

AP1 Vorbereitung

Samir Loukili

Inhalt

Cloud Service Modelle:.....	2
Netzwerktechnik:	3
Schnittstellen/Bussysteme:	8
Datenbanken:	9
UML – Unified Modelling Language:	10
Softwareentwicklung:.....	11
Wirtschaft:.....	13
IT-Security:.....	15
Projektplanung:.....	20
Hardware:.....	25
Weitere nützliche Begriffe:	27
Tipps für die Prüfung:.....	29

Cloud Service Modelle:

- **Public Cloud:**
externe Anbieter stellen Ressourcen wie Server, Speicher, Anwendungen über das öffentliche Internet zur Verfügung
- **Private Cloud:**
dedizierte Cloud-Computing Umgebung die von einer Organisation allein genutzt wird um Datenschutz und IT-Sicherheit zu erhöhen, entweder im eigenen Rechenzentrum (on-premise) oder durch externe Dritte gehostet
- **Hybrid Cloud:**
gewisse Services werden über öffentliche Anbieter empfangen, datenschutzkritische Anwendungen und Daten aber weiterhin im eigenen Unternehmen betrieben, gehostet und verarbeitet
- **IaaS – Infrastructure as a Service:**
Der Anbieter liefert die Infrastruktur wie Storage, Virtualisierung, Server und Netzwerk über die Cloud, der Nutzer verwaltet die Entwicklungsumgebung, Anwendungen, Daten, Skalierbarkeit und Laufzeit selbst
Beispiel: Amazon Web Services, Microsoft Azure
- **PaaS – Platform as a Service:**
Der Anbieter liefert die Infrastruktur und ist für den Aufbau, Updates und Wartung der Entwicklungsumgebung zuständig. Der Nutzer ist für die Entwicklung, Ausführung und Verwaltung eigener Anwendungen verantwortlich
Beispiel: Force.com, Google App Engine
- **SaaS – Software as a Service:**
Der Anbieter stellt Infrastruktur, Umgebung und Anwendungen selbst, diese Anwendung(en) werden vom Nutzer über den Browser oder eine API nur noch verwendet/ausgeführt, Updates, Fehlerbehebungen und Wartungen führt der Anbieter durch
Beispiel: Microsoft OneDrive, Google Drive

Netzwerktechnik:

- **OSI (Open Systems Interconnection)-Schichten-Modell:**

Schicht	Deutsch	Englisch	Protokolle
7	Anwendung	Application	HTTP, DNS, DHCP, Telnet
6	Darstellung	Presentation	ASCII, PNG, MP4
5	Sitzung	Session	SSL, TLS
4	Transport	Transport	TCP, UDP
3	Vermittlung	Network	IPv4, IPv6, ICMP
2	Sicherung	Data-Link	Ethernet, ARP, MAC
1	Bitübertragung	Physical	Koaxial, Twisted Pair, Glasfaser

- **TCP – Transmission Control Protocol:**
verbindungsorientiert, gewährleistet zuverlässige, geordnete, fehlerfreie Übertragung, HTTP/HTTPS, SSH
- **UDP – User Datagram Protocol:**
verbindungslos, schnelles Transportprotokoll, Streaming, Online-Gaming, DNS geringe Latenz aber möglicher Paketverlust (kein Handshake)
- **DNS – Domain Name System:**
löst Domainnamen in zugehörige IP-Adresse auf
- **DHCP – Dynamic Host Configuration Protocol:**
automatische Zuweisung von Netzwerkkonfigurationen (IP-Adresse, Subnetzmaske, Gateway, DNS) an Clients
- **HTML – Hypertext Markup Language:**
Auszeichnungssprache zur Strukturierung von Webinhalten wie Bildern, Texten und Hyperlinks, wird vom Browser interpretiert
- **CSS – Cascading Style Sheets:**
definiert das visuelle Erscheinungsbild von HTML-Dokumenten, trennt Inhalt (HTML) von Design
- **HTTP – Hypertext Transfer Protocol:**
grundlegendes Protokoll zur Datenübertragung zwischen Webbrowsern (Client) und Servern, basiert auf Anfragen (Requests) und Antworten (Responses), zustandslos, überträgt meist HTML-Dokumente
- **HTTPS – Hypertext Transfer Protocol Secure:**
sichere Version von http, Verschlüsselung durch SSL/TLS, verhindert Abfangen sensibler Daten
- **SSL – Secure Sockets Layer:**
Sicherheitsprotokoll für Datenaustausch zwischen Webbrowsern und Servern, gewährleistet Datenschutz und Integrität
- **TLS – Transport Layer Security:**
Nachfolger von SSL, sicherer als SSL, gewährleistet Vertraulichkeit, Authentizität und Integrität, durch TLS-Handshakes werden Schlüssel ausgetauscht und Server authentifiziert

- **ARP – Address Resolution Protocol:**
verbindet IPv4-Adressen (Schicht 3) mit physischen MAC-Adressen (Schicht 2), Gerät sendet Broadcast (ARP Request) um die MAC zu einer IP zu erfragen, Ziel antwortet direkt (ARP Reply)
- **SMTP – Simple Mail Transfer Protocol:**
fungiert als Postausgangsserver, übermittelt Emails vom Client zum Server oder zwischen Servern (Senden), zum Empfang werden POP3 und IMAP verwendet
- **POP3 – Post Office Protocol Version 3:**
downloadet Emails vom Server auf ein lokales Endgerät, standardmäßig werden die Mails dann vom Server gelöscht, erschwert den Zugriff auf Mails von mehreren Geräten, eignet sich für Nutzung auf nur einem Gerät
- **IMAP – Internet Message Access Protocol:**
ermöglicht die Verwaltung von Emails auf einem Mailserver, alle Ordner und Informationen werden synchronisiert, somit ist der Zugriff von mehreren Geräten möglich, Nachrichten bleiben zentral auf dem Server und werden bei Bedarf geladen
- **ICMP – Internet Control Message Protocol:**
zentrales Protokoll auf Schicht 3, von Netzwerkgeräten (Router, Hosts) zur Diagnose und Fehlerberichterstattung verwendet, übermittelt Statusinformationen, wenn Ziel nicht erreichbar ist, Basis für Tools wie **ping** oder **traceroute**
- **VPN – Virtual Private Network:**
ermöglicht eine verschlüsselte, sichere Verbindung (Tunnel) zwischen Endgerät und Internet über einen VPN-Server, dieser vergibt eine interne neue IP-Adresse und verbirgt dadurch die IP-Adresse und kann Geoblocking umgehen
- **SSH – Secure Shell:**
kryptografisches Netzwerkprotokoll zur sicheren Verbindung mit Servern und anderen Geräten in unsicheren Netzwerken, ersetzt unsichere Protokolle wie Telnet
- **Telnet:**
veraltetes, unverschlüsseltes Protokoll für textbasierten Fernzugriff auf Computer und Netzwerkgeräte über TCP/IP, heutzutage durch SSH ersetzt
- **RDP – Remote Desktop Protokoll:**
von Microsoft entwickeltes Protokoll für Fernzugriffe auf Windows Computer und Server
- **FTP – File Transfer Protokoll:**
Netzwerkprotokoll zur Datenübertragung zwischen Clients und Servern über IP-Netzwerke, standardmäßig unverschlüsselt, nutzt zwei Verbindungen, eine für Befehle, eine separate für Daten
- **SFTP – SSH File Transfer Protokoll:**
Port 22 (SSH), verschlüsselte Datenübertragung zwischen Clients und Servern, nutzt nur eine Verbindung für Befehle und Datentransfer
- **MQTT – Message Queuing Telemetry Transport:**
Netzwerkprotokoll speziell für **M2M (Machine-to-Machine)** Kommunikation bei IoT Geräten
- **LoRaWAN – Long Range Wide Area Network:**
stromsparendes Funknetzprotokoll für IoT über große Distanzen (15km), Smart City

- **Bluetooth, BLE – Bluetooth Low Energy:**
Funkstandard für IoT (seit Bluetooth 4.0), stromsparend
- **WIFI – Wireless Fidelity:**
drahtlose Netzwerktechnologie um Geräte per Funk mit dem Internet oder lokalen Netzwerken (**WLAN**) zu verbinden
- **ZigBee:**
drahtloses Mesh-Netzwerk für Gebäudeautomation, Beleuchtung oder Sensornetzwerke
- **RFID – Radio Frequency Identification:**
berührungslose Identifikation und Datenspeicherung mittels Radiowellen, Transponder sendet Daten + Lesegerät
- **NFC – Near Field Communication:**
basiert auf RFID, drahtloser Datenaustausch auf kurzer Distanz, kontaktloses Bezahlen, Zugangskontrollsysteme
- **MAC (Media Access Control)-Adressen:**
eindeutige, physikalische Identifikationsnummer für Netzwerkadapter (WLAN oder Ethernet-Karten)
Bsp.: 00-D8-61-1A-DC-1B
 - **Aufbau:** 48Bit, hexadezimal dargestellt, erste 24Bit Herstellerkennung (OUI – Organizationally Unique Identifier)
- **IPv4 (Internet Protokoll Version 4)-Adressen:**
binäre Adressen zur Identifizierung von Geräten in Netzwerken
Bsp.: 192.168.0.1
 - **Aufbau:** 32Bit, 4 Oktette mit je 8Bit Länge, bestehen aus Netzteil (identifiziert das Netzwerk) und Hostteil (identifiziert das Gerät)
 - **Subnetzmaske:** gibt an welcher Teil Netzteil und welcher Hostteil ist, Bsp.: 255.255.255.0 → die ersten 3 Oktette sind Netzteil, das letzte Hostteil
 - **Suffix: CIDR-Notation (Classless Inter-Domain Routing),** Zeigt an wie viele Bits zum Netzteil der Adresse gehören, Bsp.: 192.168.0.1/24 → 24Bits also die ersten 3 Oktette gehören zum Netzteil, andere Darstellung der Subnetzmaske
 - **APIPA – Automatic Private IP Addressing:**
Windows-Funktion die, wenn kein DHCP-Server erreichbar ist, eine IP-Adresse zwischen 169.254.0.1 und 169.254.255.254 vergibt, ermöglicht lokale Kommunikation in kleinen Netzwerken, Subnetzmaske: 255.255.0.0, kein Zugriff auf das Internet oder andere Netze möglich da kein Gateway zugewiesen wird

- **IPv6 (Internet Protokoll Version 6)-Adressen:**

hexadezimale Adressen zur Identifizierung von Geräten in Netzwerken

Bsp.: 2a02:810b:4b02:99a0:9f15:ba62:40aa:1c1a

- **Aufbau:** 128Bit, 8 Blöcke je 16Bit, jedes Zeichen repräsentiert 4Bit
- **Netzwerk Präfix:** Standard ist /64 (Netzteil bei IPv4)
 - **Standortpräfix:** Präfix des Standorts des Unternehmens
 - **Teilnetz-ID:** identifiziert das interne Subnetz innerhalb des Standorts
- **Interface Identifier:** Identifiziert das Gerät (Hostteil bei IPv4)

Beispiel zur Veranschaulichung:

IPv6-Adresse: **2a02:810b:4b02:99a0:9f15:ba62:40aa:1c1a**

Netzwerkpräfix: **2a02:810b:4b02:99a0**

Standortpräfix: **2a02:810b:4b02**

Teilnetz-ID: **:99a0**

Interface Identifier: **:9f15:ba62:40aa:1c1a**

- **Unique Local: fc00::/7**, private Adressen
- **Global-Unicast: 2000::/3** (fängt immer mit 2xxx oder 3xxx an), weltweit eindeutige, im IPv6-Internet routbare Adresse, ermöglicht direkte Kommunikation im Internet
- **Link Local: fe80::/10** (muss immer vorhanden sein), wie APIPA bei IPv4
- **Loopback-Adresse: ::1** (31x 0 dann 1)
- **Adressvergabe:** DHCPv6, SCLAAC (Stateless Address Autoconfiguration), statisch
- **Standard-Gateway:** Link-Local-Adresse des Routers
- **Multicast:** löst Broadcast-Adresse ab, zentraler Mechanismus um mehrere Adressen gleichzeitig anzusprechen
- **Adresskonflikte:**
 - **NDP – Neighbor Discovery Protocol**
 - **DAD – Duplicate Address Detection**
 - NDP und DAD kombiniert verhindern Adressdopplungen
- **Datenschutz:**
 - **Privacy Extensions:** zufällige Zuweisung von Adressen um nicht immer die gleiche Adresse zu verwenden

○ **Kürzung der Schreibweise:**

Bei IPv6 Adressen können führende Nullen in Blöcken gekürzt werden

2a02:010b:4b02:99a0:0f15:ba62:00aa:1c1a wird zu:

2a02:10b:4b02:99a0:f15:ba62:aa:1c1a

Außerdem dürfen Blöcke, die nur aus Nullen bestehen durch :: ersetzt werden:

2a02:0000:0000:99a0:bf15:0000:67aa:1c1a wird zu:

2a02::99a0:bf15:0000:67aa:1c1a

es darf aber immer nur an **einer Stelle** ersetzt werden da sonst nicht klar ist, wie die Verteilung der Blöcke aussieht.

Würden wir die Adresse jetzt so kürzen:

2a02::99a0:bf15::67aa:1c1a

wäre nicht klar ob die Adresse ausgeschrieben so:

2a02:0000:0000:99a0:bf15:0000:67aa:1c1a

oder so:

2a02:0000:99a0:bf15:0000:0000:67aa:1c1a

aussieht.

Weitere Nuller-Blöcke dürfen aber trotzdem auf eine Null gekürzt werden, die drei gekürzten Nullen gelten dann als führende:

2a02::99a0:bf15:0:67aa:1c1a

- **Ports die man kennen sollte:**

Port	Protokoll
20/21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	http
110	POP3
143	IMAP
443	HTTPS
3389	RDP

Schnittstellen/Bussysteme:

- **GPIO – General Purpose Input Output:**
universell programmierbare Pins auf Mikrocontrollern die als Ein- oder Ausgänge verwendet werden können
- **UART – Universal Asynchronous Receiver / Transmitter:**
Protokoll für serielle Datenübertragung zwischen Mikrocontrollern und Geräten
- **I2C – Inter- Integrated Circuit:**
2-Draht-Busprotokoll zur seriellen Kommunikation zwischen Mikrocontrollern und Peripheriegeräten (Sensoren, Displays)
- **SPI – Serial Peripheral Interface:**
4-Draht-Kommunikationsprotokoll zur seriellen Übertragung zwischen einem Master und einem Slave über kurze Distanz
- **OneWire:**
1-Draht-Bus, serielle Schnittstelle die eine einzelne Datenader als Stromversorgung, Sende- und Empfangsleitung verwendet

Datenbanken:

Datenbanken sind digitale Systeme zur Speicherung und Organisation von Daten, die Daten werden in strukturierten Tabellen gespeichert, ermöglicht schnellen Zugriff und eine effiziente Verwaltung des Datenbestands, jede Tabelle hat dabei einen Primärschlüssel mit dem die Tabelle eindeutig identifizierbar ist

- **DBS – Datenbanksystem:**
Gesamtpaket aus Datenbank (den Daten) und dem Datenbankmanagementsystem (Software)
- **DBMS – Datenbankmanagementsystem:**
Software zur Verwaltung, Strukturierung und Abfrage großer Datensätze
- **Normalisierung in Datenbanken:**
logische Aufteilung in zusammenhängende Tabellen, verhindert **Redundanz** (doppelte Speicherung) und **Anomalien** (Fehler bei Änderung und Löschung) in den Datensätzen und verbessert damit die Datenkonsistenz und den Speicherplatzbedarf
- **ERM – Entity Relationship Model:**
Modell zur Darstellung von Entitäten, Attributen und Beziehungen von Datenstrukturen in einer relationalen Datenbank
Entität: individuell identifizierbares Objekt der Wirklichkeit
Attribut: Eigenschaft einer Entität
Beziehung: Verknüpfung zwischen Entitäten
Kardinalitäten: legen fest welche Beziehungsart vorliegt:
1:1, 1:n oder n:m
- **RM – Relationenmodell/relationales Modell:**
wird nach bestimmten Regeln aus dem ERM abgeleitet, stellt die Entitäten in Tabellenform mit ihren Attributen, Primärschlüsseln und Fremdschlüsseln und Beziehungen dar

UML – Unified Modelling Language:

grafische Modellierungssprache um Softwareteile und andere Systeme zu visualisieren, sie wird zur Planung aber auch zur Dokumentation verwendet, es gibt mehrere Diagramme die durch UML genormt sind:

- **UML-Use-Case-Diagramm:**
abstraktes Diagramm zur Darstellung von Anwendungsfällen, den involvierten Akteuren und ihren Beziehungen, es beschreibt das **Was** aber nicht wie oder womit ein System umgesetzt wird
- **UML-Aktivitätsdiagramm:**
dient der Darstellung des Verhaltens eines Systems von einem Startknoten hin zu einem Endknoten mit allen Entscheidungspfaden und weiteren Prozessen dargestellt werden
- **UML-Klassendiagramm:**
Strukturdiagramm, welches Klassen in der Objektorientierung mit ihren Attributen und Methoden und ihre Beziehungen zu anderen Klassen darstellt

Softwareentwicklung:

- **Schreibtischtest:**
manuelle Durchlaufkontrolle eines Programmcodes bei der schrittweise der Code durchlaufen wird und die Werte von Variablen in einer Tabelle notiert werden um logische Fehler, Schleifen oder Grenzwertprobleme zu identifizieren
- **Programmiersprachen:**
 - **Maschinensprache:**
binär, kann vom PC gelesen & verarbeitet werden
 - **Assemblersprache:**
für Menschen besser lesbar, wird von einem Assembler in Maschinensprache übersetzt
 - **Hochsprache:**
unabhängig vom Prozessor, menschlicher Sprache sehr nah, wird durch Compiler oder Interpreter in Maschinensprache übersetzt
- **Programmierparadigmen:**
 - **Imperative Programmiersprachen:**
Folge von Anweisungen beschreibt, zu welchem Zeitpunkt was vom Rechner ausgeführt werden soll, ältestes Programmierparadigma
Beispiel: C, C++, Java, Python
 - **Deklarative Programmiersprachen:**
Geben im Gegensatz zu imperativen nicht den Lösungsweg, sondern das gewünschte Ergebnis an
Beispiel: SQL, HTML, CSS
 - **Objektorientierte Programmiersprachen:**
kapseln Daten & Programmcode in übersichtlichen, wiederverwendbaren Objekten
Beispiel: Java, C++, C#, Python
- **Phasen der Softwareentwicklung:**
 - Anforderungsanalyse
 - Entwurf
 - Implementierung
 - Test
 - Dokumentation
 - Integration und Betrieb
 - Wartung und Support
- **Systemsoftware:**
 - Betriebssysteme
 - Gerätetreiber
 - Dienstprogramme
- **Standardsoftware:**
vorgefertigte, für den breiten Markt entwickelte und sofort einsatzbereite Software, die zentrale Funktionen für viele Nutzer und Unternehmen abdeckt
 - Microsoft Office
 - Adobe Acrobat Reader
 - SAP

- **Individualsoftware:**
speziell für einen Kunden entwickelte oder angepasste Software
- **Open-Source-Software:**
frei nutzbar, Quellcode ist öffentlich und darf verwendet, modifiziert und veröffentlicht werden
Beispiel: Linux, Firefox, LibreOffice
- **Freeware:**
kostenlos nutzbar, Urheberrecht verbleibt aber beim Entwickler, Quellcode nicht einsehbar
Beispiel: VLC Media Player, Adobe Reader
- **Shareware:**
kostenlose Nutzung ist entweder zeitlich oder funktionell begrenzt (Testphase)
Beispiel: verschiedene Antivirenprogramme, WinRAR
- **Closed-Source/Proprietäre Software:**
Quellcode ist nicht öffentlich, meist kostenpflichtig (Lizenzgebühren), Urheberrecht liegt beim Anbieter
Beispiel: Microsoft Windows, Adobe Photoshop, Microsoft Office
- **Compiler:**
übersetzen den Quellcode zu Beginn komplett in Maschinensprache jedoch ohne den Code auszuführen & werden danach, zur Laufzeit, nicht mehr benötigt
- **Interpreter:**
übersetzen den Quellcode Zeile für Zeile zur Laufzeit
- **Linker:**
führt Programmteile wie Quellcode-Dateien & Bibliotheken zu einer ausführbaren Datei (.exe) zusammen
- **Debugger:**
Erlaubt es, den Quellcode Schritt für Schritt auszuführen und die einzelnen Programmzustände zu untersuchen, so können logische Fehler besser gefunden werden
- **IDE – Integrated Development Environment:**
Software in der Entwickler Quellcode schreiben, ausführen, testen und debuggen können, typische Bestandteile sind Compiler, Interpreter, Linker, Debugger, Code-Editor
- **Bibliotheken:**
Sammlung von Funktionen oder Klassen für gewissen Einsatzzwecke z.B. mathematische Funktionen (cmath), sie können flexibel in unterschiedlichen Projekten verwendet werden
- **Frameworks:**
Grundgerüst für Softwarelösungen, für häufig wiederholende Aufgaben, stellt Struktur zur Verfügung, die von sämtlichen Anwendungen gleichermaßen genutzt werden kann, Spiele-Engines wie Unity, Godot etc. sind Frameworks, Frameworks umfassen auch Bibliotheken die der Entwickler direkt verwenden kann

Wirtschaft:

- **Miete:**
flexible Laufzeit, Vermieter trägt die Verantwortung für Wartung, Reparatur und Instandhaltung, Objekt wird am Ende der Laufzeit zurückgegeben
- **Leasing:**
langfristige, feste Vertragslänge, der Leasingnehmer trägt die Verantwortung für Reparaturen und Wartung, am Ende der Laufzeit wird das Objekt zurückgegeben oder optional gekauft (Restwert)
- **Kauf:**
Gut gehört dem Käufer, dieser trägt die volle Verantwortung (Wertverlust, Reparaturen), profitiert aber vom Wiederverkaufswert
- **Kaufverträge:**
kommen zustande bei beidseitiger Willenserklärung von Käufer und Verkäufer, dies kann beispielsweise bei einem Angebot und Annahme des Angebots erfolgen
- **Vertragsstörungen:**
Lieferverzug, Zahlungsverzug, Annahmeverzug, mangelnde Lieferung
- **Angebotsbewertung:**
 - **Quantitativ:**
 - Betrachtung von Faktoren wie Listeneinkaufspreis, Bezugskosten (Transport, Verpackung), Rabatte, Skonto
 - Kalkulationsschema:
Listeneinkaufspreis
- Rabatt
= Zieleinkaufspreis
- Skonto
= Bareinkaufspreis
+ Bezugskosten
= Bezugspreis
 - **Qualitativ (Nutzwertanalyse):**
Durchführung einer Nutzwertanalyse. Bewertung der Angebote durch Entscheidungskriterien, diese haben unterschiedlich hohe Bedeutungen, daher werden sie in der Rechnung gewichtet
Mögliche Entscheidungskriterien:
 - Mindestbestellmenge
 - Zahlungsbedingungen
 - Fristen
 - Qualität
 - Nachhaltigkeit
 - Zuverlässigkeit
 - Flexibilität
 - Lieferbedingungen
 - Serviceleistungen

- **Direkter Vertrieb:**
direkter Verkauf an den Kunden, ohne Zwischenhändler z.B. eigener Online-Shop, Werksverkauf
Vorteile:
 - Volle Margenkontrolle
 - Kundennähe
- **Indirekter Vertrieb:**
Verkauf über Zwischenhändler (Groß-/Einzelhändler, Reseller)
Vorteile:
 - Schnellere Skalierung
 - Höhere Reichweite
 - Geringere Fixkosten
- **Kosten von IT-Systemen:**
 - **Einmalige Kosten:**
 - Anschaffungskosten für Hard- und Software
 - Installationsaufwand
 - **Laufende Kosten:**
 - Stromverbrauch
 - Support und Wartungsverträge
 - Lizenzkosten für Software
- **Urheberrecht in der Softwareentwicklung:**
geschützt werden Quellcode, Dokumentation, Datenbanken und Anwendungsdesign
- **CRM – Customer-Relationship-Management:**
Dokumentation und Verwaltung von Kundenbeziehungen um Kundenbindung zu pflegen und zu stärken
- **ERP – Enterprise Resource Planning:**
zentrale Steuerung und Integration aller Geschäftsprozesse wie Einkauf, Produktion, Lager und Buchhaltung
- **DMS – Dokumenten Management System:**
datenbankgestützte Verwaltung elektronischer Dokumente
- **CMS – Content Management System:**
Erstellung, Bearbeitung, Organisation und Auslieferung digitaler Inhalte (Content) für Webseiten, Apps und Social Media

IT-Security:

- **Informationssicherheit:**
Umfassender Schutz von Informationen, unabhängig ihrer Form (digital oder Papier),
Überbegriff der Datenschutz und Datensicherheit einschließt
- **Datensicherheit:**
beschäftigt sich mit den technischen und organisatorischen Maßnahmen (TOM) zur
Einhaltung der Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit aller Daten
- **Datenschutz:**
Der Schutz personenbezogener Daten natürlicher Personen vor dem Missbrauch
durch Dritte
 - **Rechtliche Grundlagen des Datenschutzes:**
 - DSGVO – EU-Datenschutz Grundverordnung
 - Bundesdatenschutzgesetz
 - **Betroffenenrechte nach DSGVO:**
 - Recht auf Auskunft
 - Recht auf Berichtigung
 - Recht auf Löschung
 - Recht auf Einschränkung der Verarbeitung
 - Recht auf Widerspruch
 - **Grundsätze der Verarbeitung personenbezogener Daten (Art. 5):**
 - **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
 - **Zweckbindung** – Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke
 - **Datenminimierung** – dem Zweck angemessen, auf das notwendige Maß beschränkt
 - **Richtigkeit** – unrichtige Daten müssen unverzüglich gelöscht oder berichtigt werden
 - **Speicherbegrenzung** – Speicherung zur Identifizierung einer Person nur solange wie nötig
 - **Integrität & Vertraulichkeit** – Sicherheit, Schutz vor Verlust oder Zerstörung oder Schädigung
- **IT-Schutzziele:**
 - **Vertraulichkeit (Confidentiality):**
Sicherstellung, dass nur berechtigte Personen Zugriff auf Daten haben,
Zugriffskontrolle und Verschlüsselung
 - **Integrität (Integrity):**
garantiert Richtigkeit, Vollständigkeit und Unversehrtheit von Daten und System, HASH-Wert
 - **Verfügbarkeit (Availability):**
gewährleistet, dass Systeme, Daten und Dienste zugänglich und nutzbar sind
 - **Authentizität (Authenticity):**
Bestätigt die Echtheit einer Quelle oder eines Kommunikationspartners
 - **Verbindlichkeit (Liability):**
stellt sicher, dass Handlungen oder Nachrichten im Nachhinein nicht abgestritten werden können

- **HASH-Verfahren:**
Errechnung eines Hashwerts fester Zeichenfolge aus Daten beliebiger Größe, der Hashwert dient als digitaler Fingerabdruck, kleinste Änderungen an den Daten verändern den errechneten Hashwert stark, somit kann die Integrität der Daten überprüft werden, die gängigsten Algorithmen sind **SHA-256** und **SHA-3**, MD5 gilt heute als unsicher
- **Zweifaktorauthentifizierung:**
Kombiniert Wissen (Passwort) und Besitz (SMS- oder Email-Code, Authenticator-App) und Inhärenz (biometrische Daten wie Fingerabdruck) wird das Passwort kompromittiert ist der Zugang vor Dritten weiterhin geschützt
- **Anonymisierung:**
Daten werden so verändert, dass kein Bezug mehr zu den personenbezogenen Daten einer Person möglich ist.
- **Pseudonymisierung:**
Identifikationsmerkmale werden durch Pseudonyme ersetzt, also verschleiert um die Feststellung der Identität auszuschließen, die personenbezogenen Daten sind aber wiederherstellbar
- **Malware:**
 - **Viren:** hängen sich an legitime Dateien oder Programme, verbreiten sich, wenn diese ausgeführt werden
 - **Würmer (Worms):** replizieren sich selbstständig über Netzwerke ohne Nutzerinteraktion
 - **Trojaner:** tarnen sich als nützliche Software, öffnen Hintertüren in Systeme oder laden weitere Schadsoftware nach
 - **Spyware:** überwachen heimlich Nutzeraktivitäten, stehlen persönliche Daten oder Passwörter
 - **Ransomware:** verschlüsseln Daten auf dem System, meist in Kombination mit Lösegeldforderung für die Entschlüsselung
 - **Adware:** Schadsoftware, die durch Werbung platziert wird
 - **Botnets:** Zusammenschluss infizierter Computer und IoTs, werden ferngesteuert um Angriffe (**DDos – Distributed Denial of Service**) durchzuführen
 - **Keylogger:** zeichnen Tastatureingaben auf um Zugangsdaten abzufangen

- **Schutzbedarfsanalyse:**
zentraler Prozess der Informationssicherheit um den Schutzbedarf von IT-Systemen, Anwendungen und Daten zu ermitteln. Sie bewertet Schadensszenarien um angemessene Sicherheitsmaßnahmen in Bezug auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu definieren
- **Schadenskategorien:**
 - **Niedrig:** Ausfall hat geringe, kaum spürbare Auswirkung
 - **Normal:** spürbare Auswirkung
 - **Hoch:** erhebliche Auswirkung
 - **Sehr hoch:** wenn ein Ausfall oder eine Beeinträchtigung sich existenziell bedrohlich auswirkt
- **Schutzbedarfskategorien:**
 - **Normal, hoch, sehr hoch**
 - Bewertung abhängig von:
 - Tolerierbaren Ausfallzeiten
 - Schnelligkeit der Regelung/Qualität der Notfallpläne
 - Negativen Kumulationseffekten von Schäden
 - Positiven Verteilungseffekten (Lastausgleich)
 - Existenziell bedrohlichen Maximalfällen
- **Kriterien bei der Auswahl von Sicherheitsmaßnahmen:**
 - **Wirksamkeit (Effektivität):** Sie müssen vor den möglichen Gefährdungen wirksam schützen, also den identifizierten Schutzbedarf abdecken
 - **Eignung:** Sie müssen in der Praxis tatsächlich umsetzbar sein, dürfen also z.B. nicht die Organisationsabläufe behindern oder andere Sicherheitsmaßnahmen aushebeln
 - **Praktikabilität:** Sie sollen leicht verständlich, einfach anzuwenden und wenig fehleranfällig sein
 - **Akzeptanz:** Sie müssen für alle Benutzer anwendbar (barrierefrei) sein und dürfen niemanden diskriminieren oder beeinträchtigen
 - **Wirtschaftlichkeit:** Mit den eingesetzten Mitteln sollte ein möglichst gutes Ergebnis erreicht werden. Die Maßnahmen sollten also einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu den zu schützenden Werten stehen
- **Härtung von Betriebssystemen:**
 - Deaktivierung nicht genutzter Dienste
 - Firewall-Konfiguration
 - Patch-Management-Systeme
 - Nutzung von **Secure Boot:**
Boot auf vorher signierte Bootloader beschränkt, der Start von Schadsoftware kann dadurch verhindert werden

- **Verschlüsselung:**
 - **Symmetrische Verschlüsselung:**
Ein Schlüssel wird zum Ver- und Entschlüsseln verwendet, sehr schnell und effizient, Hauptproblem: sicherer Austausch des Schlüssels
 - **Asymmetrische Verschlüsselung:**
zwei Schlüssel, privater und öffentlicher Schlüssel, der private darf niemals öffentlich werden, der öffentliche soll weitergegeben werden, andere Parteien können mit dem öffentlichen Schlüssel verschlüsseln, der Empfänger entschlüsselt dann mit seinem privaten Schlüssel, dadurch kann die Vertraulichkeit gewährleistet werden, da nur der Empfänger mit dem zu dem öffentlichen Schlüssel gehörenden privaten Schlüssel die Nachricht entschlüsseln kann, die Nachricht kann jedoch von jedem verschlüsselt worden sein, da der öffentliche Schlüssel für jeden zugänglich ist, die Authentizität ist nicht gewährleistet
- **Datensicherung:**
 - **Vollsicherung:**
gesamter Datensatz wird gesichert
 - **Vorteil:** einfachste Wiederherstellung da nur ein Backup nötig ist
 - **Nachteil:** benötigt am meisten Speicherplatz und Zeit zur Erstellung
 - **Inkrementelle Sicherung:**
sichert nur Daten, die seit der letzten Sicherung geändert wurden
 - **Vorteil:** geringster Speicherplatzbedarf, schnellste Art der Sicherung
 - **Nachteil:** Wiederherstellung komplex da die Vollsicherung und **alle** folgenden inkrementellen Backups benötigt werden
 - **Differenzielle Sicherung:**
sichert alle Daten, die seit der **letzten Vollsicherung** geändert wurden
 - **Vorteil:** schneller als Vollsicherung, Wiederherstellung einfacher als bei der inkrementellen Sicherung
 - **Nachteil:** Speicherplatzbedarf wächst mit der Zeit bis die nächste Vollsicherung erstellt wird

- **Firewalls:**
 - **Stateless Packet Inspection Firewall:**
kontrolliert die Header von Datenpaketen (IP-Adresse, Port, Protokolle), protokolliert abgelehnte Pakete
 - **Stateful Packet Inspection Firewall:**
kontrolliert die Header und den Verbindungszustand (Request oder Reply/Answer), protokolliert Beziehungen/Zugriffe in State Tables
 - **DPI – Deep Packet Inspection Firewall:**
analysiert den gesamten Inhalt des Pakets, nicht nur die Header, auch die Daten selbst
 - **Application-Level Firewall:**
Schicht 7, prüft den Datenverkehr nicht nur auf Header und Daten sondern auch auf Protokolle der Anwendungsschicht (HTTP/HTTPS, SMTP, FTP), blockiert böartige Anfragen wie SQL-Injections
 - **NGFW – Next Generation Firewall:**
kombiniert DPI und Application-Level Funktionen, verwendet Erkennungsmuster und prüft Anwendungen und Nutzer, ermöglicht Cloud-Sandboxing (Analyse unbekannter Dateien in isolierter Umgebung)
- **Passwörter:**
 - **Länge:** je länger ein Passwort desto mehr Kombinationen gibt es, dies macht es schwerer das Passwort zu erraten
 - **Komplexität:** Verwendung von Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen, keine Worte aus dem Wörterbuch verwenden, je komplexer ein Passwort desto schwerer ist es durch reines Ausprobieren (Brute Force) das Passwort zu erraten, macht Wörterbuchattacken (Dictionary Attacks) schwerer
 - **Regelmäßige Änderung: ACHTUNG!** Wird laut **BSI NICHT MEHR** empfohlen da eine regelmäßige Änderungspflicht dazu führt, dass Personen eher einfache, schwache Passwörter verwenden
- **Privacy by Design:**
Software und Hardware sollte so konzipiert und entwickelt werden, dass sie relevante Datenschutzmaßnahmen von Beginn an berücksichtigt, technische Integration des Datenschutzes nach DSGVO
- **Privacy by Default:**
Software und Hardware sollte bei Auslieferung datenschutzfreundlich vorkonfiguriert sein um die Privatsphäre der Nutzer zu respektieren

Projektplanung:

- Merkmale:

- Einmaligkeit
- Zeitlich begrenzt
- Klare Problemstellung
- Komplexes Problem dessen Lösungsweg zu Beginn unbekannt ist

- SMART-Kriterien:

- S – Spezifisch (specific)
- M – Messbar (measurable)
- A – Erreichbar (attainable, attractive, achievable)
- R – Angemessen (reasonable)
- T – Terminiert (time-bound)

- **Lastenheft:**

Die vom Auftraggeber festgelegte Gesamtheit der Forderungen an die Lieferungen und Leistungen eines Auftragnehmers innerhalb eines Auftrags

Es beschreibt das **Was?** und **Wofür?**

- **Pflichtenheft:**

Die vom Auftragnehmer erarbeiteten Realisierungsvorgaben aufgrund der Umsetzung des vom Auftraggeber vorgegebenen Lastenhefts

Es beschreibt das **Wie?** und **Womit?**

- **Beispiele für Inhalte:**

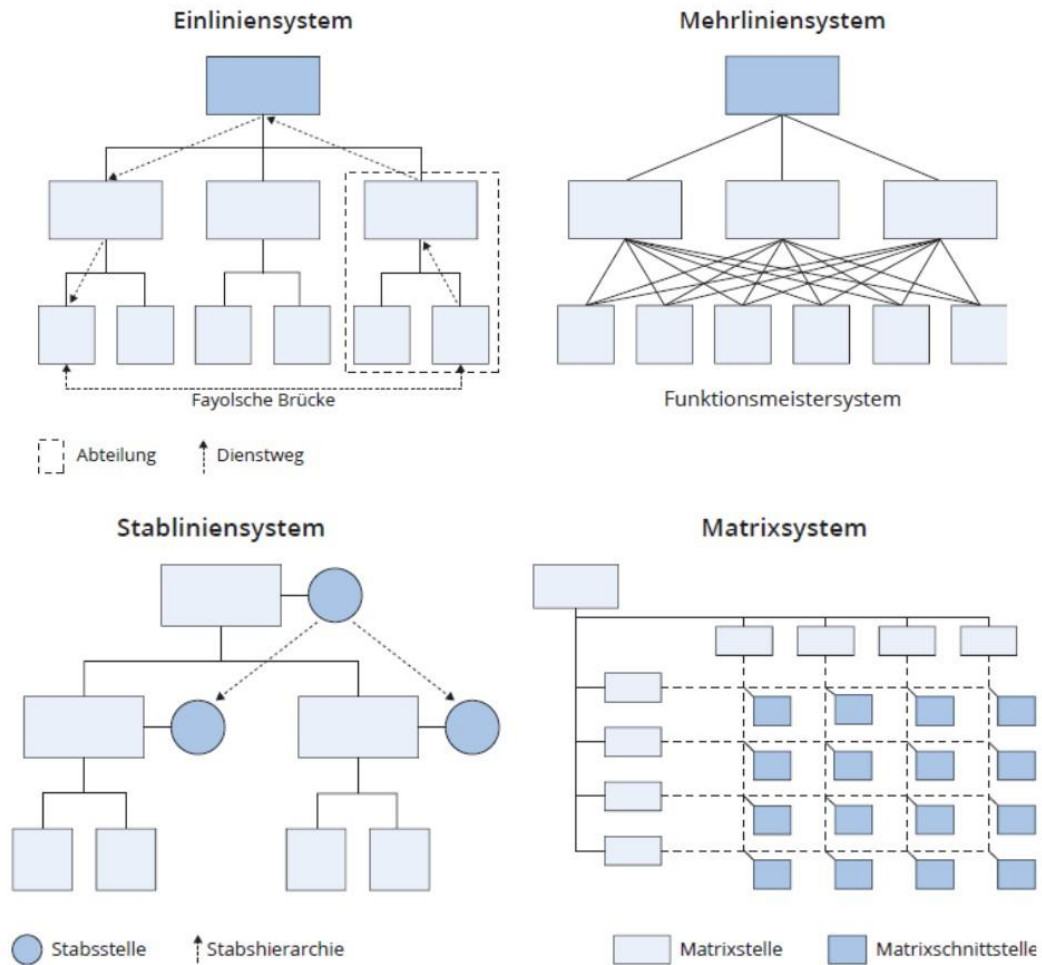
Lastenheft	Pflichtenheft
Ausgangssituation und Zielsetzung: - Beschreibung Ist-Zustand - Beschreibung Soll-Konzept	Ausgangssituation und Zielsetzung: - Beschreibung Ist-Zustand - Beschreibung Soll-Konzept
Funktionale Anforderungen: - Muss-Kriterien - Kann-Kriterien - Abgrenzungskriterien	Funktionale Anforderungen: - Softwarearchitektur - Leistungen der Komponenten - Datenmodell -Anwendungsfalldiagramm
Nichtfunktionale Anforderungen: - Einsatzumgebung Hardware - Einsatzumgebung Software - Verarbeitungsgeschwindigkeit	Nichtfunktionale Anforderungen: - Einsatzumgebung Hardware - Einsatzumgebung Software - Benutzerführung - Verarbeitungsgeschwindigkeit
Lebenszyklus des Gesamtsystems: - Zeitpunkt des Einsatzes - Abzulösende Systeme - Zukünftige Anforderungen	Schnittstellenübersicht
Lieferumfang: - Dokumentation - Softwarebereitstellung - Installation und Datentransfer - Supportleistungen - Schulungsleistungen	Lieferumfang: - Dokumentation - Softwarebereitstellung - Installation und Datentransfer - Supportleistungen - Schulungsleistungen
Abnahmekriterien: - Qualitätsziele - Testszenarien	Abnahmekriterien: - Qualitätsziele - Testszenarien

- **Stakeholder:**

Personen, Gruppen oder Organisationen die von den Aktivitäten eines Projekts direkt oder indirekt beeinflusst werden oder diese beeinflussen, sie haben ein berechtigtes Interesse am Erfolg oder Misserfolg des Projekts

Beispiel: Kunden, Lieferanten, Mitarbeiter, Geschäftsführung, Management

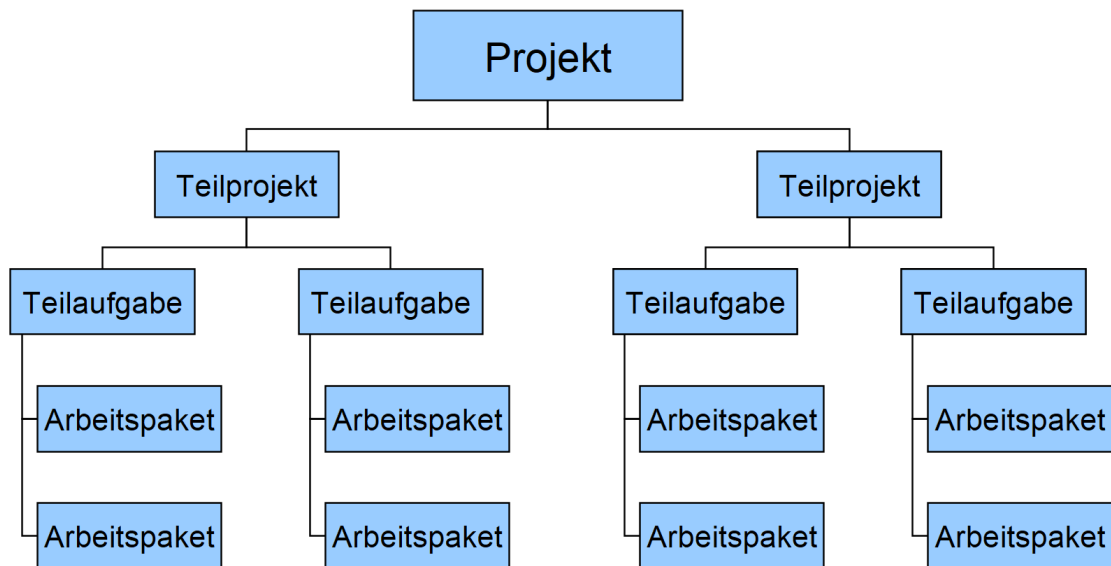
- **Aufbauorganisation:**
hierarchische Gliederung einer Organisation in funktionsfähige Stellen und Abteilungen. Festlegung eines Systems von Informations- und Anweisungswegen



- **Ablauforganisation:**
Regelt die funktionalen, zeitlichen und räumlichen Arbeitsabläufe zum optimalen Einsatz vorhandener Kapazitäten, Mitarbeiter und Betriebsmittel

- **Projektstrukturplan:**

hierarchische Darstellung von Projekten durch überschaubare Aufteilung in Teilprojekte, Teilaufgaben und Arbeitspakete, dient der Zuordnung von Aufgaben und Transparenz für alle Stakeholder



- **Netzplan:**

Darstellung von Vorgängen eines Projekts mit Knoten und Pfeilen für Zusammenhänge, ideal für komplexe Projekte mit vielen Abhängigkeiten, zeigen logische Abfolge

- **Dauer:** Zeitspanne der einzelnen Vorgänge
- **FAZ – Frühester Anfangszeitpunkt:** spätester FEZ der Vorgänger
- **FEZ – Frühester Endzeitpunkt:** FAZ + Dauer
- **SAZ – Spätester Anfangszeitpunkt:** SEZ - Dauer
- **SEZ – Spätester Endzeitpunkt:** Frühester SAZ des Nachfolgers
- **FP – Freier Puffer:** FAZ des Nachfolgers – FEZ des aktuellen Vorgangs
- **GP – Gesamtpuffer:** SAZ - FAZ

- **Gantt-Diagramm:**

Darstellung durch horizontale Balken auf einem Zeitstrahl, zeigt zeitliche Dauer und Überlappungen von Vorgängen, dient der Erstellung anschaulicher Terminpläne und zeigt Start- und Endtermine sowohl Fortschritt der Vorgänge

- **Wirtschaftlichkeit:**

hier wird geprüft, ob der Nutzen des Projekts größer ist als die Kosten (Kosten-Nutzen-Vergleich)

- **Risiken:**
 - **Finanzielle Risiken:** Budgetüberschreitung
 - **Zeitliche Risiken:** Verzögerung durch unklare Anforderungen
 - **Technologische Risiken:** Einsatz neuer oder unreifer Technologien
 - **Sicherheitsrisiken:** Datenverluste, Cyberangriffe, unzureichender IT-Grundschutz
 - **Organisatorische Risiken:** mangelnde Akzeptanz bei Nutzern, unklare Verantwortlichkeiten, Widerstand durch Stakeholder
 - **Externe Risiken:** gesetzliche Änderungen, Marktschwankungen, Lieferprobleme
- **Projektphasen:**
 - Anforderungsanalyse
 - Entwurf
 - Implementierung
 - Test
 - Dokumentation
 - Integration und Betrieb
 - Wartung und Support
- **Vorgehensmodelle:**
 - **Wasserfallmodell:**

lineares Modell, Phasen werden nacheinander abgearbeitet, jede Phase besteht aus Startpunkt, Meilensteinen und Endpunkt, Dokumentation wird über den Projektzeitraum parallel zu den Phasen erstellt, es ist nur sehr eingeschränkt möglich auf sich ändernde Anforderungen zu reagieren
 - **SCRUM:**

agile Vorgehensweise, man geht davon aus, dass ein Projekt nicht von Anfang bis Ende durchgeplant werden kann, Entwicklung erfolgt iterativ (wiederholend) in Sprints mit regelmäßigen Feedback-Schleifen, besteht aus:

 - Product Owner
 - SCRUM Master
 - Entwicklungsteam

Hardware:

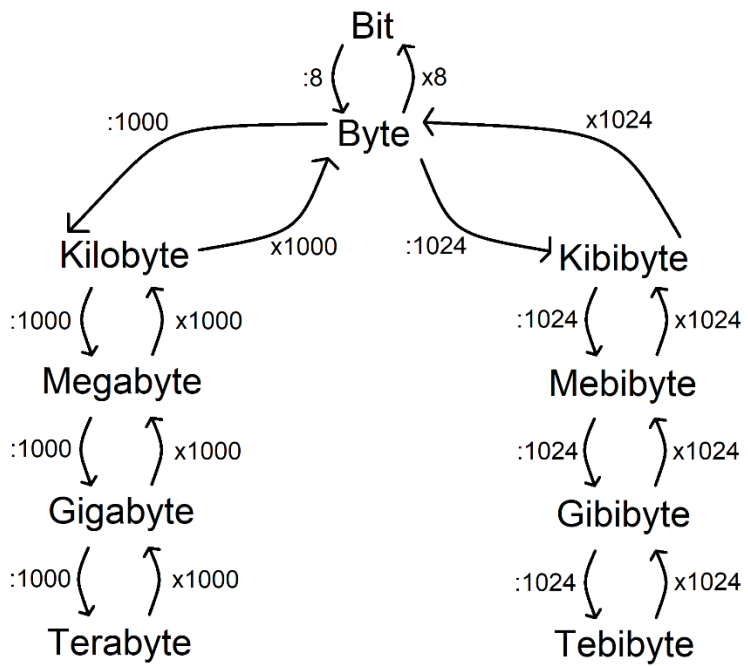
- **Bewertungskriterien bei der Auswahl von Hardware:**
 - **Leistungsparameter:**
 - Prozessorleistung (CPU)
 - Arbeitsspeicher (RAM)
 - Speichergröße und Geschwindigkeit (SSD)
 - **Arbeitsplatzergonomie:**
Benutzerfreundliche, gesundheitsfördernde, augenschonende Gestaltung von Hard- und Software um Beschwerden entgegenzuwirken
 - **Barrierefreiheit:**
 - Skalierbare Schriftgrößen
 - Vorlesefunktionen
 - Tastaturnavigation
 - **Energieverbrauch/Energieeffizienz**
 - **Nutzungsdauer**
 - **Recyclingfähigkeit**
- **CPU – Central Processing Unit:**
zentraler Mikrochip eines PCs, verarbeitet Befehle, berechnet Daten, steuert Informationsfluss zwischen allen Komponenten,
besteht aus:
 - **CU – Control Unit:** Steuerwerk
 - **ALU – Arithmetic Logic Unit:** Rechenwerk
 - **Cache-Speicher (L1, L2, L3):** Puffer, die häufig benötigte Daten aus dem RAM speichern um die Anfragen der CPU an den RAM zu verringern
- **GPU – Graphics Processing Unit:**
spezialisierte Prozessor der auf die Darstellung von Grafiken, Bild und Videos auf Monitoren ausgelegt ist, spezialisiert auf massive, gleichzeitige Berechnungen
- **RAM – Random Access Memory:**
extrem schnelle Kurzzeitspeicher der Daten aktuell genutzter Programme für die CPU bereithält. Am häufigsten verwendet ist DDR-SRAM (**Double Data Rate Synchronous Dynamic RAM**), Dual-Channel Mode, Multi-Channel Mode Voraussetzung und Vorteil
- **HDD – Hard Disk Drive:**
rotierende Magnetscheiben mit Schreib-Lese-Kopf der die Scheiben berührungslos magnetisiert, günstiger (pro Gigabyte) als SSDs
- **SSD – Solid State Drive:**
verwenden Flash-Speicher, sind robuster, leiser und bieten höhere Zugriffsgeschwindigkeiten und geringeren Stromverbrauch als HDDs
- **Thin-Client:**
schmale Arbeitsplatzrechner die hauptsächlich auf Serverressourcen zugreifen und daher kaum eigene Rechenleistung benötigen
- **NAS – Network Attached Storage:**
Zentraler Netzwerkspeicher, der Daten für berechnete Nutzer verfügbar macht, fungiert als unabhängiger Server, oft mit mehreren Festplatten zur Datensicherheit, häufig eingesetzt für Backups, zentrales Filesharing oder Medien-Streaming

- **SAN – Storage Area Network:**
spezialisiertes, hochleistungsfähiges Netzwerk, das Server mit gemeinsam genutzten Speichergeräten verbindet, alle Speichermedien werden zu einer virtuellen Speichereinheit zusammengefasst und zentral verwaltet, der Zugriff erfolgt über entsprechend konfigurierte Server, das SAN wird parallel zu einem LAN betrieben
- **Filesysteme:**
 - **FAT32 – File Allocation Table:** maximale Dateigröße 4GB, 8TB Partitionsgröße betriebssystemübergreifend
 - **NTFS – New Technology File System:** Windows Standard
 - **APFS – Apple File System:** macOS Standard
 - **ext4 – Fourth Extended Filesystem:** Linux Standard
- **BIOS – Basic Input/Output System:**
Firmware auf dem Mainboard, lädt das Betriebssystem und initialisiert Hardwarekomponenten wie CPU, GPU, RAM, Festplatten (**POST – Power-On Self-Test**)
- **UEFI: Unified Extensible Firmware Interface:**
moderner Nachfolger von BIOS, grafische Oberfläche, Schnittstelle zwischen Hardware und Betriebssystem, unterstützt größere Festplatten, ermöglicht schnellere Bootzeiten und bietet Sicherheitsfunktionen wie **Secure Boot**
- **IoT – Internet of Things:**
Vernetzung physischer Gegenstände wie Lampen, Kühlschränke, Rollläden, Smart Home Systeme
- **IIoT – Industrial Internet of Things:**
Vernetzung physischer Maschinen, Sensoren, Anlagen über das Internet zur Optimierung von Produktionsprozessen durch Echtzeit-Datenanalyse, Smart Factory
- **Sensor, Aktor:**
 - Sensoren erfassen physikalische Größen und wandeln diese in elektrische Signale
 - Aktoren wandeln diese Signale zurück in physische Aktionen
- **Mikrocontroller vs Mikroprozessor:**
 - Mikrocontroller sind vollständige Computer auf einem Chip
 - Ein Mikroprozessor ist lediglich der Rechenkern (CPU) und benötigt externe Komponenten
- **USV – Unterbrechungsfreie Stromversorgung:**
 - **VFI – Voltage and Frequency Independent:**
auch Online USV genannt
 - **VI – Voltage Independent:**
auch Line-Interactive USV genannt
 - **VFD – Voltage and Frequency Dependent:**
auch Offline USV genannt

Weitere nützliche Begriffe:

- **First-Level-Support:**
Erste Anlaufstelle für Nutzer, hier werden Tickets aufgenommen und häufig auftretende, einfache Standardprobleme gelöst
- **Second-Level-Support:**
Übernimmt, wenn Fachwissen oder spezielles Systemwissen für komplexere Probleme benötigt wird
- **Third-Level-Support:**
Schwerwiegende Probleme werden durch Spezialisten/Entwickler gelöst, möglicherweise durch externe Mitarbeiter oder in Zusammenarbeit mit dem Hersteller
- **Client-Server-Systeme:**
Clients fragen Dienste bei zentralen Servern an, bspw. Datei-, Druck- oder Authentifizierungsdienste
- **Künstliche Intelligenz:**
 - **Offline KI:**
KI läuft lokal auf eigener Hardware, maximaler Datenschutz, begrenzt durch die Leistung des eigenen Rechners, KI lernt nur durch die lokalen Benutzer, Aktualität des Wissens bleibt auf dem Stand der Installation außer es wird lokal aktualisiert
 - **Online KI:**
cloud-basiert, KI lernt durch alle Benutzer und ist immer auf dem neuesten Stand, sehr leistungsfähig da auf Serverfarmen gehostet, Datenschutz kritisch da die Daten das eigene System verlassen
- **Industrielle Revolutionen:**
 - **Industrie 1.0:**
Mechanisierung durch Wasser- und Dampfkraft
 - **Industrie 2.0:**
Massenanfertigung durch elektrische Energie (Fließbänder)
 - **Industrie 3.0:**
Digitale Revolution durch Elektronik und IT zur Automatisierung von Produktion
 - **Industrie 4.0:**
Weiterentwicklung durch umfassende Digitalisierung und Vernetzung, IoT, KI, Cyber-Physische Systeme, Smart Home, - Factory, -Health, -City
- **Smart Factory, Smart Home, Smart Health, Smart City**

- **Speichergrößen-Einheitenumrechnung:**



Tipps für die Prüfung:

- **Nenne:**
klar unterscheidbare Nennung, stichwortartig
- **Beschreibe:**
in ganzen, zusammenhängenden Sätzen alle Bestandteile darstellen, OHNE Erläuterungen, Begründungen oder Anwendungen
- **Erläutere:**
in ganzen Sätzen alle Bestandteile darstellen, zusätzlich Unterschiede, Gemeinsamkeiten, Begründungen oder eigene Stellungnahme hinzufügen
- **Verneinungen oder doppelte Verneinungen beachten**
- **Punkteverteilung beachten und Zeit einteilen**
- **Deutlich und sauber Schreiben/Zeichnen**
- **Eigenen Block mitbringen**