bzw. DMZ ↔ Internet erlaubt
TRANSPARENTE DIENSTE	Dienste der DMZ sind für externe Benutzer zugänglich, ohne Sicherheitsrisiko fürs LAN

Typische Dienste in der DMZ

DIENST	GRUND FÜR PLATZIERUNG IN DER DMZ
WEBSERVER	Öffentlicher Zugriff, aber getrennt vom internen Backend
MAILSERVER (SMTP-GATEWAY)	Filterung & Weiterleitung ohne direkten LAN-Zugriff
DNS-SERVER (ÖFFENTLICH)	Beantwortet Namensanfragen von außen, schützt internen DNS
REVERSE PROXY / VPN-GATEWAY	Steuerung & Kontrolle des externen Datenverkehrs

Fachbegriff Stateful Packet Inspection

Definition

Stateful Packet Inspection (SPI) ist ein Firewall-Prinzip, bei dem nicht nur einzelne Datenpakete analysiert werden, sondern der gesamte Zustand einer Verbindung berücksichtigt wird. Dabei speichert die Firewall Informationen zu aktiven Verbindungen (z. B. TCP-Sitzungen) und prüft, ob empfangene Pakete logisch zu einer bestehenden Verbindung gehören.

Funktionsweise von SPI (vereinfacht)

1. Ein Client sendet eine Anfrage (z. B. HTTP an Webserver).
2. Die SPI-Firewall merkt sich:
    a. Quell-/Ziel-IP und -Port
    b. Protokolltyp (TCP, UDP)
    c. Status (z. B. SYN gesendet)
3. Die Antwort vom Server wird überprüft, ob sie zu einer bestehenden Verbindung gehört.
4. Nur gültige Antworten werden zugelassen, alles andere wird verworfen oder geloggt.

Zustands-Tabelle (State Table)

Die Firewall verwaltet einen sogenannten State Table, in dem alle aktiven Verbindungen gespeichert sind. Diese Tabelle enthält:

- Verbindungsschlüssel (IP, Port, Protokoll)
- Status (z. B. „ESTABLISHED“, „SYN_SENT“)
- Zeitstempel (zum automatischen Entfernen inaktiver Verbindungen)

Vorteile von SPI

VORTEIL	BESCHREIBUNG
SICHERER	Nur legitime Verbindungen werden zugelassen
EFFEKTIV GEGEN SPOOFING	Unbekannte, nicht initiierte Pakete werden verworfen
VERBINDUNGSORIENTIERT	Ideal für TCP-basierte Dienste (Web, Mail, Remote Access)
GRUNDLAGE FÜR DEEP PACKET INSPECTION	SPI ist häufig Grundlage für erweiterte Firewall-Techniken

Funktionsweise eines Port-Scanners

Ein Port-Scanner ist ein Werkzeug zur Analyse eines Computers oder Netzwerks, das prüft, welche Netzwerkports geöffnet, geschlossen oder gefiltert sind. Port-Scanner werden in der IT-Sicherheit, Netzwerkwartung und Penetrationstests eingesetzt – sowohl zu legitimen als auch zu böswilligen Zwecken.

Ziel eines Port-Scans

- Herausfinden, welche Dienste auf einem Zielsystem aktiv sind.
- Einschätzung von Sicherheitslücken (z. B. ungesicherter offener Port).
- Vorbereitung für weitere Analysen (z. B. Versions-Scan, Exploit-Tests).

Funktionsweise in Schritten

1. Zielauswahl: IP-Adresse oder Hostname wird angegeben.
2. Portspezifikation: Auswahl von Portbereichen (z. B. 1–1024).
3. Scan-Methode wählen (siehe unten).
4. Verbindungsversuche starten: Scanner sendet Netzwerkpakete (z. B. SYN).
5. Antwort analysieren:
    a. Antwort erhalten → Port offen
    b. Verbindung abgelehnt → Port geschlossen
    c. Keine Antwort oder Filter → Port gefiltert
6. Bericht erstellen: Ergebnisse je nach Scanner grafisch oder tabellarisch.

Typische Scan-Techniken

SCAN-TYP	BESCHREIBUNG	ERKENNBAR - FIREWALL?
TCP-CONNECT-SCAN	Volle Verbindung mit Zielport (3-Way-Handshake)	JA
SYN-SCAN	Sendet nur SYN, ohne Verbindung abzuschließen („Half-Open“)	Teilweise (je nach Firewall)
UDP-SCAN	Sendet leere UDP-Pakete → auf Antwort wird geachtet	Schwerer erkennbar
STEALTH-SCAN	Verwendet ungewöhnliche Flags (FIN, NULL, Xmas)	Sehr schwer erkennbar
PING-SCAN	Nur prüfen, ob Ziel host erreichbar ist (kein Portscan!)	Einfach

Kenntnisse über Sicherheitstechnologie TLS

TLS (Transport Layer Security) ist ein kryptografisches Protokoll, das sichere Kommunikation über ein Netzwerk ermöglicht. Es schützt Daten durch Verschlüsselung, Integritätssicherung und Authentifizierung, insbesondere bei der Übertragung über unsichere Netzwerke wie das Internet.

Einsatzbereiche von TLS

ANWENDUNG	BESCHREIBUNG
HTTPS	Sichere Web-Kommunikation (TLS über HTTP, erkennbar an „https://“
E-MAIL (SMTP, IMAP, POP3)	Schutz der E-Mail-Kommunikation durch TLS-Erweiterungen
VPN-VERBINDUNGEN	Teilweise TLS-basiert (z. B. OpenVPN
VOIP & MESSAGING	Verschlüsselung bei Echtzeitkommunikation

Grundfunktionen von TLS

FUNKTION	ZWECK
VERSCHLÜSSELUNG	Schutz vor Mitlesen durch Dritte (z. B. bei öffentlichem WLAN)
INTEGRITÄTSPRÜFUNG	Erkennung manipulierter Daten während der Übertragung
AUTHENTIFIZIERUNG	Überprüfung der Identität des Kommunikationspartners (z. B. Server-Zertifikat)

Wie funktioniert TLS (vereinfacht)?

TLS-Handshake – Ablauf in Kurzform:

1. Client Hello
    - Client sendet Versionsinfo, unterstützte Cipher Suites, Zufallswert
2. Server Hello
    - Server wählt Cipher Suite, sendet sein Zertifikat
3. Zertifikatsprüfung
    - Client prüft Zertifikat (gültig? vertrauenswürdig? richtig signiert?)
4. Schlüsselaustausch
    - Gemeinsam wird ein Sitzungsschlüssel erzeugt (z. B. per Diffie-Hellman)
5. Verschlüsselung beginnt
    - Ab jetzt wird die Datenkommunikation verschlüsselt übertragen

Zentrale Technologien in TLS

TECHNIK	BESCHREIBUNG
ASYMMETRISCHE VERSCHLÜSSELUNG	Für Schlüsselaustausch (z. B. RSA, ECDHE)
SYMMETRISCHE VERSCHLÜSSELUNG	Für schnelle Datenübertragung nach dem Handshake (z. B. AES)
ZERTIFIKATE (X.509)	Digital signierte Nachweise der Identität (z. B. für Webseiten)
HASHFUNKTIONEN	Sicherstellung der Integrität (z. B. SHA-256)

Zertifikate & CA (Certificate Authority)

Zertifikate werden von Zertifizierungsstellen (z. B. Let's Encrypt, DigiCert) ausgestellt.
Sie bestätigen:

- Eigentümer der Domain
- Gültigkeitsdauer
- Signatur durch vertrauenswürdige CA

Fachbegriff CA in Zusammenhang mit Zertifikaten

Eine CA (Certificate Authority) ist eine vertrauenswürdige Organisation, die digitale Zertifikate ausstellt, überprüft und signiert. Diese Zertifikate dienen zur Authentifizierung von Identitäten (z. B. von Webseiten, Servern, Personen oder Geräten) im Rahmen der Public Key Infrastructure (PKI).

Aufgaben einer CA

AUFGABE	BESCHREIBUNG
ZERTIFIKATE AUSSTELLEN	Generierung und Signierung eines Zertifikats nach erfolgreicher Prüfung
IDENTITÄTSPRÜFUNG	Verifizierung, ob Antragsteller tatsächlich die Domain oder Identität besitzt
ZERTIFIKATSSTATUS VERWALTEN	Veröffentlichung von Sperrlisten (CRL) oder Onlineprüfung (OCSP)
ZERTIFIKATE VERLÄNGERN ODER WIDERRUFEN	Verwaltung des gesamten Lebenszyklus eines Zertifikats

Arten von Zertifizierungsstellen

TYP	BESCHREIBUNG
ROOT CA	Stammzertifizierungsstelle – höchste Instanz, direkt im Trust Store enthalten
INTERMEDIATE CA	Zwischeninstanz – stellt Zertifikate im Namen der Root CA aus (mehr Sicherheit)
PRIVATE CA	Firmeneigene CA für interne Netzwerke (z. B. Active Directory-Zertifikate)
PUBLIC CA	Öffentliche CAs wie Let's Encrypt, DigiCert, GlobalSign, etc.

Fachbegriffe Private Key und Public Key

Public Key – Öffentlicher Schlüssel

MERKMAL	BESCHREIBUNG
VERÖFFENTLICHUNG	Darf offen geteilt werden (z. B. auf Webseiten, Zertifikaten, E-Mails)
FUNKTION	Dient zum Verschlüsseln von Nachrichten und zur Überprüfung digitaler Signaturen
BEISPIELHAFTE NUTZUNG	Jemand sendet dir verschlüsselte Daten → verwendet deinen Public Key

Private Key – Privater Schlüssel

MERKMAL	BESCHREIBUNG
GEHEIMHALTUNG	Muss streng geschützt bleiben – nur der Besitzer darf Zugriff haben
FUNKTION	Wird verwendet zum Entschlüsseln von Nachrichten oder zum Signieren von Daten
KRITISCHE SICHERHEIT	Wer Zugriff auf den Private Key hat, kann sich als der Inhaber ausgeben

Funktionsprinzip im Überblick

Verschlüsselung:

- Sender: Public Key des Empfängers → verschlüsselt Nachricht
- Empfänger: eigener Private Key → entschlüsselt Nachricht

Digitale Signatur:

- Absender: signiert mit eigenem Private Key
- Empfänger: prüft Signatur mit dem Public Key des Absenders

Sicherstellen von Datenvertraulichkeit bei gemeinsamen Netzlaufwerken

Gemeinsame Netzlaufwerke ermöglichen den zentralen Zugriff auf Dateien innerhalb eines Unternehmens oder Teams. Um Datenvertraulichkeit zu gewährleisten – also sicherzustellen, dass nur autorisierte Benutzer Zugriff auf sensible Daten haben – müssen technische und organisatorische Schutzmaßnahmen umgesetzt werden.

Ziele beim Schutz von Netzlaufwerken

ZIEL	BEDEUTUNG
VERTRAULICHKEIT	Daten dürfen nur von berechtigten Personen gelesen werden
INTEGRITÄT	Daten dürfen nicht unbefugt verändert werden
ZUGRIFFSKONTROLLE	Wer darf was (lesen, schreiben, löschen)?
NACHVOLLZIEHBARKEIT	Wer hat wann was gemacht?

Technische Maßnahmen zur Sicherung

Berechtigungsmanagement (ACLs / NTFS-Rechte)

EBENE	MAßNAHME
FREIGABEEBENE (SHARE)	Grobe Rechtevergabe (z. B. „Lesen“, „Ändern“, „Vollzugriff“)
DATEISYSTEMEBENE (NTFS)	Fein granulare Kontrolle auf Ordner- und Dateiebene
BEST PRACTICE	NTFS-Rechte restriktiver als Freigaberechte – Prinzip der minimalen Rechte

Gruppenbasierte Rechtevergabe

- Benutzer werden in Sicherheitsgruppen organisiert (z. B. „HR_Lesen“, „IT_Schreiben“)
- Zugriffsrechte werden der Gruppe, nicht dem einzelnen User zugewiesen
- Vereinfacht Verwaltung, erhöht Nachvollziehbarkeit

Zugriffsprotokollierung (Auditing)

- Aktivieren der Überwachung von Datei- und Ordnerzugriffen
- Logging: Wer hat wann welche Datei geöffnet, geändert oder gelöscht?
- Wichtig für Datenschutz, Nachverfolgung und interne Revision

Netzwerkzugang sichern

- Zugriff nur aus dem internen Netzwerk oder via VPN
- Schutz der Freigaben durch Firewall, VLANs und Netzsegmentierung
- Sperren anonymer oder veralteter Protokolle (z. B. SMBv1)

Erarbeiten von Berechtigungskonzepten im Active Directory

Ein Berechtigungskonzept im Active Directory (AD) legt fest, wer in einem Netzwerk auf welche Ressourcen wie zugreifen darf. Ziel ist es, Sicherheit, Nachvollziehbarkeit und einfache Verwaltung von Zugriffsrechten auf Benutzer, Gruppen, Ordner, Freigaben und Dienste zu gewährleisten.

Ziele eines Berechtigungskonzepts

ZIEL	BEDEUTUNG
DATENSICHERHEIT	Nur autorisierte Benutzer erhalten Zugriff auf sensible Ressourcen
TRANSPARENZ & KONTROLLE	Klar definierte Rechtevergabe – wer darf was?
VERWALTUNGSAUFWAND REDUZIEREN	Durch Gruppenvergabe und Standardisierung
AUDITING & COMPLIANCE	Rechte sind dokumentiert, überprüfbar und revisionssicher

Grundprinzipien der Rechtevergabe (Best Practices)

PRINZIP	BESCHREIBUNG
NEED-TO-KNOW-PRINZIP	Benutzer erhalten nur Zugriff auf Ressourcen, die sie wirklich benötigen
PRINZIP DER MINIMALEN RECHTE	So wenig Rechte wie möglich, so viele wie nötig
GRUPPENBASIERTE VERGABE	Rechte werden Gruppen, nicht Einzelpersonen zugewiesen
TRENNUNG VON BERECHTIGUNGEN UND ROLLEN	klare Trennung von Benutzerrollen, Aufgaben und Ressourcen

Erstellen eines Berechtigungskonzepts

SCHRITT	MAßNAHME
1. IST-ANALYSE	Erfassen aktueller Benutzer, Gruppen, Freigaben, Rechte
2. ROLLEN DEFINIEREN	Wer braucht welche Zugriffe in welcher Rolle?
3. GRUPPEN PLANEN	Global Groups für Benutzer, Domain Local Groups für Berechtigungen
4. ZUWEISUNG & IMPLEMENTIERUNG	Gruppenrechte auf Ordnern/Freigaben mit NTFS & Freigaberechten setzen
5. DOKUMENTATION	Alle Gruppen, Zuweisungen, Rechte erfassen und versionieren
6. REGELMÄßIGE ÜBERPRÜFUNG	Rechteverwaltung prüfen, veraltete Zugriffe entfernen (Rezertifizierung)

Tools zur Unterstützung

TOOL	ZWECK
ACTIVE DIRECTORY USERS AND COMPUTERS (ADUC)	Gruppen und Benutzer verwalten
GROUP POLICY MANAGEMENT CONSOLE (GPMC)	Gruppenrichtlinien konfigurieren
POWERSHELL	Automatisierung & Abfragen großer Umgebungen
DSACLS / ACCESSCHK	Analyse effektiver Berechtigungen auf Objekte
AD-DOKUMENTATIONSTOOLS	z. B. XIA Configuration, AD Info, ADRecon

Festlegen von Gruppenrichtlinien (GPOs)

Gruppenrichtlinien (Group Policy Objects – GPOs) sind eine zentrale Verwaltungsmethode in Active Directory (AD), mit der Systemeinstellungen, Sicherheitsrichtlinien und Benutzerverhalten automatisch gesteuert werden.

GPOs werden auf Benutzer oder Computer angewendet – abhängig von ihrer Position in der AD-Hierarchie (Domäne, OU, Standort).

Ziele von GPOs

ZIEL	BESCHREIBUNG
SICHERHEIT ERHÖHEN	Einschränkung unsicherer Funktionen (z. B. USB, Systemsteuerung, CMD)
STANDARDISIERUNG	Einheitliche Konfiguration von Benutzerumgebungen und Desktops
AUTOMATISIERUNG	Zentrale Steuerung von Updates, Programmen, Netzlaufwerken usw.
BENUTZERFREUNDLICHKEIT	Vorkonfigurierte Systeme entlasten Benutzer

GPO-Struktur

Verknüpfungsebenen (in Hierarchie)

- Standort (selten genutzt)
- Domäne (z. B. firma.local)
- Organisationseinheit (OU) (z. B. Benutzer, Clients, Server)

Merke: Die Richtlinie auf der untersten Ebene (OU) überschreibt – sofern nicht blockiert – die übergeordnete.

Typen von Richtlinieneinstellungen

BEREICH	BEISPIELE
COMPUTERKONFIGURATION	Firewall-Regeln, Update-Richtlinien, Geräteinstallation
BENUTZERKONFIGURATION	Desktop-Hintergrund, Startmenü, Softwareverknüpfungen
SICHERHEITSRICHTLINIEN	Kennwortrichtlinien, Sperrzeit, Laufwerkszugriff
SKRIPTE	Anmelde-, Abmelde-, Start- und Herunterfahrskripte
ORDNERUMLEITUNGEN	Dokumente, Desktop auf Netzlaufwerk umleiten
SOFTWAREVERTEILUNG	MSI-Pakete installieren oder deinstallieren über GPO

Erstellen & Verwalten von GPOs (Ablauf)

SCHRITT	BESCHREIBUNG
1. GPMC ÖFFNEN	Group Policy Management Console auf Domänencontroller
2. NEUE GPO ERSTELLEN	Rechte Maustaste auf Domäne/OU → „Neue GPO erstellen und hier verknüpfen“
3. GPO KONFIGURIEREN	Richtlinien über Editor setzen (z. B. Benutzer- oder Computereinstellungen)
4. VERERBUNG PRÜFEN/ANPASSEN	Welche Richtlinien greifen? (Erweiterte Einstellungen, Priorität, Block)
5. GÜLTIGKEIT TESTEN	Testnutzer, gpresult /r, rsop.msc verwenden

Beispiele für sinnvolle Gruppenrichtlinien

ZIEL	GPO-EINSTELLUNG
USB-ZUGRIFF SPERREN	Administrative Vorlagen → System → Wechseldatenträger deaktivieren
FIREWALL ERZWINGEN	Windows-Einstellungen → Sicherheitsrichtlinien
HINTERGRUNDBILD FESTLEGEN	Benutzerkonfiguration → Desktop → Desktop-Hintergrund festlegen
WINDOWS-UPDATES VERWALTEN	Computerkonfiguration → Windows Update → Automatische Updates
KENNWORTRICHTLINIE SETZEN	Sicherheitsrichtlinie → Kennwortkomplexität, Alter, Mindestlänge

Erzwingen von Passwortrichtlinien

Passwortrichtlinien definieren Mindestanforderungen an Benutzerkennwörter. Ihr Ziel ist es, sichere, komplexe und regelmäßig aktualisierte Passwörter zu erzwingen, um unbefugten Zugriff auf Benutzerkonten zu verhindern. In Windows-Domänenumgebungen werden Passwortrichtlinien typischerweise über Gruppenrichtlinien (GPOs) definiert.

Einstellmöglichkeiten in Active Directory (per GPO oder Default Domain Policy)

EINSTELLUNG	BEDEUTUNG	BEISPIELWERT
KENNWORTLÄNGE	Mindestanzahl Zeichen	z. B. 10 Zeichen
KENNWORTKOMPLEXITÄT AKTIVIEREN	Kombination aus Groß-/Kleinschreibung, Zahl, Sonderzeichen	Aktiviert
MAXIMALES KENNWORTALTER	Wie lange darf ein Passwort maximal gültig sein?	90 Tage
MINIMALES KENNWORTALTER	Verhindert zu schnelle Passwortänderungen	1 Tag
ANZAHL GESPEICHERTER KENNWÖRTER (HISTORIE)	Wie viele alte Passwörter werden gesperrt?	z. B. 24
KONTOSPERRUNGSRICHTLINIE	Schutz gegen wiederholte Fehlversuche (z. B. 5 Falscheingaben)	z. B. 5 Versuche, 30 Min Sperre

Einrichten in der Gruppenrichtlinien-Verwaltung

1. GPMC öffnen (Group Policy Management Console)
2. Default Domain Policy oder neue GPO auf Domänenebene verknüpfen
3. Navigieren zu: Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Kontorichtlinien → Kennwortrichtlinien
4. Richtlinien wie oben beschrieben setzen
5. Änderungen am Client in CMD mit gpupdate /force anwenden

Best Practices für sichere Passwortrichtlinien

EMPFEHLUNG	BEGRÜNDUNG
MINDESTENS 10–12 ZEICHEN ERZWINGEN	Erhöht Sicherheit massiv bei gleicher Benutzerfreundlichkeit
KOMPLEXITÄT ERZWINGEN (MIND. 3 ZEICHENTYPEN)	Vermeidung einfacher Kombinationen
PASSWÖRTER NIEMALS AUFSCHREIBEN	Verwendung eines Passwort-Managers bei Bedarf
ZWEI-FAKTOR-AUTHENTIFIZIERUNG ERGÄNZEN	Weitere Schutzebene bei besonders kritischen Systemen
HISTORIE AKTIVIEREN	Verhindert Zurückwechseln auf vorherige Passwörter

Kenntnisse über User Account Control (UAC)

User Account Control (UAC) ist eine Sicherheitsfunktion in Windows, die hilft, das System vor unautorisierten Änderungen zu schützen. UAC stellt sicher, dass Programme nur mit expliziter Benutzerfreigabe administrative Rechte erhalten, selbst wenn der Benutzer über ein Administratorkonto verfügt.

Ziel und Nutzen von UAC

ZIEL	BESCHREIBUNG
SCHUTZ VOR MALWARE	Programme dürfen nicht automatisch Änderungen am System vornehmen
BEWUSSTES HANDELN FÖRDERN	Benutzer wird aktiv nach Zustimmung gefragt – verhindert „Hintergrundaktionen“
STANDARDNUTZER STÄRKEN	Auch Administratoren arbeiten im Alltag mit normalen Rechten
SYSTEMINTEGRITÄT SICHERN	Nur bestätigte Aktionen ändern Systemdateien, Registry oder Dienste

Wie funktioniert UAC? (Ablauf)

1. Ein Programm möchte eine geschützte Aktion ausführen (z. B. Software installieren, Dienste ändern).
2. UAC erkennt den „Elevationsbedarf“.
3. Es erscheint ein Bestätigungsdialog:
    a. Als Admin: „Möchten Sie diese Aktion zulassen?“
    b. Als Standardbenutzer: Eingabe eines Admin-Benutzers erforderlich
4. Nur bei Zustimmung wird die Aktion mit Administratorrechten ausgeführt.

UAC-Stufen (Konfigurierbar)

STUFE	VERHALTEN
NIE BENACHRICHTIGEN	Alle Programme erhalten sofort Adminrechte – unsicher!
NUR BEI PROGRAMMEN OHNE SIGNATUR	Warnung bei unbekannten oder potenziell gefährlichen Programmen
STANDARD (EMPFOHLEN)	Immer nach Erhöhung fragen, Desktop wird verdunkelt („Secure Desktop“)
IMMER BENACHRICHTIGEN	Auch bei Benutzeraktionen wird gefragt (z. B. Systemeinstellungen ändern)

Konfiguration:

Systemsteuerung → Benutzerkonten → Benutzerkonten → Einstellungen der Benutzerkontensteuerung ändern

Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

Client-PCs sind oft das Einfallstor für Sicherheitslücken in Netzwerken. Sie werden direkt von Anwendern genutzt und sind damit besonders anfällig für Manipulation, Schadsoftware und unbefugte Nutzung.

Technische Schutzmaßnahmen

Betriebssystem absichern

MAßNAHME	WIRKUNG
BENUTZERKONTENSTEUERUNG (UAC)	Verhindert stillschweigende Systemänderungen
STANDARDBENUTZER STATT ADMIN	Alltagsarbeit mit eingeschränkten Rechten
SICHERHEITSUPDATES AUTOMATISIEREN	Schließen von Schwachstellen
SICHERHEITSRICHTLINIEN ÜBER GPOS	Zentral gesteuerte Vorgaben in Unternehmensnetzwerken

Netzwerk- und Internetzugriff kontrollieren

MAßNAHME	FUNKTION
CLIENT-FIREWALL AKTIVIEREN	Kontrolliert eingehenden und ausgehenden Netzwerkverkehr
WEBFILTER EINSETZEN	Sperrt unsichere oder unerwünschte Webseiten
NETZWERKZUGANG ÜBER VLANS	Isoliert Clients in logische Sicherheitszonen
VPN-NUTZUNG ABSICHERN	Sichere Verbindung ins Unternehmensnetz über TLS/IPsec

Malware- und Virenschutz

KOMPONENTE	BEDEUTUNG
ECHTZEIT-VIRENSCANNER	Erkennt und blockiert Schadsoftware beim Zugriff
SIGNATUR-UPDATES AUTOMATISIEREN	Schützt vor neuen Bedrohungen
VERHALTENSANALYSE (HEURISTIK)	Erkennung unbekannter Malware anhand typischen Verhaltens
USB-SCHUTZ	Automatischer Scan und ggf. Sperre von Wechseldatenträgern

Zugriffsschutz & Authentifizierung

MAßNAHME	BESCHREIBUNG
STARKE PASSWORTRICHTLINIEN (GPO)	Mindestlänge, Komplexität, Ablaufdatum
MEHRFAKTOR-AUTHENTIFIZIERUNG (MFA)	Erhöht Sicherheit beim Login durch zusätzlichen Faktor
BILDSCHIRMSPERRE NACH INAKTIVITÄT	Automatische Sperre bei Nichtbenutzung
BIOS-/UEFI-PASSWORT	Verhindert Startänderungen und Boot von externen Medien

Daten- und Systemsicherheit

MAßNAHME	WIRKUNG
VERSCHLÜSSELUNG (BITLOCKER)	Schutz der Festplatte bei Diebstahl oder unbefugtem Zugriff
EFS (ENCRYPTING FILE SYSTEM)	Datei-/ordnerbasierte Verschlüsselung unter NTFS
BACKUP EINRICHTEN	Datenwiederherstellung bei Verlust, Ransomware oder Defekt
SYSTEMABBILD ERSTELLEN	Schnelle Wiederherstellung bei Systemfehlern oder Malwarebefall

Organisatorische Maßnahmen

MAßNAHME	BESCHREIBUNG
MITARBEITERSCHULUNG	Aufklärung über Phishing, sichere Passwortwahl, Umgang mit Daten
ZUGRIFFSPROTOKOLLIERUNG (AUDITING)	Erfassung und Analyse von Benutzeraktionen und Systemereignissen
NUTZUNGSRICHTLINIEN (IT-POLICY)	Klar definierte Regeln zur Nutzung von IT-Ressourcen
INVENTARISIERUNG UND MONITORING	Überwachung der eingesetzten Systeme und Software

Kenntnisse über Methoden der sicheren Löschung von Daten

Die sichere Löschung von Daten ist essenziell, um die Wiederherstellung sensibler Informationen zu verhindern – etwa beim Gerätewechsel, bei der Entsorgung oder bei der Weitergabe von Datenträgern. Einfaches Löschen (z. B. durch das Leeren des Papierkorbs) entfernt nur die Verweise, nicht jedoch die eigentlichen Datenblöcke.

Ziel der sicheren Löschung

ZIEL	BESCHREIBUNG
DATENSCHUTZ	Vertrauliche Informationen (z. B. personenbezogene Daten) unlesbar machen
RECHTSKONFORMITÄT	Einhaltung von DSGVO, BSI-Empfehlungen, ISO-Normen
TECHNISCHE SICHERHEIT	Schutz vor Datenlecks bei Weitergabe, Recycling oder Diebstahl

Unterschied zwischen Löschen, Überschreiben und Vernichten

AKTION	WIRKUNG
LÖSCHEN (STANDARD)	Verzeichnis-Eintrag entfernt, Daten bleiben physisch erhalten
ÜBERSCHREIBEN	Datenblöcke werden durch Zufallsdaten oder Muster ersetzt
VERNICHTEN	Datenträger wird physisch zerstört oder unbrauchbar gemacht

Methoden zur sicheren Datenlöschung

Softwarebasierte Methoden (logisch)

METHODE	BESCHREIBUNG
1X ÜBERSCHREIBEN (Z. B. MIT NULLEN)	Schnelle Methode, für Alltagsgebrauch ausreichend
MEHRFACHÜBERSCHREIBEN (Z. B. 3X, 7X)	BSI-konform, überschreibt Daten mehrfach mit Zufallswerten
DOD 5220.22-M	US-Standard mit 3–7 Durchläufen
GUTMANN-METHODE (35X)	Extrem aufwändig, überholt für moderne Medien
CRYPTO-ERASE (BEI SSDS)	Schlüssel löschen statt Daten selbst

Beliebte Tools:

- Windows CMD: cipher /w:C:\ (freier Speicher löschen)
- Linux Terminal: shred, wipe, dd
- Spezialsoftware: DBAN, Eraser, Blancco, KillDisk

Physikalische Methoden

METHODE	BESCHREIBUNG
ENTMAGNETISIEREN (DEGAUSSING)	Magnetfeld löscht HDD-Daten – wirkt nicht bei SSDs
ZERSTÖRUNG (SHREDDER, HAMMER)	Mechanische Zerstörung, z. B. durch Schreddern, Lochen, Verbiegen
VERBRENNEN / SCHMELZEN	Komplette thermische Vernichtung – nur für sehr sensible Daten

Inhalte von Unternehmensrichtlinien für Datenträgerentsorgung

Eine Unternehmensrichtlinie zur Datenträgerentsorgung regelt den korrekten, sicheren und gesetzeskonformen Umgang mit Datenträgern, die außer Betrieb genommen, ersetzt oder entsorgt werden. Ziel ist der vollständige Schutz sensibler Daten vor unbefugtem Zugriff – auch nach der Außerbetriebnahme.

Ziele der Richtlinie

ZIEL	BEDEUTUNG
DATENSICHERHEIT	Schutz vor Datenabfluss bei Hardwareweitergabe oder Entsorgung
RECHTSSICHERHEIT	Einhaltung gesetzlicher Vorgaben (z. B. DSGVO, BDSG, ISO 27001)
VERFAHRENSSTANDARDISIERUNG	Einheitliches Vorgehen im gesamten Unternehmen
DOKUMENTATION & NACHWEISBARKEIT	Rückverfolgbarkeit jeder Löschung oder Zerstörung

Wichtige Inhalte einer solchen Richtlinie

1.Geltungsbereich

- Für alle IT-gestützten Datenträger: HDDs, SSDs, USB-Sticks, Speicherkarten, CDs/DVDs, Backup-Bänder, Smartphones, Tablets
- Gilt für alle Unternehmensbereiche, Mitarbeiter und externen Dienstleister

2.Klassifizierung von Datenträgern

- Nach Schutzbedarf der gespeicherten Daten (z. B. intern, vertraulich, streng vertraulich)
- Unterscheidung zwischen mobilen und fest installierten Datenträgern
- Aufbewahrungs- vs. Vernichtungsfristen (Archivsysteme)

3.Anweisungen zur sicheren Datenlöschung

LÖSCHVERFAHREN	BESCHREIBUNG
SOFTWAREBASIERTE LÖSCHUNG	z. B. mehrfaches Überschreiben mit zertifizierten Tools
SECURE ERASE	Spezielle Befehle für SSDs, um Controller-intern zu löschen
PHYSIKALISCHE ZERSTÖRUNG	Schreddern, Lochen, Entmagnetisieren oder thermische Verfahren
PROTOKOLLIERUNG	Jeder Löschvorgang muss dokumentiert werden (Wer, Was, Wann)

4.Lagerung und Transport vor Entsorgung

- Sicher verschlossen und vor unbefugtem Zugriff geschützt
- Getrennte Lagerung von noch zu löschenden und bereits gelöschten Medien
- Protokollierter Transport, ggf. durch zertifizierte Anbieter

5.Entsorgungsnachweis und Dokumentation

Verpflichtende Lösch- oder Vernichtungsprotokolle mit:

- Seriennummer / Inventarnummer
- Datenträgertyp
- Löschmethode / Zerstörungsart
- Datum, Name, Unterschrift
- Archivierung der Protokolle für mindestens 3–5 Jahre

6.Zuständigkeiten und Rollen

ROLLE	AUFGABEN
IT-ADMINISTRATOR	Durchführung, Prüfung, Dokumentation von Löschmaßnahmen
INFORMATIONSSICHERHEITS-BEAUFTRAGTER	Überwachung, Prüfung der Einhaltung der Richtlinie
EXTERNE DIENSTLEISTER	Nur nach AV-Vertrag (Auftragsverarbeitung), mit Nachweis der Fachentsorgung

7.Besondere Sicherheitsmaßnahmen

- Keine Entsorgung über normalen Hausmüll
- Keine Wiederverwendung ohne vorherige zertifizierte Datenlöschung
- Verwendung von zertifizierten Dienstleistern (nach ISO 27001 / DIN 66399)
- Festgelegte Verstöße und Konsequenzen (z. B. Disziplinarmaßnahmen)