

Ausarbeitung-Themenkatalog

1. Der Lehrbetrieb

1.1 Ergonomische Gestaltung eines Arbeitsplatzes

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Der Lehrbetrieb	1
1.1 Ergonomische Gestaltung eines Arbeitsplatzes	1
1.1.1 Ergonomische Gestaltung eines Arbeitsplatzes	2
1.1.2 Einrichtung eines Bildschirmarbeitsplatzes	2
1.1.3 Optimaler Aufstellungsort (Lichteinfall)	2
1.1.4 Gesetzliche Pausenregelungen	2
1.1.5 Maße und Abstände	2
1.1.6 Schutzmaßnahmen & Entspannungsübungen	3

1.1.1 Ergonomische Gestaltung eines Arbeitsplatzes

Unter Ergonomie versteht man die **Anpassung der Arbeitsbedingungen an den Menschen** (und nicht umgekehrt). Das Ziel ist es, die Belastung für den Körper so gering wie möglich zu halten, um Gesundheitsschäden (wie Sehnenscheidenentzündungen oder Bandscheibenvorfälle) vorzubeugen und die Leistungsfähigkeit zu erhalten.

1.1.2 Einrichtung eines Bildschirmarbeitsplatzes

Ein ergonomischer Bildschirmarbeitsplatz besteht aus einem Zusammenspiel von Möbeln und Geräten:

- **Bürostuhl:** Dynamisches Sitzen muss möglich sein (verstellbare Rückenlehne und Höhe). Die Füße stehen flach auf dem Boden, Ober- und Unterschenkel bilden einen Winkel von mindestens 90°.
- **Tastatur & Maus:** Sollten auf einer Ebene liegen. Die Handgelenke sollten nicht geknickt werden (ggf. Handballenauflage nutzen).

1.1.3 Optimaler Aufstellungsort (Lichteinfall)

Die Position des Monitors im Raum ist entscheidend für die Augen:

- **Parallel zum Fenster:** Der Bildschirm sollte idealerweise im rechten Winkel zum Fenster stehen.
- **Vermeidung von Blendung:** Lichtquellen (Fenster oder Lampen) dürfen sich nicht im Monitor spiegeln und dem Benutzer auch nicht direkt ins Gesicht scheinen (Kontrastverlust).

1.1.4 Gesetzliche Pausenregelungen

In der Regel gelten für Bildschirmarbeit (je nach nationalem Recht, z. B. ArbSchG oder Bildschirmarbeitsverordnung) folgende Richtlinien:

- **Tätigkeitswechsel:** Nach 50 Minuten Bildschirmarbeit sollte eine 10-minütige Pause oder eine andere Tätigkeit (ohne Bildschirm) erfolgen.
- **Pausen sind Arbeitszeit:** Diese kurzen Unterbrechungen dienen der Regeneration der Augen und der Muskulatur.

1.1.5 Maße und Abstände

Für die ideale Haltung gelten folgende Richtwerte:

- **Bildschirmoberkante:** Sie sollte auf Augenhöhe oder leicht darunter liegen (leicht gesenkter Blick entspannt die Nackenmuskulatur).
- **Sehabstand:** Je nach Monitorgröße zwischen **50 cm und 70 cm**.
- **Tischhöhe:** Die Unterarme sollten locker auf dem Tisch aufliegen, wobei Ober- und Unterarm einen Winkel von **90° bis 100°** bilden.

1.1.6 Schutzmaßnahmen & Entspannungsübungen

Um körperliche Schäden bei sitzender Tätigkeit zu vermeiden, helfen präventive Maßnahmen und gezielte Bewegung:

Schutzmaßnahmen

- **Dynamisches Sitzen:** Häufiges Wechseln der Sitzposition.
- **Steh-Sitz-Dynamik:** Einsatz von höhenverstellbaren Schreibtischen.
- **Indirekte Beleuchtung:** Vermeidung von hartem Licht direkt auf den Arbeitsbereich.

Entspannungsübungen

- **Augen-Training:** Die "20-20-20-Regel" (alle 20 Minuten für 20 Sekunden auf einen Punkt in 20 Fuß/6 Meter Entfernung schauen).
- **Schulterkreisen:** Lockert Verspannungen im Nackenbereich.
- **Dehnen:** Regelmäßiges Strecken der Wirbelsäule und Dehnen der Handgelenke.

Ausarbeitung-Themenkatalog

1. Der Lehrbetrieb

1.1 Arbeitssicherheit und Schutzmaßnahmen

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Der Lehrbetrieb	1
1.1 Arbeitssicherheit und Schutzmaßnahmen	1
Arbeitssicherheit und Schutzmaßnahmen	2
1.1.1 Wirkungsweise und Gefahren des elektrischen Stroms.....	2
1.1.2 Verhalten bei einem Elektrounfall (Reihenfolge)	2
1.1.3 Brandfall: Gefahren und Verhalten (Reihenfolge)	2
1.1.4 CO ₂ - und Pulver-Feuerlöscher	3
1.1.5 Verwendung bei elektrischen Anlagen.....	3
1.1.6 Umgang und Lagerung von Akkus (insb. Lithium-Ionen)	3
1.1.7 Umweltgerechte Entsorgung.....	3
1.1.8 Arbeitsrechtliche Gesetze.....	4

Arbeitssicherheit und Schutzmaßnahmen

Unter Arbeitssicherheit versteht man alle Maßnahmen zur Vermeidung von Arbeitsunfällen und Berufskrankheiten.

- **Schutzmaßnahmen:** Man unterscheidet zwischen technischen (z. B. Schutzabdeckungen), organisatorischen (z. B. Unterweisungen) und persönlichen Schutzmaßnahmen (**PSA** – z. B. Sicherheitsschuhe, Helm).
- **Grundsatz:** Gefahren sind primär an der Quelle zu bekämpfen (S-T-O-P Prinzip: Substitution, Technische, Organisatorische, Personenbezogene Maßnahmen).

1.1.1 Wirkungsweise und Gefahren des elektrischen Stroms

Der menschliche Körper leitet Strom. Die Wirkung hängt von Stromstärke (\$I\$), Einwirkdauer (\$t\$) und dem Weg durch den Körper ab.

- **Thermische Wirkung:** Verbrennungen an Ein- und Austrittsstellen.
- **Chemische Wirkung:** Elektrolyse des Blutes (Vergiftungsgefahr).
- **Muskelreizwirkung:** Verkrampfung (Loslassschwelle), Atemstillstand und **Herzkammerflimmern**.

1.1.2 Verhalten bei einem Elektrounfall (Reihenfolge)

Hier zählt jede Sekunde, aber **Eigenschutz geht vor!**

1. **Stromkreis unterbrechen:** Stecker ziehen, Sicherung ausschalten oder Verunglückten mit isolierendem Gegenstand von der Quelle trennen.
2. **Notruf absetzen:** 144 (Rettung) oder 112 (Euro-Notruf).
3. **Erste Hilfe:** * Bei Bewusstsein: Schocklagerung, betreuen.
 - Bewusstlos/Atmung vorhanden: Stabile Seitenlage.
 - Keine Atmung: Wiederbelebung (Herzdruckmassage/Defibrillator).
4. **Ärztliche Kontrolle:** Auch wenn der Patient sich gut fühlt (Gefahr des verzögerten Herztods).

1.1.3 Brandfall: Gefahren und Verhalten (Reihenfolge)

Gefahren: Rauchgasvergiftung (meist tödlicher als Flammen), Sauerstoffmangel, Hitze, Einsturzgefahr.

Reihenfolge:

1. **Alarmieren:** Feuerwehr (122) rufen, Hausalarm auslösen.

2. **Retten:** Menschen aus der Gefahrenzone bringen, Fenster/Türen schließen (Sauerstoffentzug).
3. **Löschen:** Kleinbrände mit vorhandenen Mitteln bekämpfen (nur ohne Eigengefährdung).

1.1.4 CO₂- und Pulver-Feuerlöscher

Typ	Einsatzgebiet	Vorteil / Nachteil
CO₂ (Kohlendioxid)	Brände der Klasse B, Elektronik, EDV-Räume.	Rückstandsfrei, erstickt das Feuer; Vorsicht in engen Räumen (Erstickungsgefahr).
Pulver (ABC)	Universell einsetzbar (Feststoffe, Flüssigkeiten, Gase).	Hohe Löschkraft; Nachteil: Massive Verschmutzung, Pulver ist korrosiv für Elektronik.

1.1.5 Verwendung bei elektrischen Anlagen

- **Sicherheitsabstand einhalten:** Bei Niederspannung (bis 1000V) meist **1 Meter** Mindestabstand.
- **Bevorzugtes Löschmittel:** CO₂-Löscher, da sie nicht leiten und keine Rückstände hinterlassen, die Kurzschlüsse verursachen könnten.

1.1.6 Umgang und Lagerung von Akkus (insb. Lithium-Ionen)

- **Lagerung:** Kühl, trocken und bei ca. 40–60 % Ladestand. Nicht in der prallen Sonne oder bei Frost lagern.
- **Umgang:** Nur Original-Ladegeräte verwenden. Mechanische Beschädigungen (Sturz, Verformung) unbedingt vermeiden – Brandgefahr durch „Thermal Runaway“.

1.1.7 Umweltgerechte Entsorgung

Elektronikschrott und Akkus enthalten Schadstoffe (Blei, Cadmium, Quecksilber), aber auch wertvolle Rohstoffe.

- **Gesetz:** Verpflichtung zur getrennten Sammlung (WEEE-Richtlinie).
- **Entsorgung:** Rückgabe im Handel oder bei kommunalen Sammelstellen (Mistplatz). Akku-Pole bei Lithium-Batterien abkleben (Kurzschlussbrandgefahr).

1.1.8 Arbeitsrechtliche Gesetze

- **KJBG (Kinder- und Jugendlichenbeschäftigungsgesetz):** Regelt Arbeitszeiten, Ruhepausen und Nachtarbeitsverbote für Personen unter 18 Jahren.
- **ASchG (ArbeitnehmerInnenschutzgesetz):** Verpflichtet Arbeitgeber zur Gefahrenminderung und Arbeitnehmer zur Einhaltung von Sicherheitsvorschriften.
- **GIBG (Gleichbehandlungsgesetz):** Verbietet Diskriminierung am Arbeitsplatz aufgrund von Geschlecht, Alter, Religion, Herkunft oder sexueller Orientierung.

Ausarbeitung-Themenkatalog

2. Kaufmännische Grundlagen

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

2. Kaufmännische Grundlagen.....	1
2.1 Durchführung einer Preiskalkulation	2
2.2 Inhalte von Geschäftspapieren	2
2.3 Bezahlungsmöglichkeiten	2
Recht & Verkauf.....	3
2.4 Verkaufsbezogene rechtliche Bestimmungen	3
Beratung & Kommunikation	3
2.5 Fachspezifische Verkaufsgespräche & Produktberatung.....	3
2.6 Technische Zusammenhänge beratend erklären.....	3
2.7 Erstellen kundenorientierter Softwarelösungen	3
Reklamations- & Krisenmanagement	4
2.8 Umgang bei Reklamationen	4
2.9 Kundenumgang bei folgenreichen technischen Problemen.....	4

2.1 Durchführung einer Preiskalkulation

Die Preiskalkulation dient der Ermittlung des Verkaufspreises einer Ware oder Dienstleistung. Sie stellt sicher, dass alle Kosten gedeckt sind und ein Gewinn erzielt wird.

- **Schema:** Einstandspreis (Einkauf) + Regiekosten (Miete, Strom, Personal) + Gewinnmarge = Nettoverkaufspreis (+ USt = Bruttoverkaufspreis).
- **Wichtig:** In der IT/Technik müssen auch Lizenzen und Arbeitszeit (Stundensatz) einkalkuliert werden.

2.2 Inhalte von Geschäftspapieren

Diese Dokumente bilden den rechtlichen Ablauf eines Verkaufs ab:

- **Anbot:** Rechtlich bindende Erklärung, Waren oder Dienste zu bestimmten Konditionen zu liefern.
- **Auftragsbestätigung:** Annahme des Kundenangebots; damit kommt der Kaufvertrag zustande.
- **Lieferschein:** Dokumentiert den Warenfluss (was wurde wann geliefert?). Wichtig für die Warenübernahme.
- **Rechnung:** Die Zahlungsaufforderung. Muss gesetzliche Merkmale (UID-Nummer, Rechnungsdatum, Steuerbetrag etc.) enthalten.

2.3 Bezahlungsmöglichkeiten

Unterscheidung in:

- **Barzahlung:** Unmittelbarer Austausch von Geld gegen Ware.
 - **Bargeldlose Zahlung:** Überweisung (Rechnung), Kreditkarte, Debitkarte (Bankomat) oder Online-Dienste (PayPal).
 - **Finanzierung:** Ratenkauf oder Leasing (oft bei teurer Hardware/Software-Projekten).
-

Recht & Verkauf

2.4 Verkaufsbezogene rechtliche Bestimmungen

Hier geht es vor allem um den Schutz beider Vertragspartner:

- **Gewährleistung:** Gesetzliche Pflicht des Verkäufers, für Mängel zu haften, die zum Zeitpunkt der Übergabe bestanden (2 Jahre bei beweglichen Sachen).
- **Garantie:** Eine freiwillige Zusage (meist des Herstellers), die über die gesetzliche Gewährleistung hinausgeht.
- **KSchG (Konsumentenschutzgesetz):** Besondere Regeln für Geschäfte zwischen Unternehmen (B2B) und Privatpersonen (B2C), z. B. Rücktrittsrechte bei Fernabsatzgeschäften.

Beratung & Kommunikation

2.5 Fachspezifische Verkaufsgespräche & Produktberatung

Ein strukturiertes Gespräch, das nicht nur "verkauft", sondern Lösungen bietet.

- **Phasen:** Begrüßung → Bedarfsermittlung (Was braucht der Kunde wirklich?) → Präsentation (Nutzen-Argumentation) → Einwandbehandlung → Abschluss.
- **Fokus:** Der Kunde kauft nicht die "Technik", sondern den Nutzen (z.B. Zeitersparnis, Sicherheit).

2.6 Technische Zusammenhänge beratend erklären

Die Fähigkeit, komplexe Sachverhalte in die Sprache des Kunden zu übersetzen ("Vom Fachchinesisch zum Anwendernutzen").

- **Beispiel:** Statt "Wir nutzen ein RAID 1 System" sagst du "Ihre Daten werden gespiegelt, damit bei einem Festplattenausfall nichts verloren geht".

2.7 Erstellen kundenorientierter Softwarelösungen

Hier steht die **Analyse der Workflows** des Kunden im Vordergrund. Eine Lösung ist dann kundenorientiert, wenn sie ein spezifisches Problem löst, intuitiv bedienbar ist und sich in die bestehende Infrastruktur einfügt.

Reklamations- & Krisenmanagement

2.8 Umgang bei Reklamationen

Reklamationen sind keine persönliche Kritik, sondern eine Chance zur Kundenbindung.

- **Vorgehen:** Ausreden lassen → Verständnis zeigen (Empathie) → Den Sachverhalt prüfen → Lösung anbieten (Austausch, Reparatur, Gutschrift) → Nachfassen.

2.9 Kundenumgang bei folgenreichen technischen Problemen

Wenn Systeme stehen oder Datenverlust droht, ist **Deeskalationsmanagement** gefragt:

- **Transparenz:** Den Kunden ehrlich über den Stand der Dinge informieren. Keine leeren Versprechungen machen.
- **Professionalität:** Ruhe bewahren, Prioritäten setzen und den Kunden regelmäßig über Fortschritte bei der Fehlerbehebung informieren (Status-Updates).

Ausarbeitung-Themenkatalog

3. Fachliche Grundlagen

3.1 Technische Dokumentation

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

3. Fachliche Grundlagen	1
3.1 Technische Dokumentation	1
3.1.1 Aufgabe und Strukturierung von Testläufen	2
3.1.2 Protokollieren technischer Arbeiten	4
3.1.3 Anwenden von Fachausdrücken (Deutsch/Englisch)	4
3.1.4 Inhalt technischer Dokumentationen & Protokolle	4
3.1.5 Aufbereitung technischer Dokumente	4
3.1.6 Handhabung von Textverarbeitung & Screenshots	5
3.1.7 Anwendung der Schrittaufzeichnung (Step Recorder).....	5
3.1.8 Beilagen technischer Dokumentationen	5
3.1.9 Gestaltung und Vorbereitung von Präsentationen	5

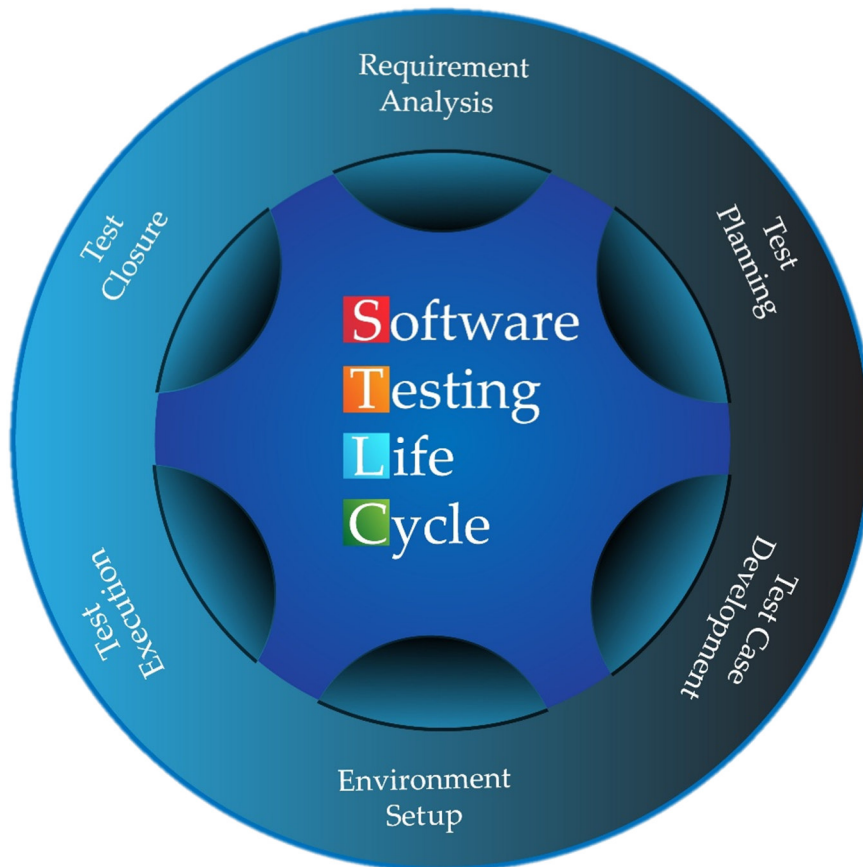
Die technische Dokumentation umfasst alle Informationen, die ein technisches Produkt (Hardware oder Software) beschreiben. Sie dient dazu, den gesamten Lebenszyklus – von der Planung über die Installation bis zur Wartung – nachvollziehbar zu machen.

- **Ziel:** Informationstransfer an Benutzer, Techniker oder Auftraggeber sowie rechtliche Absicherung.

3.1.1 Aufgabe und Strukturierung von Testläufen

Testläufe dienen der Qualitätssicherung. Sie prüfen, ob das System die im Pflichtenheft definierten Anforderungen erfüllt.

- **Struktur:**
 1. **Testziel:** Was wird geprüft? (z. B. Konnektivität).
 2. **Testumgebung:** Hardware/Software-Setup.
 3. **Testschritte:** Detaillierte Anleitung.
 4. **Erwartetes Ergebnis:** Was sollte passieren?
 5. **Tatsächliches Ergebnis:** Was ist passiert (Ist-Zustand)?



3.1.2 Protokollieren technischer Arbeiten

Hierbei handelt es sich um die zeitliche und sachliche Erfassung von Tätigkeiten (z. B. Installationen, Fehlerbehebungen).

- **Wichtig:** Es muss für Dritte (Kollegen oder Nachfolger) so geschrieben sein, dass die Arbeit ohne Rückfragen reproduziert werden kann.

3.1.3 Anwenden von Fachausdrücken (Deutsch/Englisch)

In der IT ist die korrekte Verwendung von Termini entscheidend für die professionelle Kommunikation.

- **Beispiele:**
 - *Schnittstelle* → Interface
 - *Bereitstellung* → Deployment
 - *Fehlerbehebung* → Troubleshooting
 - *Sicherung* → Backup

3.1.4 Inhalt technischer Dokumentationen & Protokolle

Eine professionelle Dokumentation sollte folgende Elemente enthalten:

- **Deckblatt:** Titel, Ersteller, Datum, Version.
- **Inhaltsverzeichnis:** Strukturierte Übersicht.
- **Einleitung:** Zweck und Zielgruppe.
- **Hauptteil:** Konfiguration, Installationsschritte, Topologien.
- **Abschluss:** Abnahmeprotokoll, Fazit.

3.1.5 Aufbereitung technischer Dokumente

Die Aufbereitung bezieht sich auf das **Layout** und die **Lesbarkeit**.

- Verwendung von Formatvorlagen.
- Einheitliche Schriftarten und Farben (Corporate Design).
- Klare Hierarchien durch Nummerierungen (1., 1.1, 1.1.1).

3.1.6 Handhabung von Textverarbeitung & Screenshots

- **Textverarbeitung:** Effiziente Nutzung von automatischen Verzeichnissen (Inhalt, Abbildungen) und Fußzeilen (Seitenzahlen).
- **Screenshots:** Bilder sollten nur relevante Bildschirmausschnitte zeigen, scharf sein und ggf. durch Markierungen (Pfeile, Rahmen) ergänzt werden.

3.1.7 Anwendung der Schrittaufzeichnung (Step Recorder)

Der **Windows Step Recorder** (oder ähnliche Tools) zeichnet jeden Klick und jede Tastatureingabe inklusive Screenshots automatisch auf.

- **Vorteil:** Enorme Zeitersparnis bei der Erstellung von Klickanleitungen und eine präzise Fehlerdokumentation für den Support.

3.1.8 Beilagen technischer Dokumentationen

Beilagen ergänzen den Haupttext durch detaillierte Fachgrafiken oder Nachweise:

- **Netzwerkplan:** Visuelle Darstellung der Infrastruktur.
- **Testprotokoll:** Nachweis der Funktionsfähigkeit.
- **Quellcode-Auszüge** oder **Datenblätter** von Komponenten.

3.1.9 Gestaltung und Vorbereitung von Präsentationen

Die Präsentation ist die visuelle Unterstützung deines Fachgesprächs.

- **Regeln:** "Weniger ist mehr" (max. 5-7 Stichpunkte pro Folie).
- **Medienmix:** Einsatz von Folien, Live-Demos oder Whiteboard.
- **Struktur:** Einleitung (Agenda), Hauptteil (Kernprojekt), Schluss (Zusammenfassung & Fragerunde).

Ausarbeitung-Themenkatalog

3. Fachliche Grundlagen

3.3 Gesetzliche Bestimmungen/Datenschutz

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

3. Fachliche Grundlagen	1
3.3 Gesetzliche Bestimmungen/Datenschutz	1
Datenschutzgrundverordnung (DSGVO).....	2
Grundlagen & Fachbegriffe	2
3.3.1 Aktuelle DSGVO	2
3.3.2 Datenminimierung.....	2
3.3.3 Personenbezogene Daten	2
3.3.4 Sensible Daten	2
Rollen im Datenschutz.....	2
3.3.5 Betroffene Person.....	2
3.3.6 Verantwortlicher	2
3.3.7 Auftragsverarbeiter	2
Rechte der betroffenen Personen	2
Spezielle Konzepte & Rollen.....	3
Urheberrecht & IT-Recht	3
3.3.8 Urheberrecht	3
3.3.9 Gewährleistung vs. Garantie	3
3.3.10 E-Commerce (ECG) & Telekom (TKG).....	3
Impressumpflicht & Kommunikation	4
3.3.11 Pflichtangaben Homepage (Impressum).....	4
3.3.12 Pflichtangaben im E-Mail-Verkehr	4
3.3.13 Bildschirmpausen	4

Datenschutzgrundverordnung (DSGVO)

Grundlagen & Fachbegriffe

3.3.1 Aktuelle DSGVO

- Seit Mai 2018 EU-weit einheitliche Verordnung zum Schutz personenbezogener Daten. Ziel ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen.

3.3.2 Datenminimierung

- Ein Grundsatz der DSGVO. Es dürfen nur so viele Daten erhoben werden, wie für den spezifischen Zweck **unbedingt erforderlich** sind ("So wenig wie möglich, so viel wie nötig").

3.3.3 Personenbezogene Daten

- Alle Infos, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Name, IP-Adresse, Standortdaten).

3.3.4 Sensible Daten

- Besondere Kategorien (Art. 9 DSGVO), z. B. Religionszugehörigkeit, politische Meinung, Gesundheitsdaten oder biometrische Daten. Diese unterliegen einem deutlich höheren Schutzbedarfs.

Rollen im Datenschutz

3.3.5 Betroffene Person

- Die natürliche Person, deren Daten verarbeitet werden (z. B. der Kunde).

3.3.6 Verantwortlicher

- Die Stelle (Unternehmen/Verein), die über Zweck und Mittel der Datenverarbeitung entscheidet.

3.3.7 Auftragsverarbeiter

- Ein Dienstleister (z. B. Cloud-Anbieter), der Daten im Auftrag des Verantwortlichen weisungsgebunden verarbeitet.

Rechte der betroffenen Personen

Jede Person hat unter anderem folgende Rechte:

1. **Auskunftsrecht:** Wissen, welche Daten gespeichert sind.
2. **Recht auf Berichtigung:** Korrektur falscher Daten.
3. **Recht auf Löschung:** ("Recht auf Vergessenwerden").
4. **Recht auf Datenübertragbarkeit:** Mitnahme der Daten zu einem anderen Anbieter.
5. **Widerspruchsrecht:** Gegen die Verarbeitung (z. B. bei Direktwerbung).

Spezielle Konzepte & Rollen

- **Kopplungsverbot:** Die Erbringung einer Dienstleistung darf nicht davon abhängig gemacht werden, dass der Nutzer in eine Datenverarbeitung einwilligt, die für den Vertrag gar nicht notwendig ist (z. B. Newsletter-Zwang für einen App-Download).
- **Datenschutzbeauftragter (DSB):** Eine Person, die auf die Einhaltung der DSGVO im Betrieb achtet, Mitarbeiter schult und als Ansprechpartner für Behörden dient. Pflicht ab einer gewissen Unternehmensgröße oder bei risikoreichen Daten.
- **Datendiebstahl (Data Breach):** Bei einer Verletzung des Schutzes personenbezogener Daten muss das Unternehmen dies **innerhalb von 72 Stunden** der Aufsichtsbehörde melden (sofern ein Risiko für die Betroffenen besteht).

Urheberrecht & IT-Recht

3.3.8 Urheberrecht

- **Grundbegriff:** Schützt geistige Schöpfungen (Software, Bilder, Texte, Musik). Es entsteht automatisch mit der Erschaffung des Werkes (keine Registrierung nötig).
- **Gültigkeitsbereich:** Endet in der Regel **70 Jahre nach dem Tod** des Urhebers. Software wird wie literarische Werke geschützt.

3.3.9 Gewährleistung vs. Garantie

Merkmal	Gewährleistung	Garantie
Natur	Gesetzlich vorgeschrieben (24 Monate).	Freiwillige Zusage des Herstellers/Händlers.
Inhalt	Haftung für Mängel, die zum Zeitpunkt der Übergabe bestanden.	Versprechen über Funktionsfähigkeit für die Zukunft.
Anwendung	Hardware (Physischer Defekt) & Software (Bug, fehlende Funktion).	Oft nur auf Hardware-Komponenten beschränkt.

3.3.10 E-Commerce (ECG) & Telekom (TKG)

- **ECG:** Regelt den Online-Handel. Wichtig sind hier die Informationspflichten für Online-Shops und der rechtssichere Vertragsabschluss.
- **TKG:** Regelt den Bereich der Telekommunikation (z. B. Spam-Verbot, Rufnummernanzeige, Cookie-Einwilligung über den Fernmeldeaspekt).

Impressumspflicht & Kommunikation

3.3.11 Pflichtangaben Homepage (Impressum)

Ein Impressum muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Inhalte:

- Name/Firma des Betreibers.
- Geografische Anschrift (kein Postfach).
- Kontaktdaten (E-Mail, Telefon).
- UID-Nummer (falls vorhanden).
- Firmenbuchnummer und Gericht (bei GmbH/AG).

3.3.12 Pflichtangaben im E-Mail-Verkehr

E-Mails von Unternehmen gelten als Geschäftsbriefe. Sie müssen enthalten:

- Firmenname (laut Firmenbuch).
- Rechtsform (z. B. GmbH).
- Sitz des Unternehmens.
- Firmenbuchnummer und Firmenbuchgericht.

3.3.13 Bildschirmpausen

Nach dem Arbeitnehmerinnenschutzgesetz (AsVG) bzw. der Bildschirmarbeitsverordnung gilt:

- Nach **50 Minuten** ununterbrochener Bildschirmarbeit steht dem Arbeitnehmer eine **Pause von 10 Minuten** (oder ein Tätigkeitswechsel) zu.
- Diese Pausen sind bezahlte Arbeitszeit, dürfen aber nicht am Ende des Tages "gesammelt" werden, um früher zu gehen.

Ausarbeitung-Themenkatalog

3. Fachliche Grundlagen

3.3 Informatik und Gesellschaft

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

3. Fachliche Grundlagen	1
3.3 Informatik und Gesellschaft	1
Informatik und Gesellschaft	2
3.3.1 Fachbegriff: Big Data	2
3.3.2 Fachbegriff: Web 2.0	2
3.3.3 Fachbegriff: Industrie 4.0	2
3.3.4 Fachbegriff: IoT (Internet of Things)	2
3.3.5 Sprachassistenten: Vor- und Nachteile	2
3.3.6 Government & Digitale Signatur	3
3.3.7 Schutz vor Tracking	3
3.3.8 Gefahr von Identitätsdiebstahl	3
3.3.9 Fachbegriff: Netzneutralität	3
3.3.10 Biometrische Daten: Vor- und Nachteile	3
3.3.11 Unternehmensrichtlinien für Social Media	3

Informatik und Gesellschaft

Dieser Bereich beschreibt die **Wechselwirkung** zwischen der Entwicklung von Informationstechnologien und dem Zusammenleben der Menschen. Er behandelt ethische, rechtliche und soziale Fragen, wie z. B. die digitale Kluft, den Wandel der Arbeitswelt durch Automatisierung und den Einfluss von Algorithmen auf die Meinungsbildung.

3.3.1 Fachbegriff: Big Data

Big Data bezeichnet Datenmengen, die zu groß, zu komplex oder zu schnelllebig sind, um sie mit herkömmlichen Methoden der Datenverarbeitung auszuwerten. Die Definition erfolgt meist über die **"V-Regel"**:

- **Volume:** Enormes Datenvolumen.
- **Velocity:** Hohe Geschwindigkeit der Datenerzeugung.
- **Variety:** Vielfalt der Datenquellen (Text, Video, Sensoren).

3.3.2 Fachbegriff: Web 2.0

Das Web 2.0 markiert den Wandel des Internets vom reinen "Konsum-Medium" (statische Seiten) hin zum **Mitmach-Web**. Nutzer sind nicht mehr nur Leser, sondern Produzenten von Inhalten (*Prosumer*). Beispiele sind Social Media, Wikis und Blogs.

3.3.3 Fachbegriff: Industrie 4.0

Die vierte industrielle Revolution beschreibt die **intelligente Vernetzung** von Maschinen und Abläufen in der Industrie mithilfe von Informations- und Kommunikationstechnologie. Ziel ist die "Smart Factory", in der Produkte und Anlagen autonom miteinander kommunizieren.

3.3.4 Fachbegriff: IoT (Internet of Things)

Das Internet der Dinge bezeichnet die Vernetzung von physischen Objekten ("Dingen") mit dem Internet, damit diese selbstständig kommunizieren und Aufgaben erledigen können.

Beispiel: Ein Kühlschrank, der Milch nachbestellt, oder vernetzte Thermostate, die Energie sparen.

3.3.5 Sprachassistenten: Vor- und Nachteile

Vorteile	Nachteile
Barrierefreiheit: Erleichterte Bedienung für Menschen mit Beeinträchtigung.	Datenschutz: Ständige Aufnahmebereitschaft ("Mithören").
Effizienz: Schnelle Informationssuche und Steuerung per Hand-free.	Profilbildung: Daten werden für personalisierte Werbung genutzt.

3.3.6 Government & Digitale Signatur

- **e-Government:** Die Vereinfachung von Behördenwegen über digitale Kanäle (z. B. FinanzOnline).
- **Digitale Signatur:** Ein kryptografisches Verfahren, das die Echtheit (Authentizität) und Unveränderlichkeit (Integrität) eines digitalen Dokuments garantiert.
- **Handy-Signatur / ID Austria:** Die rechtliche Entsprechung zur eigenhändigen Unterschrift im digitalen Raum, gesichert durch Zwei-Faktor-Authentifizierung.

3.3.7 Schutz vor Tracking

- **Cookie-Tracking:** Browser-Einstellungen nutzen (Cookies von Drittanbietern blockieren), Inkognito-Modus oder Add-ons wie "uBlock Origin".
- **Cookieless-Tracking:** (z. B. Fingerprinting) Hier hilft die Nutzung von VPNs, spezialisierten Browsern (Tor, Brave) oder das Deaktivieren von JavaScript (mit Komforteinbußen).

3.3.8 Gefahr von Identitätsdiebstahl

Hierbei werden personenbezogene Daten (Name, Geburtsdatum, Passwörter) gestohlen, um im Namen des Opfers kriminelle Handlungen zu begehen (z. B. Warenbetrug, Eröffnung von Bankkonten). **Schutz:** Starke Passwörter, MFA (Multi-Faktor-Authentifizierung) und Skepsis bei Phishing-Mails.

3.3.9 Fachbegriff: Netzneutralität

Netzneutralität ist der Grundsatz, dass alle Datenpakete im Internet **gleichberechtigt** übertragen werden müssen – unabhängig von Inhalt, Anwendung, Herkunft oder Ziel. Provider dürfen also keine Dienste (z. B. Netflix) künstlich drosseln oder gegen Aufpreis bevorzugen.

3.3.10 Biometrische Daten: Vor- und Nachteile

Vorteile	Nachteile
Komfort: Kein Merken von Passwörtern (Face-ID, Fingerabdruck).	Unveränderlichkeit: Ein gestohlener Fingerabdruck kann nicht "geändert" werden.
Sicherheit: Schwieriger zu fälschen als einfache PINs.	Missbrauchsgefahr: Zentral gespeicherte Biometrie-Daten sind ein Ziel für Hacker.

3.3.11 Unternehmensrichtlinien für Social Media

Unternehmen legen Regeln fest, um Image und Sicherheit zu schützen:

- **Trennungsgebot:** Klare Trennung zwischen privater Meinung und offiziellen Firmenstatements.

- **Verschwiegenheit:** Verbot der Veröffentlichung von Interna oder Kundendaten.
- **Respekt:** Verpflichtung zu einem höflichen Umgangston (Netiquette).
- **Rechtliches:** Beachtung von Urheberrechten und Kennzeichnungspflichten.

Ausarbeitung-Themenkatalog

3. Fachliche Grundlagen

3.1 Datenaustausch

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Möglichkeiten des Datenaustausches	2
2. Datenübertragung & Bandbreite	2
3. Sichere Verbindungen & Verschlüsselung	3
4. Fachbegriff: VPN (Virtual Private Network)	3
5. Fachbegriff: Intranet	4
6. Schnittstellen & Übertragungstechnologien	4
7. Vor- und Nachteile: Hosting- vs. Cloud-Lösungen	5
8. Voraussetzungen zur Nutzung von Clouddiensten.....	5

4. Möglichkeiten des Datenaustausches

Der Datenaustausch beschreibt den Prozess des Verschiebens oder Kopierens digitaler Informationen zwischen Systemen.

- **Netzwerkfreigaben (SMB/NFS):** In lokalen Netzwerken (LAN) werden Protokolle wie **SMB** (Server Message Block – Windows) oder **NFS** (Network File System – Linux/Unix) genutzt, um Verzeichnisse so bereitzustellen, dass sie wie lokale Festplatten wirken.
- **FTP/SFTP/FTPS:** Das *File Transfer Protocol* ist der Klassiker für das Up- und Downloaden von Dateien auf Webserver. **SFTP** (über SSH) und **FTPS** (über SSL/TLS) sind die sicheren, verschlüsselten Varianten.
- **Cloud-Synchronisation:** Dienste wie OneDrive oder Dropbox nutzen Agenten (Software), die im Hintergrund lokale Ordner mit einem Cloud-Speicher abgleichen (Delta-Synchronisation).
- **E-Mail & Messaging:** Für kleine Dateien. Problematisch ist hier die "Schatten-IT", wenn Mitarbeiter sensible Firmendaten über private Messenger (WhatsApp etc.) austauschen.
- **Web-APIs (REST/SOAP):** Hier tauschen nicht Menschen Dateien aus, sondern Programme Datenpakete (meist im JSON- oder XML-Format), z. B. ein Onlineshop, der Lagerbestände vom Server abfragt.

5. Datenübertragung & Bandbreite

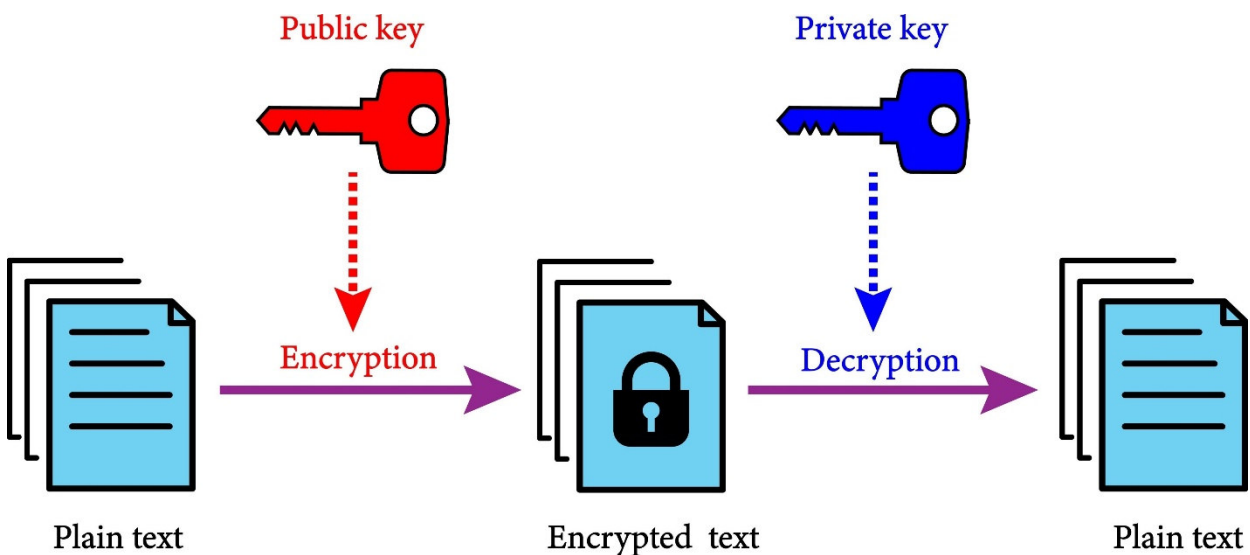
Dies ist die physikalische und logische Basis jedes Austausches.

- **Bandbreite:** Kapazität eines Übertragungskanal. Sie wird in **Bit pro Sekunde** (bps) angegeben.
 - *Beispiel:* 100 Mbit/s bedeutet, dass **theoretisch** 100 Millionen Nullen und Einsen pro Sekunde fließen können.
- **Durchsatz (Throughput):** Die **tatsächlich** erreichte Geschwindigkeit (Netto), die meist unter der theoretischen Bandbreite (Brutto) liegt, da Protokoll-Overhead (Steuerdaten) abgezogen werden muss.
- **Latenz (Verzögerung):** Zeit, die ein Datenpaket vom Sender zum Empfänger und zurück benötigt (Ping). Hohe Bandbreite bedeutet nicht automatisch niedrige Latenz (z. B. Satelliten-Internet).
- **Duplex-Modi:**
 - **Full-Duplex:** Gleichzeitiges Senden und Empfangen (Standard bei modernem Ethernet).
 - **Half-Duplex:** Senden und Empfangen nur abwechselnd (z. B. WLAN oder alte Hubs).

6. Sichere Verbindungen & Verschlüsselung

Sicherheit wird durch die Einhaltung der CIA-Schutzziele (Confidentiality, Integrity, Availability) gewährleistet.

- **Verschlüsselung (Encryption):**
 - **Symmetrisch (z. B. AES):** Ein Schlüssel für alles. Schnell, aber der Schlüsselaustausch ist riskant.
 - **Asymmetrisch (z. B. RSA/ECC):** Ein öffentlicher Schlüssel verschlüsselt, nur der passende private Schlüssel kann entschlüsseln. Ideal für den Verbindungsaufbau.
- **Transportverschlüsselung (TLS/SSL):** Schützt den Weg der Daten (z. B. HTTPS beim Surfen). Die Daten sind auf dem Endgerät und dem Server wieder im Klartext.
- **Ende-zu-Ende-Verschlüsselung (E2EE):** Die Daten sind über den gesamten Weg verschlüsselt, auch der Anbieter des Dienstes (z. B. Cloud-Provider) kann nicht mitlesen.



Shutterstock

7. Fachbegriff: VPN (Virtual Private Network)

Ein VPN ist ein logisches privates Netzwerk auf einer öffentlichen Infrastruktur.

- **Tunneling:** Die Datenpakete werden in ein anderes Protokoll eingekapselt und verschlüsselt.
- **Site-to-Site VPN:** Verbindet zwei Standorte (z. B. Zentrale und Filiale) dauerhaft über Router.
- **Client-to-Site VPN (Roadwarrior):** Verbindet einen einzelnen PC (Home-Office) mit dem Firmennetzwerk.
- **Vorteil:** Erhöhte Sicherheit und Zugriff auf interne Ressourcen (Drucker, Dateiserver), ohne diese im Internet freigeben zu müssen.

8. Fachbegriff: Intranet

Ein geschlossener Informationsraum innerhalb einer Organisation.

- **Technologie:** Nutzt Standard-Webtechnologien (HTTP, Browser), ist aber durch Firewalls vom Internet abgesichert.
- **Zweck:** Bereitstellung von Informationen (Unternehmensnews, Telefonlisten, Richtlinien) und Tools (Urlaubsplaner, Wiki).
- **Abgrenzung:**
 - **Internet:** Öffentlich für alle.
 - **Intranet:** Nur für interne Mitarbeiter.
 - **Extranet:** Autorisierte Externe (Partner, Kunden) erhalten Zugriff auf spezifische Intranet-Bereiche.

9. Schnittstellen & Übertragungstechnologien

Man unterscheidet zwischen physischen Anschlüssen und den darauf laufenden Standards.

- **Ethernet (IEEE 802.3):** Der Standard für kabelgebundene Netze. Übertragungsmedien sind Kupferkabel (Twisted Pair, Cat 5e bis Cat 8) oder Glasfaser (Single-Mode/Multi-Mode).
- **WLAN (IEEE 802.11):** Funkübertragung. Aktuelle Standards wie Wi-Fi 6 (802.11ax) nutzen Frequenzen im 2,4 GHz, 5 GHz und teils 6 GHz Band.
- **Schnittstellen:**
 - **RJ45:** Standardstecker für Netzkabel.
 - **SFP/SFP+:** Einschubmodule für Glasfaserverbindungen an Switches.
 - **USB-C:** Multifunktionsschnittstelle, die Daten, Video und Strom (Power Delivery) übertragen kann.

10. Vor- und Nachteile: Hosting- vs. Cloud-Lösungen

In der IT-Strategie unterscheidet man oft zwischen:

- **On-Premise:** Hardware steht im eigenen Haus.
- **Hosting:** Ein Server (dediziert oder virtuell) wird in einem Rechenzentrum gemietet.
- **Cloud (SaaS/PaaS/IaaS):** Ressourcen werden flexibel über das Internet bezogen.

Kriterium	Cloud-Lösung	On-Premise / Eigenbau
Kostenstruktur	OPEX (laufende Kosten, Pay-per-use)	CAPEX (hohe Investitionen zu Beginn)
Wartung	Durch Anbieter (Updates, Hardware-Tausch)	Durch eigene IT-Abteilung
Skalierbarkeit	Nahezu unbegrenzt auf Knopfdruck	Begrenzt durch gekaufte Hardware
Kontrolle	Abhängigkeit vom Provider (SLA)	Volle Kontrolle über alle Schichten
Internet	Zwingend erforderlich	Interner Betrieb auch offline möglich

11. Voraussetzungen zur Nutzung von Clouddiensten

Bevor ein Unternehmen in die Cloud wechselt, müssen diese Punkte geklärt sein:

1. **Konnektivität:** Eine redundante Internetanbindung (z. B. Glasfaser + 5G-Backup), da bei Internet-Ausfall kein Arbeiten mehr möglich ist.
2. **Identitätsmanagement:** Ein System wie Azure AD (Entra ID), um Benutzerrechte zentral zu steuern.
3. **Datenschutz (Compliance):** Prüfung, ob der Anbieter Daten in Drittstaaten (USA) überträgt und ob ein AV-Vertrag vorliegt.
4. **Security:** Implementierung von **Multi-Faktor-Authentifizierung (MFA)**, da ein gestohlenes Passwort sonst Zugriff auf alle Firmendaten in der Cloud erlaubt.
5. **Exit-Strategie:** Wie bekommt man die Daten wieder weg vom Anbieter, falls man kündigen möchte (Vendor Lock-in vermeiden)?

Ausarbeitung-Themenkatalog

4. Grundlagen in der Informationstechnik

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

4. Grundlagen in der Informationstechnik	1
4.1 Fachbegriffe Hardware & Software	2
4.2 Das EVA-Prinzip	2
Signal- und Schaltungstechnik	2
4.3 Analog- vs. Digitaltechnik	2
Dateneinheiten und Zeichencodierung	3
4.4 ASCII (American Standard Code for Information Interchange).....	3
4.5 Bit & Byte.....	3
4.6 Speichergrößen: Dezimal vs. Binär (SI vs. IEC)	3
Zahlensysteme und Umwandlung	4
4.7 Gebräuchliche Zahlensysteme	4
4.8 Umwandlungs-Logik	4

4.1 Fachbegriffe Hardware & Software

- **Hardware:** Alle physischen, greifbaren Komponenten eines Computersystems (z. B. Prozessor, Mainboard, Festplatte).
- **Software:** Die Gesamtheit aller Programme und Daten, die auf der Hardware ausgeführt werden. Man unterscheidet primär zwischen **Systemsoftware** (Betriebssystem) und **Anwendungssoftware** (Browser, Office).

4.2 Das EVA-Prinzip

Das EVA-Prinzip beschreibt den grundlegenden Weg der Datenverarbeitung:

1. **Eingabe:** Daten werden über **Eingabegeräte** (Tastatur, Maus, Scanner) aufgenommen.
2. **Verarbeitung:** Die Zentraleinheit (CPU) verarbeitet die Daten nach Programmvorgaben.
3. **Ausgabe:** Die Ergebnisse werden über **Ausgabegeräte** (Monitor, Drucker, Lautsprecher) ausgegeben.

Signal- und Schaltungstechnik

4.3 Analog- vs. Digitaltechnik

- **Analogtechnik:** Verwendet kontinuierliche Signale, die jeden beliebigen Wert innerhalb eines Bereichs annehmen können (z. B. eine Schallwelle oder ein Zeigerinstrument).
- **Digitaltechnik:** Verwendet diskrete Werte (meist 0 und 1). Zustände sind klar voneinander getrennt, was die Speicherung und Übertragung wesentlich fehlerresistenter macht.

Logik-Schaltungen (Gatter)

Logische Verknüpfungen bilden das Fundament der digitalen Signalverarbeitung.

Gatter	Beschreibung	Logischer Ausdruck
AND (Und)	Ausgang ist 1, wenn beide Eingänge 1 sind.	$Y=A \wedge B$
OR (Oder)	Ausgang ist 1, wenn mindestens einer der Eingänge 1 ist.	$Y=A \vee B$
XOR (Exklusiv-Oder)	Ausgang ist 1, wenn die Eingänge unterschiedlich sind.	$Y=A \oplus B$
NOT (Nicht)	Invertiert das Signal (aus 1 wird 0 und umgekehrt).	$Y=\neg A$

Dateneinheiten und Zeichencodierung

4.4 ASCII (American Standard Code for Information Interchange)

Ein Standard zur Zeichenkodierung, der Textzeichen (Buchstaben, Zahlen, Sonderzeichen) Zahlenwerten zuordnet. Der ursprüngliche ASCII nutzt **7 Bit** (128 Zeichen). Heute ist er meist die Basis für modernere Codes wie UTF-8.

4.5 Bit & Byte

- **Bit (Binary Digit):** Die kleinste Informationseinheit (Zustand 0 oder 1).
- **Byte:** Eine Gruppe von **8 Bit**. Es ist die kleinste adressierbare Dateneinheit und kann 256 verschiedene Zustände darstellen.

4.6 Speichergrößen: Dezimal vs. Binär (SI vs. IEC)

In der IT gibt es oft Verwirrung durch die Verwendung von 1000er- vs. 1024er-Schritten.

Typ	Basis	Einheiten (Beispiele)	Verwendung
Dezimal (SI)	$10^3=1000$	KB, MB, GB, TB, PB, EB	Festplattenhersteller, Marketing
Binär (IEC)	$2^{10}=1024$	KiB, MiB, GiB, TiB, PiB, EiB	Betriebssysteme (RAM, Dateigrößen)

Einheit (binär/IEC)	Faktor	Entspricht exakt
1 KiB (Kibibyte)	1024^1	1.024 Byte
1 MiB (Mebibyte)	1024^2	1.048.576 Byte
1 GiB (Gibibyte)	1024^3	1.073.741.824 Byte
1 TiB (Tebibyte)	1024^4	1.099.511.627.776 Byte

Wichtig: Ein "Gibibyte" (GiB) ist also exakt 1024^3 Byte, während ein "Gigabyte" (GB) oft als 1000^3 Byte definiert wird.

Zahlensysteme und Umwandlung

4.7 Gebräuchliche Zahlensysteme

1. **Dezimalsystem:** Basis 10 (Ziffern 0-9). Unser Alltagssystem.
2. **Binärsystem:** Basis 2 (Ziffern 0, 1). Die "Sprache" der Hardware (Strom an/aus).
3. **Hexadezimalsystem:** Basis 16 (0-9 und A-F). Dient der übersichtlichen Darstellung großer Binärzahlen (z. B. MAC-Adressen, Farbcodes).

4.8 Umwandlungs-Logik

- **Dezimal zu Binär:** Fortlaufende Division durch 2, wobei die Reste von unten nach oben gelesen werden.
- **Binär zu Dezimal:** Addition der Stellenwerte (2⁰, 2¹, 2²...), bei denen eine "1" steht.
- **Binär zu Hexadezimal:** Man gruppiert jeweils **4 Bit** (ein Nippel) und ersetzt diese durch die entsprechende Hex-Ziffer (z. B. 1010 binär = A hex).

Ausarbeitung-Themenkatalog

5. Benutzerendgeräte und Peripheriegeräte

5.1 Hardwaresysteme

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags/Laborauftrages im Unterrichtsfach **Betriebssysteme & Labor**.

Inhalt

5. Benutzerendgeräte und Peripheriegeräte	1
5.1 Hardwaresysteme	1
Systemaufbau & Zentraleinheit	3
5.1.1 Zusammenbau eines PC-Systems	3
5.1.2 Fachbegriff CPU (Central Processing Unit)	3
Speichertechnologien	3
5.1.3 Flüchtiger vs. Nichtflüchtiger Speicher	3
5.1.4 ROM (Read Only Memory) & Flash-RAM	3
5.1.5 RAM (Random Access Memory) & Cache	4
5.1.6 HDD, SSD & SSHD	4
Firmware & Systemstart	4
5.1.7 BIOS vs. UEFI	4
5.1.8 Plug & Play (PnP)	4
Grafik & Video	5
5.1.9 Grafikkarte & Video-RAM (VRAM)	5
5.1.10 Grafikstandards & Schnittstellen	5
Mobile Datenträger & Schnittstellen	5
5.1.11 Speicherkarten & Mobile Datenträger	5
5.1.12 Schnittstellen (SATA, Seriell, USB)	5
Eingabegeräte & Peripherie	6
5.1.13 Tastatur & Optische Maus	6
5.1.14 Funk-Eingabegeräte	6
Druck- & Scantechnologie	6
5.1.15 Laserdrucker (Funktionsprinzip)	6

5.1.16 Tintenstrahldrucker	7
5.1.17 Scanner	7

Systemaufbau & Zentraleinheit

5.1.1 Zusammenbau eines PC-Systems

Der Zusammenbau folgt einer logischen Reihenfolge, um Schäden durch Elektrostatik (ESD) zu vermeiden:

1. **Vorbereitung:** ESD-Armband anlegen, Mainboard auf eine isolierende Unterlage legen.
2. **CPU-Installation:** CPU in den Sockel setzen (Markierungen beachten!), Arretierung schließen.
3. **RAM & M.2 SSD:** Arbeitsspeicher in die korrekten Slots (Dual-Channel beachten) und M.2 SSDs einbauen.
4. **Einbau ins Gehäuse:** Abstandshalter prüfen, I/O-Shield einsetzen, Mainboard verschrauben.
5. **Kühlung & Netzteil:** CPU-Kühler montieren (Wärmeleitpaste!), Netzteil einbauen.
6. **Verkabelung:** Stromversorgung (24-Pin ATX, 8-Pin CPU), Gehäuse-Anschlüsse (Front-Panel), SATA-Kabel.
7. **Grafikkarte:** GPU in den obersten PCIe-Slot setzen und mit Strom versorgen.

5.1.2 Fachbegriff CPU (Central Processing Unit)

Die CPU ist die zentrale Recheneinheit. Sie holt Befehle aus dem Speicher, dekodiert sie und führt sie in der Rechenlogik (ALU) aus. Wichtige Parameter sind die **Taktfrequenz** (GHz), die Anzahl der **Kerne/Threads** und die **IPC** (Instruktionen pro Taktzyklus).

Speichertechnologien

5.1.3 Flüchtiger vs. Nichtflüchtiger Speicher

- **Flüchtiger Speicher (Volatile):** Benötigt permanent Strom, um Informationen zu halten. Bei Stromverlust werden alle Daten gelöscht (Beispiel: **RAM, Cache**).
- **Nichtflüchtiger Speicher (Non-Volatile):** Speichert Daten dauerhaft, auch ohne Stromzufuhr (Beispiel: **HDD, SSD, ROM, Flash**).

5.1.4 ROM (Read Only Memory) & Flash-RAM

- **ROM:** Ein Speicher, der im Normalbetrieb nur gelesen werden kann. Er enthält fest einprogrammierte Routinen (z. B. für den Systemstart).

- **Flash-RAM:** Eine Weiterentwicklung des EEPROMs. Er ist nichtflüchtig, kann aber elektronisch gelöscht und wiederbeschrieben werden. Einsatz in USB-Sticks, SD-Karten und SSDs.

5.1.5 RAM (Random Access Memory) & Cache

- **RAM:** Der Hauptspeicher für laufende Programme und Daten. Aktuelle Technologien: **DDR4** und **DDR5**. DDR5 bietet höhere Bandbreiten und integrierte Fehlerkorrektur (ODECC).
- **Cache:** Extrem schneller, kleiner Speicher (L1, L2, L3) direkt in oder an der CPU, um die Geschwindigkeitsdifferenz zwischen CPU und dem langsameren RAM zu überbrücken.

5.1.6 HDD, SSD & SSHD

- **HDD (Hard Disk Drive):** Magnetische Speicherung auf rotierenden Scheiben. Günstig, hohe Kapazität, aber langsam und stoßempfindlich.
- **SSD (Solid State Drive):** Halbleiterspeicher (Flash). Lautlos, extrem schnell, unempfindlich gegen Erschütterungen.
- **SSHD (Solid State Hybrid Drive):** Eine HDD mit einem kleinen SSD-Cache für häufig genutzte Daten. Gilt heute als veraltet.

Firmware & Systemstart

5.1.7 BIOS vs. UEFI

- **BIOS (Basic Input/Output System):** Textbasiert, unterstützt nur Festplatten bis 2,2 TB, arbeitet im 16-Bit-Modus.
- **UEFI (Unified Extensible Firmware Interface):** Grafische Oberfläche (Maus), unterstützt GPT-Partitionen (> 2,2 TB), bietet **Secure Boot** und schnellere Startzeiten.

5.1.8 Plug & Play (PnP)

Ein Standard, der es ermöglicht, Hardware ohne manuelle Konfiguration (Jumper, IRQs) anzuschließen. Das System erkennt das Gerät automatisch, weist Ressourcen zu und lädt den passenden Treiber.

Grafik & Video

5.1.9 Grafikkarte & Video-RAM (VRAM)

Eine Grafikkarte übernimmt die Berechnung der Bildausgabe, um die CPU zu entlasten.

- **Aufbau:** Besteht aus Grafikprozessor (**GPU**), **VRAM**, Spannungsversorgung und Kühlsystem.
- **VRAM:** Spezialisierter Speicher (aktuell **GDDR6** oder **GDDR6X**), der über ein sehr breites Speicherinterface an die GPU angebunden ist, um enorme Datenmengen für Texturen und Bildpuffer bereitzustellen.

5.1.10 Grafikstandards & Schnittstellen

- **Grafikstandards:** Beschreiben Auflösungen und Funktionen (z. B. **DirectX** für Spiele, **Vulkan** oder **OpenGL**).
 - **HDMI:** Kombiniert Audio/Video, Standard für Heimkino.
 - **DisplayPort:** IT-Standard, höhere Bandbreite, unterstützt Daisy-Chaining.
 - **DVI:** Digitaler Standard (älter), überträgt nur Bildsignale, kein Audio.
-

Mobile Datenträger & Schnittstellen

5.1.11 Speicherkarten & Mobile Datenträger

- **Magnetisch:** Externe HDDs (große Kapazität, günstig).
- **Optisch:** DVD (4,7 GB), Blu-ray (25–100 GB). Robust gegen Magnetismus, aber kratzempfindlich.
- **Elektronisch:** USB-Sticks, SD-Karten (SDHC bis 32GB, SDXC bis 2TB). Bauformen: microSD, SD.

5.1.12 Schnittstellen (SATA, Seriell, USB)

- **SATA (Serial ATA):** Schnittstelle für HDDs/SSDs/Laufwerke. SATA III bietet bis zu 6 Gbit/s.
- **Serielle Schnittstelle (RS-232):** Überträgt Bits nacheinander. Heute noch wichtig für Wartungszugänge (Console) an Netzwerkgeräten.
- **USB (Universal Serial Bus):**
 - **USB 2.0:** 480 Mbit/s (High Speed).

- **USB 3.0 / 3.1 Gen 1 / 3.2 Gen 1:** 5 Gbit/s (SuperSpeed).
- **USB 3.2 Gen 2:** 10 Gbit/s.
- **USB 3.2 Gen 2x2:** 20 Gbit/s.
- **USB4:** Bis zu 40/80 Gbit/s (USB-C Stecker erforderlich).

Eingabegeräte & Peripherie

5.1.13 Tastatur & Optische Maus

- **Tastatur:** Arbeitet mit einer Matrix. Beim Tastendruck wird ein Stromkreis geschlossen, ein Controller sendet den Scancode an den PC.
- **Optische Maus:** Eine kleine Kamera fotografiert die Oberfläche tausende Male pro Sekunde. Ein DSP (Digitaler Signalprozessor) berechnet aus den Unterschieden der Bilder die Bewegungsrichtung und Geschwindigkeit.

5.1.14 Funk-Eingabegeräte

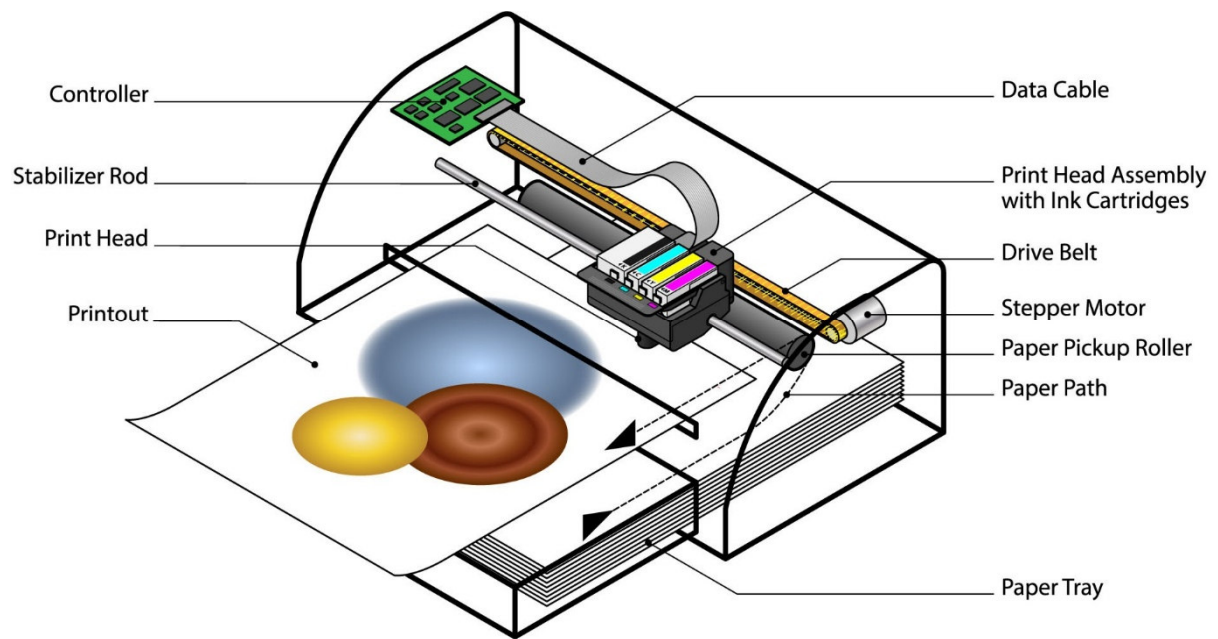
- **Vorteile:** Keine Kabel auf dem Schreibtisch, größere Reichweite, hohe Flexibilität.
- **Nachteile:** Batterien/Akkus nötig, potenzielle Funkstörungen, minimale Latenz (Verzögerung), Sicherheitsrisiko (Abhören ohne Verschlüsselung).

Druck- & Scantechnologie

5.1.15 Laserdrucker (Funktionsprinzip)

Arbeitet elektrofotografisch:

1. **Laden:** Eine Bildtrommel wird statisch aufgeladen.
2. **Belichten:** Ein Laser entlädt die Trommel an den Stellen, die bedruckt werden sollen.
3. **Entwickeln:** Toner (Pulver) haftet an den geladenen Stellen.
4. **Übertragen:** Der Toner wird auf das Papier übertragen.
5. **Fixieren:** Hitze und Druck schmelzen den Toner in die Papierfasern.



Getty Images

5.1.16 Tintenstrahldrucker

Spritzt winzige Tintentropfen auf das Papier. Man unterscheidet:

- **Thermal (Bubblejet):** Tinte wird erhitzt, Dampfblase drückt Tropfen raus.
- **Piezo-Technik:** Elektrische Spannung verformt einen Kristall, der den Tropfen mechanisch rauspresst.

5.1.17 Scanner

Beleuchtet das Dokument und fängt das reflektierte Licht über Sensoren (**CCD** oder **CIS**) ein.

- **Flachbettscanner:** Standard für Dokumente.
- **Einzugsscanner (ADF):** Für große Mengen an Einzelblättern.
- **Handscanner:** Zum manuellen Führen über Objekte.

Prüfungsvorbereitung

5. Benutzerendgeräte und Peripheriegeräte

5.2 Betriebssysteme und Software

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

5. Benutzerendgeräte und Peripheriegeräte	1
5.2 Betriebssysteme und Software	1
5.2.1 Fachbegriff Betriebssystem	3
5.2.2 Kenntnisse der am Markt führend verbreiteten Betriebssysteme	3
Windows (Microsoft)	3
macOS (Apple)	3
Linux.....	3
Android (Google)	3
iOS / iPadOS (Apple)	3
5.2.3 Kenntnisse über Desktop-Betriebssysteme.....	3
5.2.4 Fachbegriff Firmware	4
5.2.5 Fachbegriffe Systemprogramm, Anwendungsprogramm	4
Systemprogramm	4
Anwendungsprogramm	5
5.2.6 Fachbegriff Multitasking-Betriebssystem.....	5
5.2.7 Fachbegriffe Single-User-System, Multi-User-System	5
Single-User-System	5
Multi-User-System	5
5.2.8 Kenntnis der Windows Command-Line (inkl. einfacher Befehle)	6
5.2.9 Kenntnis über die PowerShell (inkl. einfacher Befehle).....	6
5.2.10 Kenntnisse über grafische Oberflächen unter Linux	7
5.2.11 Fachbegriff Dateisystem	8
5.2.12 Fachbegriffe FAT, NTFS.....	8
FAT (File Allocation Table)	8
NTFS (New Technology File System)	8

5.2.1 Fachbegriff Betriebssystem

Ein Betriebssystem (Operating System, OS) ist die zentrale Systemsoftware, die die Hardware eines Geräts verwaltet und die Ausführung von Programmen ermöglicht.

5.2.2 Kenntnisse der am Markt führend verbreiteten Betriebssysteme

Die marktführenden Betriebssysteme sind **Windows** und **macOS** bei Computern sowie **Android** und **iOS** bei mobilen Geräten. **Linux** ist besonders im Serverbereich verbreitet.

Windows (Microsoft)

- Weltweit am häufigsten genutzt
- Große Software- und Hardware-Kompatibilität
- Standard in Unternehmen

macOS (Apple)

- Nur auf Apple-Computern
- Sehr stabiles, geschlossenes System
- Beliebt bei Kreativ Anwendungen

Linux

- Open Source
- Viele Varianten (Distributionen)
- Häufig bei Servern und Technikern

Android (Google)

- Marktführer bei Smartphones und Tablets
- Auf Geräten vieler Hersteller
- Offenes System

iOS / iPadOS (Apple)

- Nur auf iPhone und iPad
- Geschlossenes, stark optimiertes System

5.2.3 Kenntnisse über Desktop-Betriebssysteme

Desktop-Betriebssysteme wie Windows, macOS und Linux verwalten Computerhardware und stellen die Benutzeroberfläche für Programme bereit.

Merkmal	Windows	macOS	Linux
Verbreitung	Sehr hoch	Mittel	Gering (Desktop)

Offenheit	Geschlossen	Geschlossen	Offen (Open Source)
Anpassbarkeit	Mittel	Gering	Sehr hoch
Sicherheit	Gut	Sehr gut	Sehr gut

5.2.4 Fachbegriff Firmware

Firmware ist fest gespeicherte Software, die die Hardware eines Geräts initialisiert und den Start des Betriebssystems ermöglicht.

Firmware ist die erste Software, die ein Gerät beim Einschalten ausführt.

Sie sagt der Hardware, was sie tun soll, noch bevor das Betriebssystem startet.

Wo befindet sich Firmware?

- In Flash- oder ROM-Speicherchips
- Direkt auf dem Gerät gespeichert
- Bleibt auch ohne Strom erhalten

Typische Beispiele

- BIOS / UEFI im PC
- Firmware im Router
- Firmware in Smartphones
- Firmware in Druckern

Eigenschaften

- Sehr hardwarenah
- Wird selten geändert
- Updates möglich (Firmware-Update)

5.2.5 Fachbegriffe Systemprogramm, Anwendungsprogramm

Systemprogramm

Ein Systemprogramm ist Software, die das Betriebssystem unterstützt, die Hardware verwaltet und grundlegende Systemfunktionen bereitstellt.

Beispiele

- Betriebssystem selbst (Windows, Android, iOS)
- Treiber (z. B. Druckertreiber)
- Dienstprogramme (z. B. Virens Scanner, Backup-Tools)

Aufgabe

- Sorgt dafür, dass Programme auf die Hardware zugreifen können

- Läuft meist im Hintergrund

Anwendungsprogramm

Ein Anwendungsprogramm ist Software, die konkrete Aufgaben für den Benutzer ausführt.

Beispiele

- Textverarbeitung (Word)
- Browser (Chrome, Firefox)
- Spiele
- Musik- und Bildbearbeitung

Aufgabe

- Direkter Nutzen für den Anwender
- Läuft auf dem Betriebssystem

5.2.6 Fachbegriff Multitasking-Betriebssystem

Ein Multitasking-Betriebssystem ist ein Betriebssystem, das mehrere Programme gleichzeitig ausführen und verwalten kann.

5.2.7 Fachbegriffe Single-User-System, Multi-User-System

Single-User-System

Ein Single-User-System ist ein Betriebssystem, das zur gleichen Zeit nur von einer Person genutzt werden kann.

Eigenschaften

- Ein aktiver Benutzer gleichzeitig
- Typisch für PCs, Laptops, Smartphones
- Benutzer kann mehrere Programme nutzen, aber nur eine Person

Beispiele

- Windows-PC zu Hause
- Smartphone mit Android oder iOS

Multi-User-System

Ein Multi-User-System ist ein Betriebssystem, das gleichzeitige Nutzung durch mehrere Benutzer ermöglicht.

Eigenschaften

- Mehrere Benutzer gleichzeitig angemeldet
- Ressourcen werden gemeinsam verwaltet
- Jeder Nutzer hat eigene Daten und Rechte

Beispiele

- Server mit Linux oder Windows Server
- Großrechner in Unternehmen

5.2.8 Kenntnis der Windows Command-Line (inkl. einfacher Befehle)

Die Windows Command-Line ist eine textbasierte Steuerung des Betriebssystems, bei der Befehle wie `dir`, `cd` oder `ipconfig` zur System- und Dateiverwaltung genutzt werden.

Wichtige Grundbefehle

Befehl	Funktion	Beispiel
dir	Zeigt Dateien im aktuellen Ordner	<code>dir</code>
cd	Ordner wechseln	<code>cd Dokumente</code>
mkdir	Neuen Ordner erstellen	<code>mkdir Test</code>
del	Datei löschen	<code>del datei.txt</code>
copy	Datei kopieren	<code>copy a.txt b.txt</code>
cls	Bildschirm löschen	<code>cls</code>
exit	CMD schließen	<code>exit</code>

Nützliche Systembefehle

Befehl	Funktion
ipconfig	Zeigt Netzwerkdaten
ping	Prüft Netzwerkverbindung
tasklist	Zeigt laufende Programme
shutdown	Computer herunterfahren

5.2.9 Kenntnis über die PowerShell (inkl. einfacher Befehle)

Die PowerShell ist eine erweiterte Windows-Kommandozeile zur Systemverwaltung und Automatisierung, die mit objektorientierten Befehlen arbeitet.

Befehl	Funktion
Get-Help	Hilfe zu Befehlen anzeigen
Get-Command	Alle verfügbaren Befehle anzeigen

Get-Process	Laufende Programme anzeigen
Get-Service	Dienste anzeigen
Get-ChildItem	Dateien im Ordner anzeigen (wie dir)
Set-Location	Ordner wechseln (wie cd)
Clear-Host	Bildschirm leeren
Get-Help	Hilfe zu Befehlen anzeigen
Get-Command	Alle verfügbaren Befehle anzeigen
Get-Process	Laufende Programme anzeigen
Get-Service	Dienste anzeigen
Get-ChildItem	Dateien im Ordner anzeigen (wie dir)

5.2.10 Kenntnisse über grafische Oberflächen unter Linux

Eine grafische Oberfläche (GUI) ermöglicht die Bedienung eines Betriebssystems über Fenster, Symbole und Mauszeiger.

Unter Linux ist die grafische Oberfläche nicht fest eingebaut, sondern kann frei gewählt werden.

Wichtige Linux-Desktops

GNOME

- Sehr modern und schlicht
- Standard bei Ubuntu und Fedora
- Fokus auf einfache Bedienung

KDE Plasma

- Stark anpassbar
- Ähnlich zu Windows
- Viele Einstellungsmöglichkeiten

XFCE

- Leichtgewichtig
- Benötigt wenig Ressourcen
- Ideal für ältere Computer

LXQt

- Sehr ressourcensparend
- Für schwache Hardware

5.2.11 Fachbegriff Dateisystem

Ein Dateisystem ist die Struktur und Methode, mit der ein Betriebssystem Daten auf einem Speichergerät organisiert, speichert und verwaltet.

5.2.12 Fachbegriffe FAT, NTFS

FAT ist ein einfaches, weit kompatibles Dateisystem, während NTFS erweiterte Sicherheits- und Verwaltungsfunktionen bietet.

FAT (File Allocation Table)

Merkmale

- Sehr weit verbreitet
- Hohe Kompatibilität (Windows, Linux, macOS)
- Begrenzte Dateigröße (FAT32: max. 4 GB)
- Keine Benutzerrechte oder Verschlüsselung

Typische Nutzung

- USB-Sticks
- SD-Karten
- Ältere Geräte

NTFS (New Technology File System)

Merkmale

- Unterstützt sehr große Dateien
- Benutzer- und Zugriffsrechte
- Dateiverschlüsselung möglich
- Fehlerprotokollierung (Journaling)

Typische Nutzung

- Windows-Systemfestplatten
- Server

Ausarbeitung-Themenkatalog

5. Benutzerendgeräte und Peripheriegeräte

5.1 Mobile Hardware

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Technische Merkmale von Smartphones	2
2. Technische Merkmale von Tablets	2
3. Kenntnisse über die Akku-Technologien (NiMh/LiPo/Lilon)	2
4. Kenntnisse über kapazitive Touchscreens	2
5. Kenntnisse über verbaute Sensorik und dessen Nutzungsmöglichkeiten.....	2
6. Fachbegriff Multitouch	3
7. Kenntnisse über Bluetooth Standards	4
8. Kenntnisse über Betriebssysteme mobiler Geräte (Android, IOS,..)	4
9. Fachbegriff QR-Code	5
10. Vor- und Nachteile von geschlossenen Systemen mit Betriebssystem und App-Store	5
11. Fachbegriff Roaming	5
12. Kenntnisse über Vor- und Nachteile von Daten-Roaming Kenntnisse über Verschlüsselungs- und Schutztechnologien von mobilen Endgeräten.....	5
13. Kenntnisse über Virenschutz und Backupmöglichkeit bei mobilen Endgeräten.....	6
14. Kenntnisse über MDM	7
15. Fachbegriff Convertible.....	7
16. Kenntnis der Merkmale von Mobile-Prozessoren	7
17. Fachbegriffe E-Ink, OLED.....	7
18. Fachbegriff Edge, 3G bzw. UMTS, 4G bzw. LTE, 5G	7
19. Fachbegriff HSDPA	7
20. Fachbegriff NFC.....	8
21. Fachbegriff GPS/GPS-Tracking	8
22. Kenntnisse über Daten-Zugriffsschutzmöglichkeiten bei Diebstahl von mobilen Endgeräten.....	8

6. Technische Merkmale von Smartphones

Smartphones besitzen einen Prozessor (CPU), Arbeitsspeicher (RAM), internen Speicher, Touchscreen, Kameras, Akku, Funkmodule (WLAN, Mobilfunk, Bluetooth) sowie ein mobiles Betriebssystem.

7. Technische Merkmale von Tablets

- Tablets sind mobile Computer mit Touchscreen
- Wichtige Merkmale: Prozessor, RAM, Speicher, Display, Akku und Kommunikation
- Betriebssystem steuert alle Funktionen

8. Kenntnisse über die Akku-Technologien (NiMH/LiPo/Lilon)

- NiMH: robuste ältere Technik, aber schwer und hohe Selbstentladung
- Li-Ion: Standardakku moderner Geräte
- Li-Po: dünne, flexible High-End-Variante

9. Kenntnisse über kapazitive Touchscreens

Ein kapazitiver Touchscreen erkennt Berührungen durch Änderung der elektrischen Kapazität auf der Displayoberfläche.

Kapazitive Touchscreens erkennen Fingerberührungen durch Änderung eines elektrischen Feldes und ermöglichen Multi-Touch-Bedienung.

10. Kenntnisse über verbaute Sensorik und dessen Nutzungsmöglichkeiten

Sensoren erfassen Bewegung, Position, Licht, Nähe, Umwelt und biometrische Daten. Sie ermöglichen automatische Bildschirmsteuerung, Navigation, Sicherheit und interaktive Anwendungen.

Bewegungssensoren

- Beschleunigungssensor (Accelerometer)
 - Erkennt Bewegung und Lage
 - Nutzung: Bildschirm dreht sich automatisch, Schrittzähler
- Gyroskop
 - Misst Drehbewegungen
 - Nutzung: 3D-Spiele, VR-Anwendungen, Bildstabilisierung

Positionssensoren

- GPS

- Bestimmt den Standort
 - Nutzung: Navigation, Karten-Apps, Tracking
- Kompass (Magnetometer)
 - Erkennt Himmelsrichtung
 - Nutzung: Navigations-App zeigt Richtung an

Näherungs- und Lichtsensoren

- Näherungssensor
 - Erkennt Objekte in der Nähe
 - Nutzung: Bildschirm schaltet sich beim Telefonieren aus
- Helligkeitssensor
 - Misst Umgebungslicht
 - Nutzung: Automatische Display-Helligkeit

Biometrische Sensoren

- Fingerabdrucksensor
 - Erkennt den Benutze
 - Nutzung: Entsperren, Bezahlen
- Gesichtserkennung (Face-ID)
 - Erfasst Gesicht
 - Nutzung: Geräteentsperrung

Umweltsensoren

- Mikrofon
 - Erkennt Geräusche
 - Nutzung: Sprachassistent, Telefonie
- Barometer
 - Misst Luftdruck
 - Nutzung: Höhenmessung, Wetter-Apps
- Temperatursensor
 - Misst Gerätetemperatur
 - Nutzung: Schutz vor Überhitzung

Kameras als Sensoren

- Erfassen Licht und Bilder
- Nutzung: Fotos, Videos, QR-Code-Scanner, AR-Anwendungen

11. Fachbegriff Multitouch

Multitouch bezeichnet eine Touchscreen-Technologie, bei der mehrere Berührungspunkte gleichzeitig erkannt und verarbeitet werden können.

Multitouch bedeutet, dass ein Touchscreen mehrere gleichzeitige Berührungen erkennt und verarbeitet.

12. Kenntnisse über Bluetooth Standards

Bluetooth ist ein Kurzstrecken-Funkstandard bei 2,4 GHz. Neuere Versionen bieten mehr Reichweite, höhere Geschwindigkeit und geringeren Energieverbrauch. BLE ist für stromsparende Geräte optimiert.

- Bluetooth 4.x
- Bluetooth 5.0
- Bluetooth 5.1
- Bluetooth 5.2
- **Bluetooth 5.3**
- **Bluetooth 5.4 → derzeitiger Standard**

13. Kenntnisse über Betriebssysteme mobiler Geräte (Android, iOS,..)

Mobile Betriebssysteme wie Android und iOS steuern die Hardware, verwalten Apps und sorgen für Sicherheit und Benutzeroberfläche.

Android (Google)

- Weltweit am häufigsten genutzt
- Open-Source-System
- Auf Geräten vieler Hersteller (Samsung, Xiaomi, etc.)
- Hohe Anpassbarkeit
- Vorteile:
- Große App-Auswahl
- Viele Geräteklassen
- Erweiterbarer Speicher oft möglich

iOS (Apple)

- Nur auf iPhone-Geräten
- Sehr stabiles, geschlossenes System
- Lange Software-Updates
- Vorteile:
- Hohe Sicherheit
- Sehr gute Optimierung
- Einheitliches Design

iPadOS (Apple)

- Speziell für Tablets
- Erweiterte Multitasking-Funktionen

- Unterstützung für Stift und Tastatur

14. Fachbegriff QR-Code

Ein QR-Code (Quick Response Code) ist ein zweidimensionaler Matrixcode, der Informationen maschinell lesbar speichert und über die Kamera eines Geräts schnell ausgelesen werden kann.

15. Vor- und Nachteile von geschlossenen Systemen mit Betriebssystem und App-Store

Ein geschlossenes System ist eine Plattform, bei der Betriebssystem, Hardware und App-Store vom selben Anbieter kontrolliert werden.

Geschlossenen Systeme bieten hohe Sicherheit und Stabilität, schränken aber die Freiheit und Anpassbarkeit der Nutzer ein.

16. Fachbegriff Roaming

Roaming bezeichnet die Nutzung des Mobilfunknetzes eines fremden Netzbetreibers, wenn sich ein Gerät außerhalb des Heimatnetzes befindet.

17. Kenntnisse über Vor- und Nachteile von Daten-Roaming Kenntnisse über Verschlüsselungs- und Schutztechnologien von mobilen Endgeräten

Was ist Daten-Roaming?

Smartphones nutzen im Ausland ein fremdes Mobilfunknetz, um mobiles Internet bereitzustellen.

Daten-Roaming ermöglicht mobiles Internet im Ausland, kann aber zusätzliche Kosten verursachen.

Verschlüsselungen

- Geräteverschlüsselung
 - Alle gespeicherten Daten werden verschlüsselt
 - Ohne Entsperrcode kein Zugriff möglich
- Ende-zu-Ende-Verschlüsselung
 - Nachrichten sind nur für Sender und Empfänger lesbar
 - Nutzung z. B. bei WhatsApp oder Signal
- HTTPS / TLS
 - Verschlüsselte Verbindung beim Surfen im Internet

Schutztechnologien

- PIN, Passwort, Muster
 - Basisschutz für Gerätesperre

- Biometrie
 - Fingerabdruck
 - Gesichtserkennung
- Secure Enclave / Trusted Execution
 - Eigener Sicherheitschip für Schlüssel und Biometriedaten
- App-Berechtigungen
 - Apps erhalten nur erlaubte Zugriffe
- Remote-Sperre & Löschen
 - Gerät bei Verlust aus der Ferne sperren

18. Kenntnisse über Virenschutz und Backupmöglichkeit bei mobilen Endgeräten

Virenschutz (Schutz vor Malware)

Wichtige Schutzmethoden

- Geprüfte App-Stores
 - Apps werden vor Veröffentlichung kontrolliert
 - → geringes Malware-Risiko
- System- und Sicherheitsupdates
 - Schließen bekannte Sicherheitslücken
- App-Berechtigungen
 - Nutzer legt fest, worauf Apps zugreifen dürfen
- Antiviren-Apps
 - Zusätzlicher Schutz, vor allem bei Android
- Gerätesperre (PIN/Biometrie)
 - Verhindert unbefugten Zugriff

Backup (Datensicherung)

- Backup-Arten
- Cloud-Backup
 - Speicherung im Internet (iCloud, Google Drive)
 - → automatisch, jederzeit abrufbar
- Lokales Backup
 - Speicherung auf PC oder externem Speicher
 - → unabhängig vom Internet

Mobile Endgeräte werden durch Virenschutzmaßnahmen vor Schadsoftware geschützt und durch Backups vor Datenverlust abgesichert.

19. Kenntnisse über MDM

MDM ist eine Softwarelösung zur zentralen Verwaltung, Sicherung und Überwachung mobiler Endgeräte in Unternehmen.

20. Fachbegriff Convertible

Ein Convertible ist ein 2-in-1-Gerät, das als Laptop und Tablet verwendet werden kann.

Ein Convertible hat:

- Einen Touchscreen
- Eine Tastatur, die sich umklappen oder abnehmen lässt
- So wird aus dem Laptop mit einem Handgriff ein Tablet.

21. Kenntnis der Merkmale von Mobile-Prozessoren

Mobile-Prozessoren sind SoC-Chips, die CPU, GPU, Modem und Speichersteuerung vereinen und für hohe Leistung bei geringem Stromverbrauch optimiert sind.

22. Fachbegriffe E-Ink, OLED

E-Ink ist eine elektronische Tintenanzeige, bei der Bildpunkte durch elektrisch bewegte Farbpartikel dargestellt werden. → E-Book-Reader & digitale Preisschilder

OLED ist eine Displaytechnologie, bei der jede Bildzelle selbst Licht erzeugt. → Smartphones, Tablets, Smartwatches, Fernseher

E-Ink eignet sich für stromsparende, papierähnliche Anzeigen, während OLED selbstleuchtende Pixel für brillante Farben und hohe Kontraste nutzt.

23. Fachbegriff Edge, 3G bzw. UMTS, 4G bzw. LTE, 5G

EDGE, UMTS, LTE und 5G sind Mobilfunkstandards unterschiedlicher Generationen, die sich in Geschwindigkeit und Leistungsfähigkeit unterscheiden.

Standard	Generation	Geschwindigkeit	Status
EDGE	2G	Sehr langsam	Veraltet
UMTS	3G	Mittel	Wird abgeschaltet
LTE	4G	Schnell	Standard
5G	5G	Sehr schnell	Zukunftssicher

24. Fachbegriff HSDPA

HSDPA (High Speed Downlink Packet Access) ist eine Erweiterung von UMTS (3G), die höhere Download-Geschwindigkeiten für mobiles Internet ermöglicht.

25. Fachbegriff NFC

NFC (Near Field Communication) ist eine drahtlose Kurzstrecken-Funktechnologie, die den kontaktlosen Datenaustausch über sehr kurze Distanz ermöglicht.

- Kontaktloses Bezahlen (Apple Pay, Google Pay)
- Fahrkarten und Tickets
- Zugangskarten
- Schnelles Bluetooth-Pairing

26. Fachbegriff GPS/GPS-Tracking

GPS (Global Positioning System) ist ein satellitengestütztes Ortungssystem, das die genaue Positionsbestimmung eines Geräts auf der Erde ermöglicht.

- Navigation (Google Maps)
- Fitness-Apps (Laufstrecken)
- Fahrzeugortung
- Diebstahlschutz

GPS ist ein satellitengestütztes System zur Positionsbestimmung.

GPS-Tracking ist die kontinuierliche Standortverfolgung eines Geräts mithilfe von GPS.

27. Kenntnisse über Daten-Zugriffsschutzmöglichkeiten bei Diebstahl von mobilen Endgeräten

Bei Diebstahl mobiler Geräte schützen Gerätesperre, Verschlüsselung und Fernlöschfunktionen vor unbefugtem Datenzugriff.

Ziel des Zugriffsschutzes: Verhindern, dass Unbefugte auf persönliche oder Firmendaten zugreifen und Möglichkeit, das Gerät aus der Ferne zu sperren oder zu löschen

Gerätesperre

- PIN, Passwort, Muster
- Fingerabdruck oder Gesichtserkennung
- → Erster Schutz gegen direkten Zugriff

Geräteverschlüsselung

- Alle gespeicherten Daten sind verschlüsselt
- Ohne Entsperrcode nicht lesbar

Fernzugriff bei Verlust

- Remote Lock

- Gerät aus der Ferne sperren
- Remote Wipe
 - Gerät aus der Ferne komplett löschen

(Beispiel: „Mein iPhone suchen“, „Google Find My Device“)

Cloud-Sicherung

- Daten vorher gesichert
- Verlust des Geräts bedeutet keinen Datenverlust

MDM (bei Firmengeräten)

- Zentrale Sperre oder Löschung durch IT-Abteilung
- Erzwingt Sicherheitsrichtlinien

zusätzliche Schutzmaßnahmen

- SIM-Sperre aktivieren
- Ortungsfunktion einschalten (GPS-Tracking)
- Keine automatischen Logins speichern

Vorteile

- Schutz sensibler Daten
- Missbrauch wird verhindert
- Gerät kann unbrauchbar gemacht werden

Grenzen

- Schutz wirkt nur, wenn vorher aktiviert
- Ohne Internet kein Fernzugriff möglich

Ausarbeitung-Themenkatalog

5. Benutzerendgeräte und Peripheriegeräte

5.4 Anwenderkenntnisse

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

5. Benutzerendgeräte und Peripheriegeräte.....	1
5.5 Programmiersprachen.....	1
5.5.1 Gängige Programmiersprachen und Anwendungen	Fehler! Textmarke nicht definiert.
5.5.2 Prozedurale vs. Objektorientierte Programmierung (OOP)	Fehler! Textmarke nicht definiert.
5.5.3 Fachbegriff: Implementierung.....	Fehler! Textmarke nicht definiert.
5.5.4 Fachbegriff: Compiler	Fehler! Textmarke nicht definiert.
5.5.5 Fachbegriff: Interpreter	Fehler! Textmarke nicht definiert.

Anwenderkenntnisse beschreiben die Fähigkeit einer Person, Computerprogramme und IT-Systeme zielgerichtet zur Lösung von Aufgaben einzusetzen. Es geht dabei weniger um das technische Verständnis der Programmierung, sondern um die **effiziente Bedienung** von Benutzeroberflächen, die Navigation in Dateisystemen und die Anwendung von Standardsoftware zur Bewältigung des Arbeitsalltags.

5.4.1 Tabellenkalkulations-Software (z. B. Excel, Calc)

Diese Software dient der Darstellung und Verarbeitung von Daten in einer Gitterstruktur (Zellen). Sie wird primär für Berechnungen, Analysen und grafische Auswertungen genutzt.

- **Formeln:** Sind vom Benutzer definierte mathematische Ausdrücke (z. B. $=(A1+B1)*0.2$), um manuelle Berechnungen zu automatisieren.
- **Funktionen:** Vordefinierte Rechenbefehle der Software, um komplexe Logiken einfach anzuwenden.
 - *Beispiele:* SUMME() (Addition), WENN() (logische Abfragen), SVERWEIS() (Datenrecherche).

5.4.2 Textverarbeitungs-Software (z. B. Word, Writer)

Hierbei handelt es sich um Programme zur Erstellung, Bearbeitung und Gestaltung von Schriftstücken (Briefe, Berichte, Dokumentationen).

- **Formatiermöglichkeiten:**
 - **Zeichenformatierung:** Ändern von Schriftart, Größe, Farbe oder Schriftschnitt (fett, kursiv).
 - **Absatzformatierung:** Ausrichtung (linksbündig, Blocksatz), Zeilenabstände und Aufzählungszeichen.
 - **Seitenformatierung:** Seitenränder, Hoch-/Querformat und Umbrüche.
 - **Formatvorlagen:** Die strukturierte Zuweisung von Designs (z. B. Überschrift 1), um ein einheitliches Layout und automatische Inhaltsverzeichnisse zu gewährleisten.

5.4.3 Bildbearbeitungs-Software (z. B. Photoshop, GIMP)

Diese Software wird zur Veränderung von digitalen Bildern (meist Rastergrafiken) verwendet. Typische Anwendungsgebiete sind:

- **Retusche:** Entfernen von Bildfehlern oder störenden Elementen.
- **Optimierung:** Anpassung von Kontrast, Helligkeit, Sättigung und Schärfe.

- **Compositing:** Das Zusammenführen mehrerer Bilder oder Ebenen zu einem neuen Gesamtbild.
- **Skalierung & Beschnitt:** Anpassung der Bildgröße und des Bildausschnitts für verschiedene Verwendungszwecke (Web vs. Druck).

5.4.4 Unterschiede von Dateiformaten

Die Wahl des Dateiformats entscheidet über die Kompatibilität und die Nutzungsrechte.

Formattyp	Definition	Beispiele
Offen	Der Quellcode und die Spezifikationen sind öffentlich zugänglich. Jeder kann Software dafür entwickeln.	.odt, .png, .svg
Proprietär	Das Format gehört einem Unternehmen. Nur dieses (oder Lizenznehmer) darf es vollumfänglich nutzen/ändern.	.psd (Adobe), .docx (Microsoft)
Plattformunabhängig	Diese Formate können auf nahezu jedem Betriebssystem (Windows, macOS, Linux) ohne Layoutverlust geöffnet werden.	.pdf, .html, .txt

Ausarbeitung-Themenkatalog

5. Benutzerendgeräte und Peripheriegeräte

5.5 Programmiersprachen

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

5. Benutzerendgeräte und Peripheriegeräte.....	1
5.5 Programmiersprachen.....	1
5.5.1 Gängige Programmiersprachen und Anwendungen	2
5.5.2 Prozedurale vs. Objektorientierte Programmierung (OOP)	2
5.5.3 Fachbegriff: Implementierung.....	2
5.5.4 Fachbegriff: Compiler	3
5.5.5 Fachbegriff: Interpreter	3

5.5.1 Gängige Programmiersprachen und Anwendungen

Programmiersprachen sind die Schnittstelle zwischen Mensch und Maschine. Man unterteilt sie oft nach ihrem Einsatzzweck:

- **Java:** Plattformunabhängig (läuft auf der JVM). Wird häufig für **Unternehmenssoftware**, Android-Apps und Backend-Systeme genutzt.
- **Python:** Bekannt für einfache Syntax. Marktführer in den Bereichen **Data Science**, **KI (Künstliche Intelligenz)** und Automatisierungsskripte.
- **C# (C-Sharp):** Die Standard-Sprache im **Microsoft-Ökosystem**. Hauptsächlich für Windows-Anwendungen und Spieleentwicklung (Unity Engine).
- **JavaScript:** Die Sprache des Webs. Unverzichtbar für **interaktive Webseiten** (Frontend) und mittlerweile auch im Backend (Node.js) verbreitet.
- **C / C++:** Hardwarenah und extrem schnell. Wird für **Betriebssysteme**, **Treiber** und eingebettete Systeme (z.B. Steuergeräte im Auto) verwendet.

5.5.2 Prozedurale vs. Objektorientierte Programmierung (OOP)

Der Unterschied liegt in der Herangehensweise, wie ein Problem gelöst wird:

Merkmal	Prozedurale Programmierung	Objektorientierte Programmierung (OOP)
Fokus	Ablauf (Was muss nacheinander getan werden?)	Datenobjekte (Wer interagiert mit wem?)
Struktur	Das Programm wird in kleine, logische Einheiten (Funktionen/Prozeduren) unterteilt.	Das Programm besteht aus Klassen und Objekten , die Daten und Funktionen kapseln.
Denkweise	Schritt-für-Schritt-Rezept.	Abbild der realen Welt (z.B. ein Objekt "Auto" mit Eigenschaften wie Farbe).
Beispiele	C, Pascal, COBOL.	Java, C#, C++, Python.

5.5.3 Fachbegriff: Implementierung

Unter **Implementierung** versteht man in der Informatik die **Umsetzung eines Entwurfs in fertigen Programmcode**. Es ist die Phase im Software-Lebenszyklus, in der nach der Planung (Design/Architektur) tatsächlich "in die Tasten gehauen" wird. Man überführt theoretische Algorithmen oder Logiken in eine konkrete Programmiersprache, damit sie ausführbar werden.

5.5.4 Fachbegriff: Compiler

Ein **Compiler** ist ein Übersetzungsprogramm, das den kompletten Quellcode einer Hochsprache (z.B. C++ oder Java) in einem Rutsch in **Maschinencode** (Binärcode) übersetzt.

- **Vorteil:** Das fertige Programm ist sehr schnell, da es bereits in der "Sprache des Prozessors" vorliegt.
 - **Besonderheit:** Vor dem Ausführen muss der gesamte Code fehlerfrei übersetzt worden sein. Es entsteht eine eigenständige Datei (z.B. eine .exe).
-

5.5.5 Fachbegriff: Interpreter

Ein **Interpreter** übersetzt den Quellcode nicht im Ganzen, sondern **Zeile für Zeile** direkt während der Ausführung des Programms.

- **Vorteil:** Fehler können sofort im laufenden Prozess gefunden werden; der Code ist oft plattformunabhängiger (da nur der Interpreter auf dem System passen muss).
- **Nachteil:** Da bei jedem Start erneut "übersetzt" wird, sind interpretierte Sprachen (wie Python oder PHP) tendenziell langsamer als compilierte Sprachen.

Ausarbeitung-Themenkatalog

5. Benutzerendgeräte und Peripheriegeräte

5.6 Fehleranalyse – Verwenden von Systemtools

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

5. Benutzerendgeräte und Peripheriegeräte	1
5.6 Fehleranalyse – Verwenden von Systemtools	1
5.6.1 Bedienung und Analyse des Event-Viewer (Windows)	2
5.6.2 Auffinden und Analysieren von Messages-Logs (Linux)	2
Netzwerk-Diagnosekommandos	2
5.6.3 Anwendung des Kommandos ping	2
5.6.4 Anwendung von ipconfig (Windows) / ifconfig oder ip addr (Linux)	3
5.6.5 Anwendung von tracert (Windows) / traceroute (Linux)	3
Hardware-Fehler & Troubleshooting	3
5.6.6 Analyse und Behebung von Hardware-Fehlern	3
5.6.7 Vorgangsweise bei einem Druckerdefekt	3
5.6.8 Behebung einer Netzwerkunterbrechung	4
5.6.9 Fehlersuche bei fehlender Internet-Verbindung	4
5.6.10 Feststellung von Fehlern an einzelnen Bauteilen	4

Die systematische Fehlersuche folgt meist dem **Ausschlussprinzip**. Systemtools dienen dazu, vom Anwender gemeldete Symptome in messbare Daten zu übersetzen.

- **Ziel:** Identifikation der Fehlerquelle (Hardware, Software, Konfiguration oder Netzwerk).

5.6.1 Bedienung und Analyse des Event-Viewer (Windows)

Der Event-Viewer (Ereignisanzeige) ist das zentrale Protokollierungstool von Windows.

- **Wichtige Protokolle:**
 - **Anwendung:** Fehler von installierten Programmen.
 - **System:** Probleme mit Treibern oder Windows-Diensten.
 - **Sicherheit:** Anmeldeversuche und Berechtigungen.
- **Kategorien:** Informationen, Warnungen und **Fehler/Kritisch** (diese sind bei der Analyse entscheidend).

5.6.2 Auffinden und Analysieren von Messages-Logs (Linux)

Unter Linux werden fast alle Systemereignisse in Textdateien im Verzeichnis `/var/log/` gespeichert.

- **Wichtige Dateien:**
 - `/var/log/syslog` oder `/var/log/messages`: Allgemeine Systemmeldungen.
 - `/var/log/auth.log`: Authentifizierungsversuche.
 - `/var/log/dmesg`: Kernel-Meldungen (wichtig für Hardware-Erkennung).
- **Tools:** `tail -f /var/log/syslog` (Live-Überwachung) oder `journalctl` bei Systemd-Systemen.

Netzwerk-Diagnosekommandos

5.6.3 Anwendung des Kommandos ping

Prüft die Erreichbarkeit eines Hosts im Netzwerk mittels ICMP-Echo-Requests.

- **Windows:** `ping [IP/Hostname]` (sendet standardmäßig 4 Pakete).
- **Linux:** `ping [IP/Hostname]` (läuft endlos, bis Abbruch mit Strg+C).
- **Parameter:**
 - `-t` (Windows): Endloser Ping.
 - `-n [Anzahl]` (Windows) / `-c [Anzahl]` (Linux): Festlegen der Paketanzahl.

5.6.4 Anwendung von ipconfig (Windows) / ifconfig oder ip addr (Linux)

Dient der Anzeige und Konfiguration der Netzwerkschnittstellen.

- **Windows ipconfig:**
 - /all: Zeigt detaillierte Infos (MAC-Adresse, DNS, DHCP).
 - /release & /renew: Erneuert die DHCP-Lease.
- **Linux ifconfig / ip a:**
 - Zeigt IP-Adressen, Subnetzmasken und den Status der Interfaces (UP/DOWN).

5.6.5 Anwendung von tracert (Windows) / traceroute (Linux)

Verfolgt den Weg eines Datenpakets über verschiedene Router (Hops) zum Ziel.

- **Nutzen:** Feststellen, an welcher Stelle in einer langen Kette (z. B. zum Internet-Provider) die Verbindung unterbrochen wird.

Hardware-Fehler & Troubleshooting

5.6.6 Analyse und Behebung von Hardware-Fehlern

Hier wird methodisch vorgegangen:

1. **Sichtprüfung:** Kabel locker? Brandgeruch? Lüfter dreht nicht?
2. **POST (Power-On Self-Test):** Achten auf Beep-Codes des Mainboards.
3. **Minimal-Konfiguration:** Nur CPU, ein RAM-Riegel und Netzteil anschließen, um defekte Peripherie auszuschließen.

5.6.7 Vorgangsweise bei einem Druckerdefekt

1. **Hardware:** Papierstau prüfen, Toner/Tintenstand kontrollieren, Verbindung (USB/LAN/WLAN) checken.
2. **Software:** Druckerwarteschlange (Spooler) prüfen/neustarten, Treiber aktualisieren.
3. **Test:** Testseite direkt am Gerät drucken (Hardware-Check) vs. Testseite über Windows (Treiber-Check).

5.6.8 Behebung einer Netzwerkunterbrechung

- **Schicht 1 (Physical):** Link-LEDs an Netzwerkkarte und Switch prüfen, Kabel tauschen.
- **Schicht 2/3 (Logisch):** Prüfen, ob eine IP-Adresse vorhanden ist (DHCP?) und das Standard-Gateway (Router) anpingen.

5.6.9 Fehlersuche bei fehlender Internet-Verbindung

1. **Lokal:** Ping auf den eigenen Router.
2. **Extern:** Ping auf eine öffentliche IP (z. B. 8.8.8.8). Wenn das geht, aber Webseiten nicht laden -> **DNS-Fehler**.
3. **DNS-Check:** Ping auf google.com. Schlägt dies fehl, DNS-Server prüfen.

5.6.10 Feststellung von Fehlern an einzelnen Bauteilen

- **RAM:** Test mit Tools wie MemTest86.
- **Festplatte/SSD:** Auslesen der **S.M.A.R.T.-Werte** (z. B. mit CrystalDiskInfo).
- **Netzteil:** Spannungsprüfung mit Multimeter oder Netzteiltester.
- **CPU/GPU:** Stresstests (z. B. Prime95), um thermische Probleme zu finden.

Themenkatalog-Ausarbeitung

6. Netzwerke

6.1 Netzwerktechnik

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

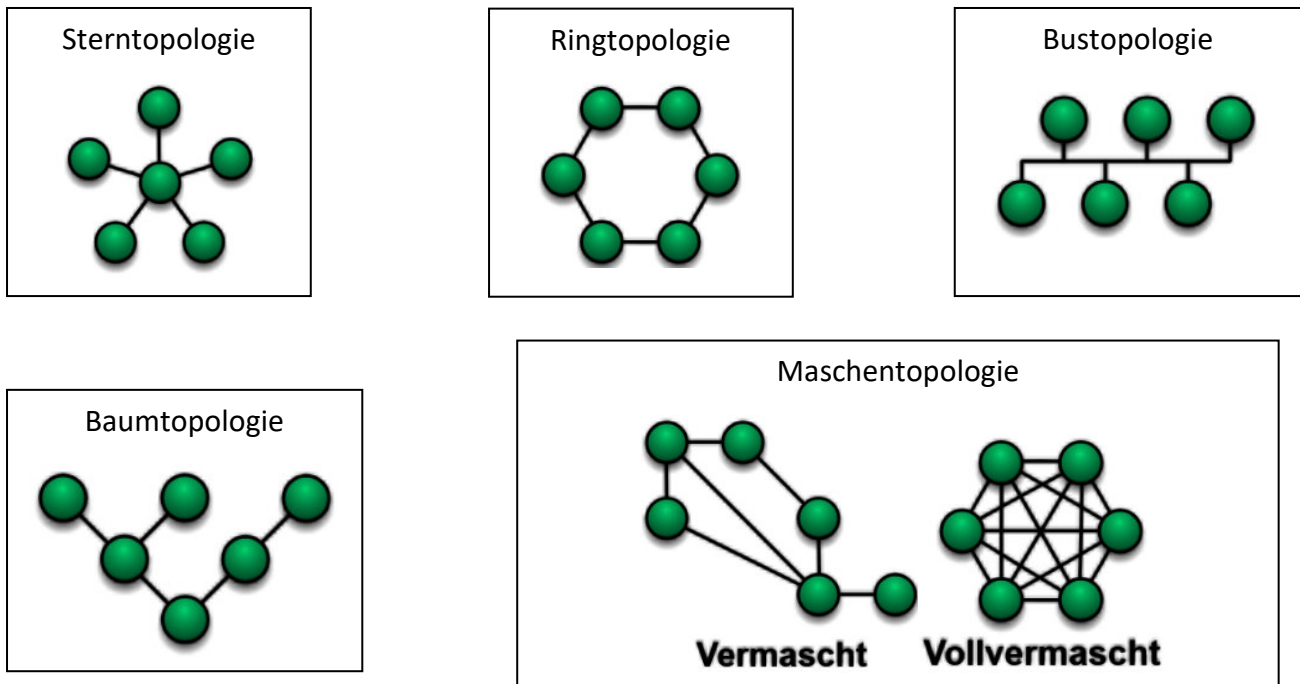
Inhalt

6. Netzwerke	1
6.1 Netzwerktechnik	1
7. Fachbegriff Netzwerk	2
7.1.1 Kenntnis der Netzwerktopologien wie Stern, Ring, Bus, Baum, Masche	2
8. Kenntnis der Vor- und Nachteile der jeweils eingesetzten Netzwerktopologien	2
9. Funktionsprinzip eines Routers, Switches	2
10. Kenntnis des Fachbegriffes Subnetzmaske und deren technischen Zusammenhänge	2
11. Kenntnisse über das OSI-Modell	3
12. Einordnung von Protokollen in das OSI-Modell	4
13. Einordnung von Netzwerk- und Hardwaregeräten in das OSI-Modell	4
14. Kenntnisse über die Protokollfamilie TCP/IP	4
15. Fachbegriff IPv4-Adresse und deren Aufbau	4
16. Kenntnisse über IPv6-Adressierung	4
17. Unterscheidung von public/private IP-Adressen	4
18. Kenntnis der privaten IP-Adress-Bereiche	5
19. Fachbegriff MAC-Adresse und deren Aufbau	5
20. Fachbegriff Ethernet	5
21. Fachbegriff Xdsl	5
22. Unterscheidung der Fachbegriffe Upload, Download	5
23. Fachbegriff WLAN	5
24. Fachbegriff Access-Point	5

6.1.1 Fachbegriff Netzwerk

Ein Netzwerk ist ein Zusammenschluss mehrerer Geräte, um Daten und Ressourcen wie Drucker, Server oder Internet gemeinsam zu nutzen.

6.1.2 Kenntnis der Netzwerktopologien wie Stern, Ring, Bus, Baum, Masche



6.1.3 Kenntnis der Vor- und Nachteile der jeweils eingesetzten Netzwerktopologien

- **Stern:** leicht erweiterbar aber zentraler Ausfallpunkt
- **Bus:** wenig Verkabelung, aber störanfällig
- **Ring:** geregelter Zugriff, aber Ausfall eines Gerätes stört das Netz
- **Baum:** gut skalierbar, aber komplex
- **Masche:** sehr ausfallsicher, aber teuer und aufwendig.

6.1.4 Funktionsprinzip eines Routers, Switches

Router verbinden unterschiedliche Netzwerke und leiten Daten anhand von IP-Adressen weiter (Layer3)

Switches verbinden Geräte innerhalb eines Netzwerkes über MAC-Adressen (Layer2)

6.1.5 Kenntnis des Fachbegriffes Subnetzmaske und deren technischen Zusammenhänge

Eine Subnetzmaske ist eine 32-bit-Zahl, die eine IP-Adresse in einen Netzwerkanteil und einen Hostanteil teilt, um größere Netzwerke in kleinere, besser verwaltbare Segmente zu unterteilen.

6.1.6 Kenntnisse über das OSI-Modell

Das OSI-Modell ist ein konzeptionelles Framework, das Netzwirkommunikation in sieben logische Schichten einteilt.

7 Anwendungsschicht (application) HTTP, HTTPS, FTP, SMTP, DNS, DHCP

Schicht 7 ist die Schnittstelle zwischen Anwendung und Netzwerk.

6 Darstellungsschicht (presentation)

Schicht 6 kümmert sich um Datenformate, Verschlüsselung und Kodierung.

5 Sitzungsschicht(session)

Schicht 5 verwaltet Sitzungen zwischen Kommunikationspartnern.

4 Transportschicht(transport) TCP (zuverlässig), UDP (schnell)

Schicht 4 regelt den Transport zwischen Anwendungen über Ports.

3 Vermittlungsschicht(network) IP, ICMP Router

Schicht 3 ist für logische Adressierung und Routing zuständig.

2 Sicherungsschicht(data-link) Ethernet (IEEE 802.3), ARP Switch, Bridge

Schicht 2 arbeitet mit MAC-Adressen und organisiert den Datenverkehr im LAN.

1 Bitübertragungsschicht(physical) überträgt Bits (0,1) Hub, Repeater, Netzwirkkabel

Schicht 1 ist für die physische Übertragung von Bits zuständig.

6.1.7 Einordnung von Protokollen in das OSI-Modell

Wie werden Protokolle im OSI-Modell eingeordnet?

Protokolle sind bestimmten Schichten zugeordnet, z. B. Ethernet (Layer 2), IP (Layer 3), TCP/UDP (Layer 4), HTTP (Layer 7).

6.1.8 Einordnung von Netzwerk- und Hardwaregeräten in das OSI-Modell

Ordnen Sie Netzwerkgeräte dem OSI-Modell zu.

- Hub: Layer 1
- Switch: Layer 2
- Router: Layer 3
- Firewall: Layer 3–7 (abhängig vom Typ)

6.1.9 Kenntnisse über die Protokollfamilie TCP/IP

Was versteht man unter der TCP/IP-Protokollfamilie?

TCP/IP ist eine Protokollsammlung für die Datenübertragung im Internet und bildet die Grundlage moderner Netzwerke.

6.1.10 Fachbegriff IPv4-Adresse und deren Aufbau

Was ist eine IPv4-Adresse und wie ist sie aufgebaut?

Eine IPv4-Adresse besteht aus 32 Bit, dargestellt in vier Dezimalzahlen zwischen 0 und 255, z. B. 192.168.1.1.

6.1.11 Kenntnisse über IPv6-Adressierung

Was ist IPv6 und warum wird es eingesetzt?

IPv6 ist der Nachfolger von IPv4, nutzt 128 Bit und bietet einen deutlich größeren Adressraum.

6.1.12 Unterscheidung von public/private IP-Adressen

Public IPs sind weltweit eindeutig und im Internet erreichbar, private IPs nur innerhalb lokaler Netzwerke.

6.1.13 Kenntnis der privaten IP-Adress-Bereiche

Welche privaten IP-Adressbereiche kennen Sie?

Klasse A 10.0.0.0 – 10.255.255.255

Klasse B 172.16.0.0 – 172.31.255.255

Klasse C 192.168.0.0 – 192.168.255.255

6.1.14 Fachbegriff MAC-Adresse und deren Aufbau

Was ist eine MAC-Adresse und wie ist sie aufgebaut?

Die MAC-Adresse ist eine eindeutige Hardwareadresse mit 48 Bit, dargestellt in hexadezimaler Form.

6.1.15 Fachbegriff Ethernet

Was versteht man unter Ethernet?

Ethernet ist der Standard für kabelgebundene lokale Netzwerke (LAN) gemäß IEEE 802.3.

6.1.16 Fachbegriff Xdsl

Was bedeutet xDSL?

xDSL bezeichnet verschiedene DSL-Technologien zur Datenübertragung über Kupfer-Telefonleitungen.

6.1.17 Unterscheidung der Fachbegriffe Upload, Download

Upload bezeichnet das Senden von Daten, Download das Empfangen von Daten.

6.1.18 Fachbegriff WLAN

Was ist WLAN?

WLAN ist ein drahtloses lokales Netzwerk auf Basis von Funktechnologie gemäß IEEE 802.11.

6.1.19 Fachbegriff Access-Point

Was ist ein Access Point?

Ein Access Point verbindet drahtlose Endgeräte mit einem kabelgebundenen Netzwerk.

Ausarbeitung-Themenkatalog

6. Netzwerke

6.1 Netzwerkdienste

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

6. Netzwerke	1
6.1 Netzwerkdienste	1
6.1.1 Aufbau eines Active-Directorys	4
Domäne	4
Domänencontroller (DC)	4
Objekte	5
Organisationseinheiten (OU)	5
Gruppen.....	5
Gruppenrichtlinien (GPO)	5
DNS	5
Gesamtstruktur (Forest).....	5
Vertrauensstellungen	6
6.1.2 Funktionsprinzip eines Domain-Controllers	6
Speicherung der AD-Datenbank.....	6
Anmeldung	6
Autorisierung.....	6
Gruppenrichtlinien-Verteilung	7
DNS-Registrierung und Namensauflösung	7
Replikation zwischen DCs	7
6.1.3 Kenntnisse über den Netzwerkdienst DHCP	7
Funktionsprinzip (DORA-Ablauf)	7
Lease-Prinzip.....	8
DHCP-Reservierung.....	8
DHCP-Relay	8
6.1.4 Funktionsprinzip eines Proxy-Servers	8

Ein Proxy-Server arbeitet als Zwischenstation auf Anwendungsebene (OSI-Schicht 7).	9
Er nimmt Client-Anfragen entgegen, verarbeitet sie selbstständig und stellt im Auftrag des Clients eine neue Anfrage an den Zielservers.	9
Der Client kommuniziert also nicht direkt mit dem Zielservers.	9
6.1.5 Funktionsprinzip eines Webservers	9
6.1.6 Kenntnis des DNS-Dienstes und dessen hierarchischen Aufbaues	9
Ebenen erklärt	9
DNS-Server-Typen	10
6.1.7 Fachbegriffe Domain, Sub-Domain und Top-Level-Domain.	10
Domain	10
Top-Level-Domain (TLD)	10
Sub-Domain	10
6.1.8 Kenntnis der Web-Protokolle HTTP und HTTPS	11
HTTP (Hypertext Transfer Protocol)	11
HTTPS (HTTP Secure)	11
6.1.9 Funktionsprinzip eines Mail-Servers	11
Beteiligte Protokolle	11
6.1.10 Kenntnis der Mailprotokolle POP3/POP3S, IMAP/IMAPS und SMTP/SMTPS	12
SMTP / SMTPS (Simple Mail Transfer Protocol)	12
POP3 / POP3S (Post Office Protocol)	12
IMAP / IMAPS (Internet Message Access Protocol)	13
6.1.11 Kenntnisse über FTP/FTPS	13
FTP (File Transfer Protocol)	13
FTPS (FTP Secure)	13
6.1.12 Kenntnisse über SSL	14
Digitale Zertifikate	15
6.1.13 Fachbegriff Cloud-Computing und Beispiele für marktbekannte Cloud-Dienste	15
6.1.14 Kenntnisse über Private/Public/Hybrid Cloud	16
Private Cloud	16
Public Cloud	16
Hybrid Cloud	16
6.1.15 Fachbegriffe IaaS, PaaS, SaaS	17
IaaS – Infrastructure as a Service	17
PaaS – Platform as a Service	17

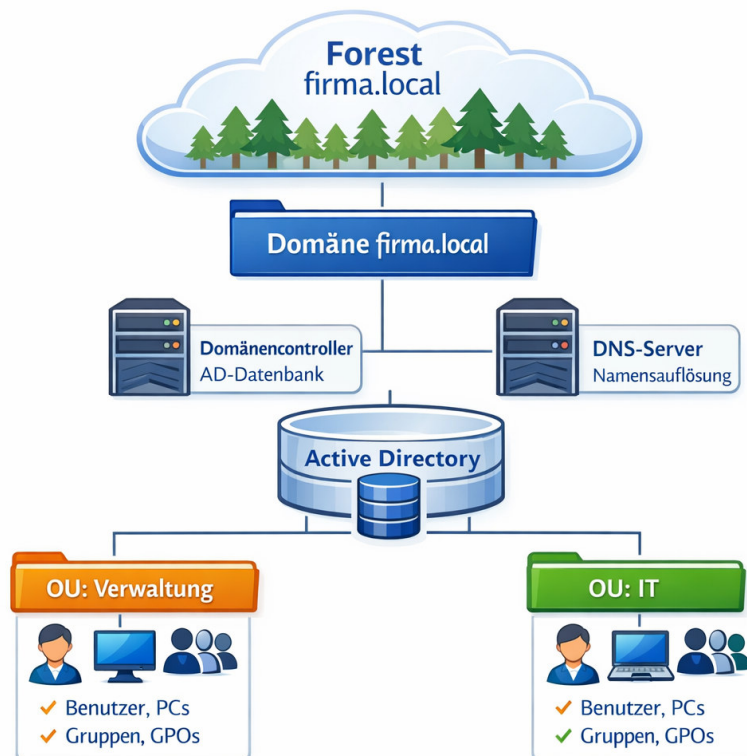
SaaS – Software as a Service	17
6.1.16 Kriterien und Voraussetzungen für den Einsatz von Cloud-Diensten	18

6.1.1 Aufbau eines Active-Directorys

Active Directory ist ein zentraler Verzeichnisdienst von Microsoft zur Verwaltung von Benutzern, Gruppen, Computern, und Gruppenrichtlinien (GPOs).

Zu den logischen Bestandteilen zählen Domänen, Organisationseinheiten (OU), Benutzer, Gruppen, Computer und Gruppenrichtlinien (GPO's)

Forest → Domäne → OU → Objekte



Domäne

Die Domäne ist die grundlegende logische Einheit.

Alle Objekte wie Benutzer oder Computer gehören zu einer Domäne (Bsp.: firma.local).

Domänencontroller (DC)

Ein Domänencontroller ist ein Server, der das Active Directory bereitstellt.

Er speichert die AD-Datenbank und übernimmt:

- Benutzeranmeldung
- Rechteprüfung
- Verzeichnisabfragen

Mehrer DCs sorgen für Ausfallsicherheit und Replikation.

Objekte

Im AD werden alle Ressourcen als Objekte gespeichert, z.B.:

- Benutzerkonten
- Computer
- Gruppen
- Drucker
- Freigaben

Jedes Objekt besitzt Attribute (z.B. Name, Passwort, Beschreibung).

Organisationseinheiten (OU)

OUs sind Container zur Strukturierung von Objekten.

Sie ermöglichen:

- Übersichtliche Verwaltung
- Gezielte Gruppenrichtlinien (GPOs)

Beispiel:

OU = „Abteilung_IT“, darin Benutzer und Computer der IT.

Gruppen

Gruppen bündeln Benutzer oder Computer, um Berechtigungen einfacher zuzuweisen.

Typisch:

- Sicherheitsgruppen für Rechte
- Verteilergruppen für E-Mail

Gruppenrichtlinien (GPO)

GPOs legen zentrale Regeln fest, z.B.:

- Passwortregeln
- Desktop-Einstellungen
- Softwareverteilung

Sie werden auf OUs oder Domänen verknüpft.

DNS

AD benötigt DNS zur Namensauflösung.

Domäne und DNS-Zone sind eng gekoppelt.

Gesamtstruktur (Forest)

Mehrer Domänen können eine Gesamtstruktur bilden.

Der Forest ist die oberste AD-Strukturebene.

Vertrauensstellungen

Zwischen Domänen oder Forests können Trusts eingerichtet werden, um gegenseitigen Zugriff zu erlauben.

6.1.2 Funktionsprinzip eines Domain-Controllers

Ein Domain-Controller ist der zentrale Authentifizierungs- und Verwaltungsserver einer Windows-Domäne.

Er stellt das Active Directory bereit und entscheidet, wer im Netzwerk rein darf und was erlaubt ist.

Der Domain-Controller verwaltet Identitäten, prüft Anmeldungen, vergibt Berechtigungen und verteilt Richtlinien im Netzwerk.

Speicherung der AD-Datenbank

Der DC speichert die Active-Directory-Datenbank.

Darin stehen alle Objekte:

- Benutzerkonten
- Computer
- Gruppen
- Rechte
- Richtlinien

Anmeldung

Wenn sich ein Benutzer anmeldet:

1. Client sendet Anmeldeanfrage an den DC
2. DC prüft Benutzernamen und Passwort
3. DC bestätigt Identität
4. DC gibt ein Zugriffsticket aus

→ Danach darf der Benutzer Ressourcen nutzen.

Autorisierung

Nach der Anmeldung prüft der DC:

- Zu welchen Gruppen gehört der Benutzer?
- Welche Berechtigungen hat er?

Er entscheidet also, was der Benutzer im Netzwerk tun darf

Gruppenrichtlinien-Verteilung

Der DC verteilt Gruppenrichtlinien (GPOs) an Clients:

- Sicherheitseinstellungen
- Softwareinstallation
- Desktop-Vorgaben

Beim Start und bei der Anmeldung werden diese automatisch angewendet.

DNS-Registrierung und Namensauflösung

Der DC registriert sich im DNS, damit Clients ihn finden können.

Ohne DNS kein AD – deshalb laufen DC und DNS fast immer zusammen.

Replikation zwischen DCs

Gibt es mehrere DCs:

- Änderungen werden automatisch synchronisiert.
- Sorgt für Ausfallsicherheit
- Kein Single Point of Failure

6.1.3 Kenntnisse über den Netzwerkdienst DHCP

DHCP = Dynamic Host Configuration Protocol

Ein Netzwerkdienst zur automatischen Vergabe von IP-Konfigurationen an Clients

Aufgaben von DHCP

Ein DHCP-Server vergibt an Clients:

- IP-Adresse
- Subnetzmaske
- Standardgateway
- DNS-Server
- Weitere Netzparameter

Der Client ist danach sofort kommunikationsfähig.

Funktionsprinzip (DORA-Ablauf)

1. Discover

Client sendet Broadcast: „Gibt es einen DHCP-Server?“

2. Offer

DHCP-Server bietet eine freie IP-Adresse an.

3. Request

Client fordert diese Adresse an.

4. Acknowledge

Server bestätigt die Vergabe.

DORA



Lease-Prinzip

IP-Adressen werden zeitlich befristet vergeben (Lease).

Nach Ablauf muss der Client erneuern, sonst wird die Adresse wieder frei.

DHCP-Reservierung

Bestimmte Geräte (z.B. Drucker, Server) bekommen immer dieselbe IP – anhand der MAC-Adresse.

DHCP-Relay

Wenn sich DHCP-Server in einem anderen Netzwerk befindet, leitet ein Relay-Agent die Anfragen weiter.

6.1.4 Funktionsprinzip eines Proxy-Servers

- Ein Proxy-Server arbeitet als Zwischenstation auf Anwendungsebene (OSI-Schicht 7).
- Er nimmt Client-Anfragen entgegen, verarbeitet sie selbstständig und stellt im Auftrag des Clients eine neue Anfrage an den Zielservers.
- Der Client kommuniziert also nicht direkt mit dem Zielservers.

6.1.5 Funktionsprinzip eines Webservers

Ein Webserver ist ein Serverdienst, der über HTTP/HTTPS Anfragen von Clients entgegennimmt, die angeforderten Webseiten oder Webinhalte verarbeitet und als Antwort an den Client zurücksendet. Er kann statische Dateien direkt ausliefern oder dynamische Inhalte durch Serverprogramme erzeugen.

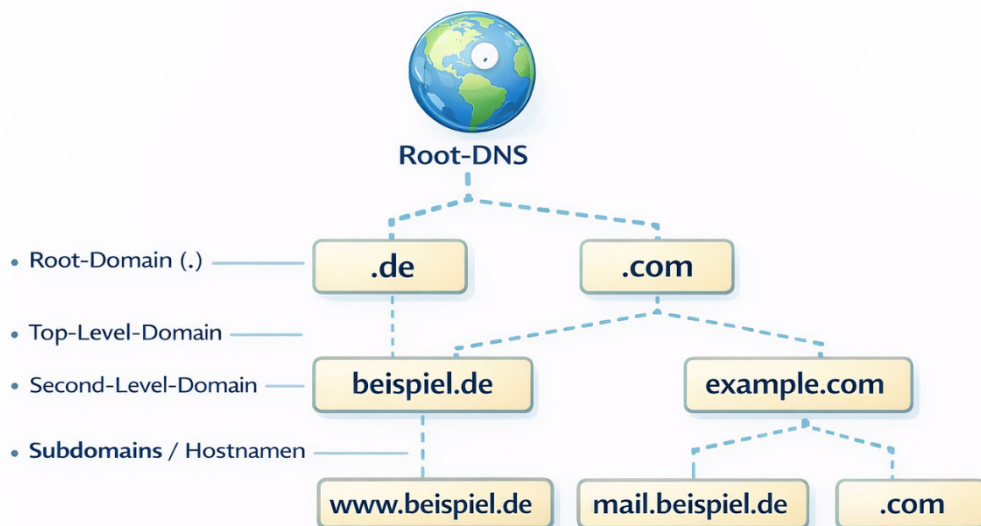
6.1.6 Kenntnis des DNS-Dienstes und dessen hierarchischen Aufbaues

DNS (Domain Name System) ist der Namensdienst des Internets.

Er übersetzt lesbare Domainnamen (z.B. www.beispiel.de) in IP-Adressen (z.B. 93.183.216.34).

Ohne DNS müsste man sich IP-Adressen merken.

Hierarchischer Aufbau des DNS



Ebenen erklärt

1. Root-Domain (.)

Oberste Ebene, verwaltet Root-Server weltweit.

2. Top-Level-Domain (TLD)

z.B. .de, .com, .org

3. Second-Level-Domain

z.B. beispiel.de

4. Subdomains / Hostnamen

z.B. www.beispiel.de, mail.beispiel.de

DNS-Server-Typen

- Root-Server → kennen TLD-Server
- TLD-Server → kennen zuständige autoritative Server
- Autoritativer DNS-Server → liefert finale IP
- Lokaler DNS-Resolver → fragt im Auftrag des Clients

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

Domain

Eine Domain ist ein eindeutig benannter Bereich im DNS, der eine Organisation oder einen Dienst im Internet repräsentiert.

Beispiel: beispiel.de

Top-Level-Domain (TLD)

Die Top-Level-Domain ist die höchste Ebene im Domainnamen.

Sie steht ganz rechts und gibt oft Länder- oder Organisationszugehörigkeit an.

Beispiele: .de, .com, .org, .net

Sub-Domain

Eine Sub-Domain ist eine Untergliederung einer Domain.

Sie dient zur Strukturierung verschiedener Dienste oder Bereiche.

Beispiel: www.beispiel.de oder mail.beispiel.de

6.1.8 Kenntnis der Web-Protokolle HTTP und HTTPS

HTTP (Hypertext Transfer Protocol)

HTTP ist das Standard-Protokoll zur Übertragung von Webseiten im Internet.

Es regelt die Kommunikation zwischen Browser (Client) und Webserver.

HTTP überträgt Webseiten – HTTPS überträgt sie sicher verschlüsselt

Eigenschaften:

- Arbeitet auf OSI-Schicht 7 (Application Layer)
- Überträgt Webseiten und Webdaten
- **Standard-Port: 80**
- Daten werden unverschlüsselt übertragen

HTTPS (HTTP Secure)

HTTPS ist die verschlüsselte Erweiterung von HTTP.

Es nutzt zusätzlich TLS/SSL, um Daten sicher zu übertragen.

Zusätzliche Eigenschaften:

- Verschlüsselte Verbindung
- Schutz vor Abhören und Manipulation
- Identitätsprüfung des Webserver durch Zertifikate
- **Standard-Port: 443**

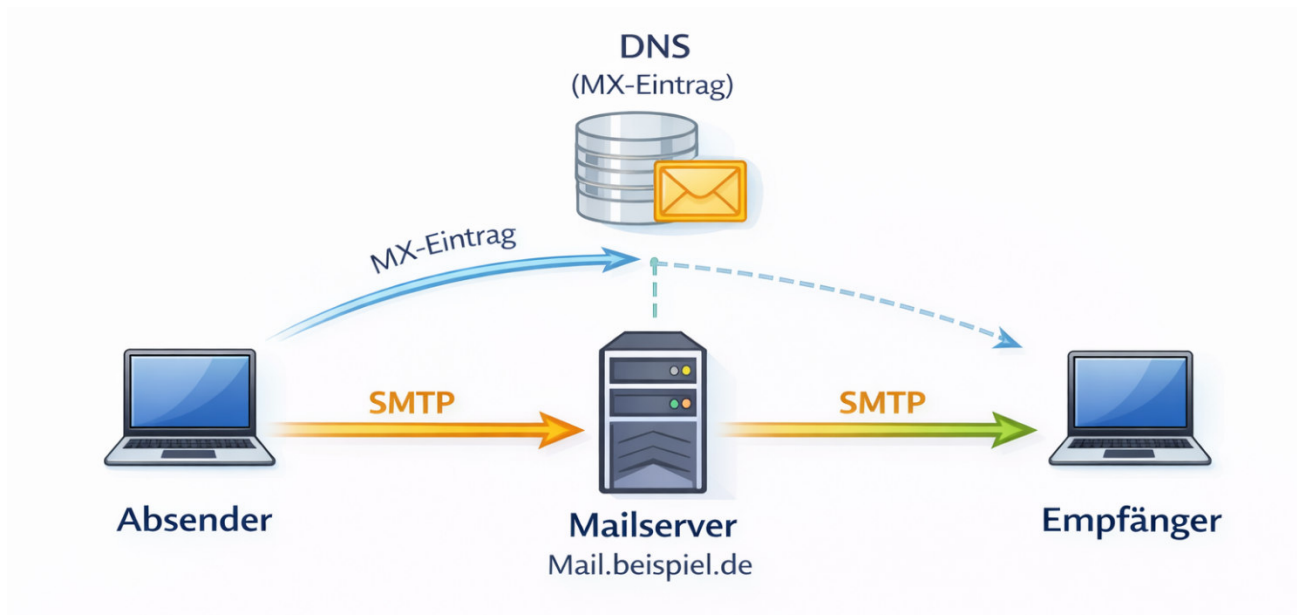
6.1.9 Funktionsprinzip eines Mail-Servers

Ein Mail-Server ist ein Serverdienst, der E-Mails versendet, empfängt, speichert und an Clients bereitstellt.

Er arbeitet mit mehreren spezialisierten Protokollen zusammen.

Beteiligte Protokolle

- SMTP – zum Senden von E-Mails
- IMAP oder POP3 – zum Abrufen von E-Mails
- DNS (MX-Eintrag) – zum Finden des zuständigen Mail-Servers



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

SMTP / SMTPS (Simple Mail Transfer Protocol)

Aufgabe: Versand von E-Mails

- Überträgt E-Mails vom Client zum Mailserver
- Überträgt E-Mails zwischen Mailservern
- SMTP: unverschlüsselt
- SMTPS: verschlüsselt per TLS/SSL

Ports:

- SMTP: 25 / 587
- SMTPS: 465

POP3 / POP3S (Post Office Protocol)

Aufgabe: Abrufen von E-Mails

- Lädt E-Mails vom Server auf den Client herunter
- Mails werden meist auf dem Client gespeichert
- POP3: unverschlüsselt
- POP3S: verschlüsselt

Ports:

- POP3: 110
- POP3S: 995

IMAP / IMAPS (Internet Message Access Protocol)

Aufgabe: Synchrones Arbeiten mit E-Mails

- E-Mails bleiben auf dem Server
- Mehrere Geräte können gleichzeitig zugreifen
- Ordnerstrukturen werden synchron gehalten
- IMAP: unverschlüsselt
- IMAPS: verschlüsselt

Ports:

- IMAP: 143
- IMAPS: 993

SMTP sendet, POP3 holt ab, IMAP synchronisiert – die „S“-Versionen verschlüsseln.

6.1.11 Kenntnisse über FTP/FTPS

FTP (File Transfer Protocol)

FTP ist ein Netzwerkprotokoll zur Übertragung von Dateien zwischen Client und Server.

Aufgaben:

- Hochladen (Upload) von Dateien
- Herunterladen (Download) von Dateien
- Verwalten von Dateien auf einem Server

Eigenschaften:

- Arbeitet auf OSI-Schicht 7
- Benötigt getrennte Verbindungen für Steuerung und Daten
- Standard-Port: 21
- Überträgt Daten unverschlüsselt

FTPS (FTP Secure)

FTPS ist die verschlüsselte Erweiterung von FTP.

Es nutzt TLS/SSL, um Benutzeranmeldung und Daten sicher zu übertragen.

Eigenschaften zusätzlich:

- Verschlüsselte Verbindung
- Schutz vor Abhören und Manipulation

FTP / FTPS



6.1.12 Kenntnisse über SSL

SSL ist ein Sicherheitsprotokoll zur Verschlüsselung von Netzwerkverbindungen.

Heute wird technisch meist TLS (Transport Layer Security) verwendet – der Begriff SSL wird aber weiterhin umgangssprachlich genutzt.

Aufgabe von SSL / TLS

- Verschlüsselung der Datenübertragung
- Schutz vor Abhören
- Schutz vor Manipulation
- Authentifizierung des Kommunikationspartners

Wo wird SSL eingesetzt?

- HTTPS (sichere Webseiten)
- SMTPS, IMAPS, POP3S (sichere E-Mail)
- FTPS (sicherer Dateitransfer)

Client verbindet sich mit Server

Server sendet Zertifikat mit öffentlichem Schlüssel

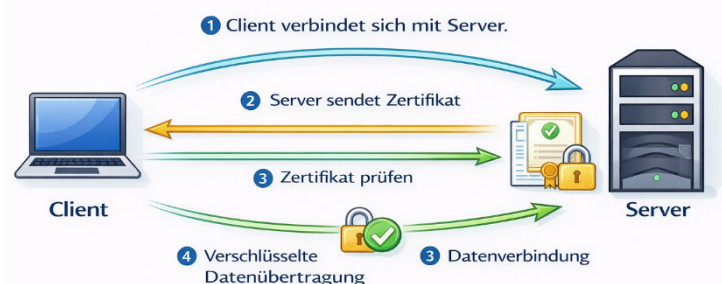
Client prüft Zertifikat

Verschlüsselter Sitzungsschlüssel wird ausgehandelt

Danach erfolgt verschlüsselte Datenübertragung

→ Dieser Ablauf heißt **TLS-Handshake**

Funktionsprinzip von SSL / TLS (vereinfacht)



Digitale Zertifikate

- Bestätigen die Identität des Servers
- Werden von Zertifizierungsstellen (CA) ausgestellt
- Verhindern Man-in-the-Middle-Angriffe

SSL/TLS verschlüsselt Verbindungen und bestätigt die Identität des Kommunikationspartners.

6.1.13 Fachbegriff Cloud-Computing und Beispiele für marktbekannte Cloud-Dienste

Cloud-Computing bezeichnet die Bereitstellung von IT-Ressourcen wie Server, Speicher, Anwendungen und Dienste über das Internet.

Statt eigene Hardware zu betreiben, werden Ressourcen nach Bedarf aus der Cloud gemietet.

Kerneigenschaften

- Nutzung über das Internet
- Skalierbar nach Bedarf
- Keine eigene Hardware nötig
- Abrechnung nach Nutzung
- Ortsunabhängiger Zugriff

Service-Modelle

- IaaS (Infrastructure as a Service)

Virtuelle Server und Speicher

Beispiel: Virtuelle Maschinen

- PaaS (Platform as a Service)

Entwicklungsplattformen

Beispiel: Web-App-Hosting

- SaaS (Software as a Service)

Fertige Anwendungen im Browser

Beispiel: Online-Office

Marktbekannte Cloud-Dienste

- Infrastruktur / Plattform:
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Anwendungsdienste (SaaS):

- Microsoft Office 365 / OneDrive
- Google Drive / Gmail
- Dropbox
- iCloud

6.1.14 Kenntnisse über Private/Public/Hybrid Cloud

Private Cloud

Eine Private Cloud ist eine Cloud-Umgebung, die nur einer Organisation gehört und von ihr betrieben oder exklusiv gemietet wird.

Eigenschaften

- Volle Kontrolle über Daten
- Hohe Sicherheit
- Betrieb im eigenen Rechenzentrum oder bei Dienstleister
- Höhere Kosten

Beispiel

Unternehmensinterne Cloud-Infrastruktur

Public Cloud

Eine Public Cloud wird von einem externen Anbieter betrieben und von vielen Kunden gemeinsam genutzt.

Eigenschaften

- Günstig und flexibel
- Keine eigene Hardware nötig
- Weltweit verfügbar
- Weniger direkte Kontrolle

Beispiele

AWS, Microsoft Azure, Google Cloud

Hybrid Cloud

Eine Hybrid Cloud kombiniert Private und Public Cloud.

Eigenschaften

- Sensible Daten bleiben in der Private Cloud
- Flexible Dienste aus der Public Cloud
- Gute Balance aus Sicherheit und Skalierbarkeit

Beispiel

Unternehmen speichert Kundendaten intern, nutzt Cloud für Web-Anwendungen

6.1.15 Fachbegriffe IaaS, PaaS, SaaS

IaaS – Infrastructure as a Service

■ Bereitstellung von virtueller Infrastruktur über das Internet.

Der Anbieter stellt

- Virtuelle Server
- Speicher
- Netzwerke

Der Kunde verwaltet

- Betriebssystem
- Anwendungen
- Daten

Beispiel

Amazon AWS EC2, Microsoft Azure VM

PaaS – Platform as a Service

■ Bereitstellung einer kompletten Entwicklungsplattform.

Der Anbieter stellt

- Betriebssystem
- Laufzeitumgebungen
- Datenbanken
- Entwicklungswerkzeuge

Der Kunde verwaltet

- Eigene Anwendungen
- Daten

Beispiel

Microsoft Azure App Service, Google App Engine

SaaS – Software as a Service

■ Bereitstellung fertiger Anwendungen über das Internet.

Der Anbieter stellt

- Anwendung
- Server
- Updates
- Wartung

Der Kunde verwaltet

- Nur Benutzerdaten und Einstellungen

Beispiel

Microsoft 365, Google Workspace, Dropbox

6.1.16 Kriterien und Voraussetzungen für den Einsatz von Cloud-Diensten

Cloud-Einsatz erfordert Technik, Sicherheit, Datenschutz, Wirtschaftlichkeit und verlässliche Anbieter.

Technische Voraussetzungen

- Stabile Internetverbindung
- Ausreichende Bandbreite
- Geeignete Endgeräte (PC, Tablet, Smartphone)
- Aktuelle Betriebssysteme und Browser

Sicherheitsanforderungen

- Verschlüsselte Datenübertragung (z. B. TLS)
- Sichere Authentifizierung
- Zugriffskontrollen und Rechtekonzepte
- Backup- und Wiederherstellungsstrategien

Datenschutz und Recht

- Einhaltung der DSGVO
- Speicherort der Daten (Rechenzentrum in EU?)
- Vertragliche Regelungen zur Datenverarbeitung

Wirtschaftliche Kriterien

- Kosten-Nutzen-Analyse
- Abrechnung nach Nutzung
- Einsparung eigener Hardware

Verfügbarkeit und Zuverlässigkeit

- Garantierte Service Level Agreements (SLA)
- Redundante Systeme

- Notfall- und Ausfallkonzepte

Skalierbarkeit

- Ressourcen flexibel erweiterbar
- Anpassung an Lastspitzen

Anbieterbewertung

- Reputation des Cloud-Anbieters
- Support und Wartung
- Zertifizierungen und Sicherheitsstandards

Ausarbeitung-Themenkatalog

6. Netzwerke

6.3 IT-Security und Betriebssicherheit

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

6. Netzwerke	1
6.3 IT-Security und Betriebssicherheit	1
6.3.1 Kenntnisse über Gefahren von Viren, Würmern, Trojanern, Spyware, Hackern, Phishing ..	3
6.3.2 Fachbegriff Zero-Day-Exploit	4
6.3.3 Kenntnisse über Einschränkungsmöglichkeiten bei Benutzerkonten	4
6.3.4 Fachbegriff Multifaktor-Authentifizierung	4
6.3.5 Kenntnis der Sicherheits-Unterschiede zw. Hardware- und Software-Firewall.....	4
6.3.6 Funktion einer Hardware-Firewall.....	5
6.3.7 Kenntnisse über notwendige Einstellungen bei Virens Scanner.....	5
6.3.8 Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen.....	5
6.3.9 Kenntnisse über sichere Planung von Backups	6
6.3.10 Kenntnisse über verschiedene Backup-Prinzipien	6
6.3.11 Kenntnisse über Backup-Medien und deren richtiger Lagerung	6
6.3.12 Fachbegriff DMZ	7
6.3.13 Fachbegriff Stateful Packet Inspection.....	7
6.3.14 Funktionsweise eines Port-Scanners.....	7
6.3.15 Kenntnisse über Sicherheitstechnologie TLS.....	7
6.3.16 Fachbegriff CA in Zusammenhang mit Zertifikaten.....	8
6.3.17 Fachbegriffe Private Key und Public Key	8
6.3.18 Sicherstellen von Datenvertraulichkeit bei gemeinsamen Netzlaufwerken.....	8
6.3.19 Erarbeiten von Berechtigungskonzepten im Active Directory	8
6.3.20 Festlegen von Gruppenrichtlinien (GPOs).....	9
6.3.21 Erzwingen von Passwortrichtlinien	9
6.3.22 Kenntnisse über User Account Control (UAC).....	10
6.3.23 Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen.....	10

6.3.24 Kenntnisse über Methoden der sicheren Löschung von Daten	10
6.3.25 Inhalte von Unternehmensrichtlinien für Datenträgerentsorgung	11

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

Viren, Würmer und Trojaner schädigen Systeme, Spyware spioniert aus, Hacker greifen an und Phishing täuscht Nutzer zur Preisgabe sensibler Daten.

Viren

- Verändern oder zerstören Dateien
- Verbreiten sich über infizierte Programme/Dateien
- Können Systeme lahmlegen

Würmer

- Verbreiten sich selbstständig über Netzwerke
- Benötigen keine Benutzeraktion
- Verursachen Netzüberlastung und Systemausfälle

Trojaner

- Tarnen sich als nützliches Programm
- Öffnen Hintertüren für Angreifer
- Ermöglichen Datenklau oder Fernsteuerung

Spyware

- Spioniert Benutzeraktivitäten aus
- Sammelt Passwörter, Tastatureingaben, Daten
- Verletzung von Datenschutz und Privatsphäre

Hacker

- Verschaffen sich unbefugten Zugriff auf Systeme
- Ziele: Datendiebstahl, Manipulation, Sabotage
- Nutzen Sicherheitslücken oder schwache Passwörter

Phishing

- Gefälschte E-Mails/Webseiten
- Ziel: Zugangsdaten oder Bankdaten stehlen
- Häufig mit Druck oder falschen Warnungen

6.3.2 Fachbegriff Zero-Day-Exploit

Ein Zero-Day-Exploit ist ein Angriff, der eine bislang unbekannte Sicherheitslücke ausnutzt, für die es noch keine Sicherheitsupdates gibt.

6.3.3 Kenntnisse über Einschränkungsmöglichkeiten bei Benutzerkonten

Benutzerkonten können durch Rechtevergabe, Zugriffsbeschränkungen und Richtlinien so eingeschränkt werden, dass Sicherheit und Systemstabilität gewährleistet sind.

- Benutzerrechte
- Zugriffsrechte auf Dateien/Ordner
- Passwortrichtlinien
- Softwareeinschränkungen
- Geräteeinschränkungen
- Zeitliche Beschränkungen
- Netzwerk- und Interneteinschränkungen

6.3.4 Fachbegriff Multifaktor-Authentifizierung

Multifaktor-Authentifizierung ist ein Anmeldeverfahren, bei dem mehrere unterschiedliche Sicherheitsfaktoren zur Identitätsprüfung verwendet werden.

Mögliche Authentifizierungsfaktoren

- Wissen (Passwort, PIN)
- Besitz (Smartphone, Token, Smartcard)
- Biometrik (Fingerabdruck, Gesichtserkennung)

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

Hardware-Firewalls sichern das Netzwerk von außen, Software-Firewalls schützen den einzelnen Rechner von innen.

Hardware-Firewall

- Eigenständiges Gerät (z.B. Router)
- Schützt das gesamte Netzwerk
- Arbeitet unabhängig vom Betriebssystem
- Hohe Ausfallsicherheit und Performance
- Weniger anfällig für Schadsoftware auf PCs

Software-Firewall

- Programm auf einem Rechner
- Schützt nur das einzelne System

- Sehr feine Regeln (Programme, Ports)
- Günstig oder kostenlos

6.3.6 Funktion einer Hardware-Firewall

Eine Hardware-Firewall ist ein eigenständiges Gerät, das den Datenverkehr zwischen internem Netzwerk und Internet kontrolliert und unerlaubte Zugriffe blockiert.

- Überwacht den gesamten Netzwerkverkehr
- Filter Datenpakete nach Regeln (IP, Port, Protokoll)
- Blockiert unbefugte Zugriffe aus dem Internet
- Trennt internes Netzwerk vom externen Netz
- Verhindert direkte Zugriffe auf interne Geräte
- Arbeitet unabhängig vom Betriebssystem

6.3.7 Kenntnisse über notwendige Einstellungen bei Virens Scanner

Ein Virens Scanner muss aktuell sein, permanent überwachen, regelmäßig scannen auf gefundene Schadsoftware sicher isolieren.

- Echtzeitschutz
- Automatische Updates
- Regelmäßige Systemscans
- Heuristik / Verhaltensanalyse
- E-Mail- & Webschutz
- Quarantäne-Funktion
- Benachrichtigungen aktiv

6.3.8 Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

Client-PCs werden durch eingeschränkte Benutzerrechte, aktuelle Software, Sicherheitsprogramme und Zugriffsbeschränkungen vor Missbrauch geschützt.

- Benutzerkonten mit eingeschränkten Rechten
- Starke Passwörter & Multifaktor-Authentifizierung
- Aktuelles Betriebssystem und Updates
- Virens Scanner & Firewall
- Gerätesperre
- Softwareeinschränkungen
- USB- & Datenträgersperren
- Verschlüsselung

6.3.9 Kenntnisse über sichere Planung von Backups

Eine sichere Backup-Planung folgt der 3-2-1-Regel, erfolgt regelmäßig, verschlüsselt und wird durch Wiederherstellungstests überprüft.

6.3.10 Kenntnisse über verschiedene Backup-Prinzipien

Vollbackup sichert alles, inkrementell und differenziell nur Änderungen, Spiegelung ist kein echtes Backup, Image-Backups sichern ganze Systeme.

Vollbackup

- Sichert alle Daten
- Hoher Speicherbedarf
- Einfache Wiederherstellung

Inkrementelles Backup

- Sichert nur Änderungen seit dem letzten Backup
- Sehr speichersparend
- Wiederherstellung benötigt mehrere Backup-Stände

Differenzielles Backup

- Sichert Änderungen seit dem letzten Vollbackup
- Mehr Speicher als inkrementell
- Schnellere Wiederherstellung

Spiegelung

- Daten werden nur 1:1 kopiert
- Kein echtes Backup, da keine Versionierung

Image-Backup

- Sichert komplettes System (inkl. Betriebssystem)
- Schnelle, komplette Wiederherstellung

6.3.11 Kenntnisse über Backup-Medien und deren richtiger Lagerung

Backup-Medien müssen zuverlässig, extern gelagert, vor Umwelteinflüssen geschützt und bei sensiblen Daten verschlüsselt sein.

Backup-Medien

- Externe Festplatten
- USB-Sticks
- Bandlaufwerke (Tape)
- NAS/Netzwerkspeicher

- Cloud-Backup

Lagerung

- Physisch getrennt von Originalsystem
- Trocken, kühl, staubfrei
- Schutz vor Feuer, Wasser, Magnetfeldern
- Datenträger regelmäßig prüfen
- Backup-Datenträger nicht dauerhaft angeschlossen
- Verschlüsselung bei sensiblen Daten

6.3.12 Fachbegriff DMZ

Eine DMZ ist ein isolierter Netzwerkbereich, der öffentlich erreichbare Dienste bereitstellt und das interne Netzwerk zusätzlich absichert.

6.3.13 Fachbegriff Stateful Packet Inspection

Stateful Packet Inspection ist eine Firewall-Methode, die Datenpaketen inklusive ihres Verbindungszustandes prüft und nur legitime Verbindungen zulässt.

6.3.14 Funktionsweise eines Port-Scanners

Ein Port-Scanner sendet Testanfragen an Netzwerk-Ports, um offene, geschlossene oder gefilterte Dienste zu erkennen.

6.3.15 Kenntnisse über Sicherheitstechnologie TLS

TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll, das eine sichere und geschützte Datenübertragung im Netzwerk ermöglicht.

Funktionsweise

- Handshake (Client und Server handeln Verschlüsselung aus)
- Zertifikatsprüfung (Server weist Identität per Zertifikat nach)
- Schlüsselaustausch (Sicherer Sitzungsschlüssel wird erstellt)
- Verschlüsselung (Alle Daten werden verschlüsselt übertragen)

Einsatzbereich

- HTTPS
- E-Mail
- VPN's

6.3.16 Fachbegriff CA in Zusammenhang mit Zertifikaten

CA = Certification Authority

Eine CA ist eine vertrauenswürdige Stelle, die digitale Zertifikate ausstellt und damit Identitäten im Internet bestätigt.

Beispiel:

Wenn man eine HTTPS-Seite aufruft, prüft der Browser, ob das Zertifikat von einer vertrauenswürdigen CA stammt.

6.3.17 Fachbegriffe Private Key und Public Key

Private Key

- Bleibt geheim beim Besitzer
- Dient zum **Entschlüsseln** der Daten
- Wird auch für digitale Signaturen verwendet
- **Darf niemals weitergegeben werden**

Public Key

- Wird öffentlich verteilt
- Dient zum **Verschlüsseln** von Daten
- Ermöglicht anderen, dir sichere Nachrichten zu senden
- Kann keine Daten entschlüsseln

6.3.18 Sicherstellen von Datenvertraulichkeit bei gemeinsamen Netzlaufwerken

Datenvertraulichkeit bei Netzlaufwerken wird durch Benutzeranmeldung, gezielte Zugriffsrechte und Verschlüsselung sichergestellt.

6.3.19 Erarbeiten von Berechtigungskonzepten im Active Directory

Im Active-Directory werden Zugriffsrechte über Gruppen, OUs und GPOs nach dem Need-to-know-Prinzip strukturiert vergeben.

- Benutzer und Gruppenkonten erstellen (Benutzer erhalten Zugriff über Gruppen, nicht einzeln)
- Gruppenprinzip (AGDLP)
 - Account → Global Group → Domain Local Group → Permissions
 - Standardmodell für saubere Rechtevergabe
- Organisationseinheiten (OU)
 - Strukturierten Benutzer und Computer
 - Erleichtern Richtlinienverwaltung

- Zugriffsrechte auf Ressourcen
 - Dateiserver, Drucker, Anwendungen
 - Rechte: Lesen, Schreiben, Ändern
- Gruppenrichtlinien (GPO)
 - Setzen von Sicherheits- und Systemeinstellungen
 - Z.B. Passwortregeln, Sperrbildschirm
- Need-to-know-Prinzip
 - Benutzer erhalten nur nötige Rechte
- Regelmäßige Überprüfung
 - Entfernen veralteter Berechtigungen

6.3.20 Festlegen von Gruppenrichtlinien (GPOs)

GPOs sind zentrale Richtlinien im Active Directory, die Benutzer- und Computereinstellungen steuern und automatisch durchgesetzt werden.

GPO (Group Policy Object)

- Zentrale Verwaltung von Benutzer- und Computereinstellungen im Active Directory

Verknüpfung mit OUs

- GPOs werden an Organisationseinheiten (OU) gebunden
- Bestimmt, welche Benutzer oder Computer betroffen sind

Typische Einstellungen

- Passwort- und Sicherheitsrichtlinien
- Desktop- und Sperrbildschirmvorgaben
- Softwareinstallation
- USB- oder Gerätesperren
- Netzwerkeinstellungen

Zentrale Durchsetzung

- Richtlinien werden beim Anmelden automatisch angewendet

Vererbung & Priorität

- GPOs können vererbt oder überschrieben werden

6.3.21 Erzwingen von Passwortrichtlinien

Passwortrichtlinien werden per GPO erzwungen und legen Länge, Komplexität, Gültigkeit und Sperrregeln für sichere Benutzerkennwörter fest.

Typische Passwortrichtlinien

- Mindestlänge (z. B. ≥ 8 Zeichen)
- Komplexität
 - Groß-/Kleinbuchstaben
 - Zahlen
 - Sonderzeichen
- Maximales Passwortalter
 - Regelmäßige Passwortänderung
- Passwort-Historie
 - Verhindert Wiederverwendung alter Passwörter
- Kontosperre
 - Sperrung nach mehreren Fehlversuchen

6.3.22 Kenntnisse über User Account Control (UAC)

Die User Account Control verhindert unautorisierte Systemänderungen, indem Administratorrechte nur nach Bestätigung vergeben werden.

UAC (Benutzerkontensteuerung) ist eine Sicherheitsfunktion von Windows.

- Trennt Benutzer- und Administratorrechte
- Programme erhalten nicht automatisch Adminrechte
- Bei systemkritischen Änderungen erscheint eine Bestätigungsabfrage
- Verhindert, dass Schadsoftware unbemerkt Systemänderungen durchführt

6.3.23 Kenntnisse über Möglichkeiten Client-PCs vor Missbrauch zu schützen

Client-PCs werden durch eingeschränkte Rechte, starke Anmeldung, Updates, Sicherheitssoftware und Zugriffsbeschränkungen vor Missbrauch geschützt.

6.3.24 Kenntnisse über Methoden der sicheren Löschung von Daten

Sichere Datenlöschung erfolgt durch Überschreiben, Secure Erase, Löschen von Verschlüsselungsschlüsseln oder physische Zerstörung.

Sichere Löschmethoden

- **Überschreiben (Wiping)**
 - Daten werden mehrfach mit Zufallswerten überschrieben
 - Macht Wiederherstellung unmöglich
 - Tools: z. B. Secure Erase, Shredder
- **Secure Erase (bei SSDs)**
 - Vom Hersteller integrierter Löschbefehl
 - Löscht alle Speicherzellen zuverlässig
- **Verschlüsselung + Schlüssel löschen**

- Daten vorher verschlüsseln
- Danach Schlüssel vernichten → Daten unlesbar
- **Physische Zerstörung**
 - Schreddern, Bohren, Zerkleinern
 - Endgültige Löschung bei defekten Datenträgern

6.3.25 Inhalte von Unternehmensrichtlinien für Datenträgerentsorgung

Unternehmensrichtlinien zur Datenträgerentsorgung regeln Löschmethoden, Verantwortlichkeiten, Dokumentation und sichere Vernichtung zum Schutz vertraulicher Daten.

Damit bei der Entsorgung von Datenträgern keine vertraulichen Informationen verloren gehen, enthalten Unternehmensrichtlinien typischerweise folgende Punkte:

Klassifizierung der Datenträger

- Einstufung nach Schutzbedarf der gespeicherten Daten (z. B. intern, vertraulich, streng vertraulich)

Zugelassene Löschmethoden

- HDD: Mehrfaches Überschreiben
- SSD: Secure Erase oder kryptografische Löschung
- Optische Medien: Physische Zerstörung
- Vorgabe, welche Methode bei welcher Datenklasse erlaubt ist

Physische Vernichtung

- Schreddern, Bohren oder Zerkleinern
- Pflicht bei hochsensiblen Daten

Dokumentation

- Protokoll über Löschung oder Vernichtung
- Nachweis für Audits und Datenschutz

Zugriffsregelung

- Nur autorisierte Mitarbeiter dürfen Datenträger entsorgen

Transport & Lagerung

- Sichere Zwischenlagerung
- Kein unbeaufsichtigter Transport

Einhaltung gesetzlicher Vorgaben

- DSGVO / Datenschutzgesetze
- Aufbewahrungsfristen beachten

Ausarbeitung-Themenkatalog

7. Qualitäts- und Projektmanagement

7.1 Projektplanung

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

7. Qualitäts- und Projektmanagement	1
7.1 Projektplanung	1
Grundlagen des Projektmanagements	2
7.1.1 Projektmanagement & Definitionen	2
7.1.2 Ziele und Spannungsfelder	2
Anforderungsmanagement & Beauftragung	2
7.1.3 Lastenheft und Pflichtenheft	2
Projektplanung & Strukturierung	3
7.1.4 Wesentliche Planungsschritte	3
7.2 Visualisierungstools	3
Organisation & Rollen	4
7.2.1 Der Projektleiter	4
7.2.2 Projektorganisation	4
Dokumentation & Kosten	4
7.2.3 Projektdokumentation	4

Grundlagen des Projektmanagements

7.1.1 Projektmanagement & Definitionen

- **Projektmanagement:** Die Gesamtheit von Führungsaufgaben, -organisation, -techniken und -mitteln für die Abwicklung eines Projekts.
- **Definition von Projekten:** Ein Vorhaben, das im Wesentlichen durch die Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist (z. B. Zielvorgabe, zeitliche, finanzielle oder personelle Begrenzungen).
- **Internes vs. Externes Projekt:** Ein **internes Projekt** wird innerhalb der eigenen Organisation für eigene Zwecke durchgeführt, während ein **externes Projekt** auf einem Vertrag mit einem Außenstehenden Kunden basiert.

7.1.2 Ziele und Spannungsfelder

- **Primäres Projektziel:** Das Hauptergebnis, das am Ende des Projekts erreicht sein muss (oft die Lösung eines spezifischen Problems oder die Erstellung eines Produkts).
- **Spannungsfelder (Magisches Dreieck):** Projekte bewegen sich immer im Spannungsfeld zwischen **Zeit** (Termine), **Kosten** (Budget) und **Leistung/Qualität** (Inhalt). Eine Änderung an einer Ecke beeinflusst zwangsläufig die anderen.

Anforderungsmanagement & Beauftragung

7.1.3 Lastenheft und Pflichtenheft

- **Lastenheft:** Beschreibt die Gesamtheit der Forderungen des Auftraggebers an die Lieferungen und Leistungen eines Auftragnehmers (Was ist zu tun und wofür?).
- **Pflichtenheft:** Beschreibt die Realisierungsvorgaben des Auftragnehmers basierend auf dem Lastenheft (Wie und womit wird es umgesetzt?).
- **Projektauftrag:** Die schriftliche Vereinbarung zwischen Auftraggeber und Projektleiter, die den Startschuss gibt und Kompetenzen sowie Ressourcen festlegt.

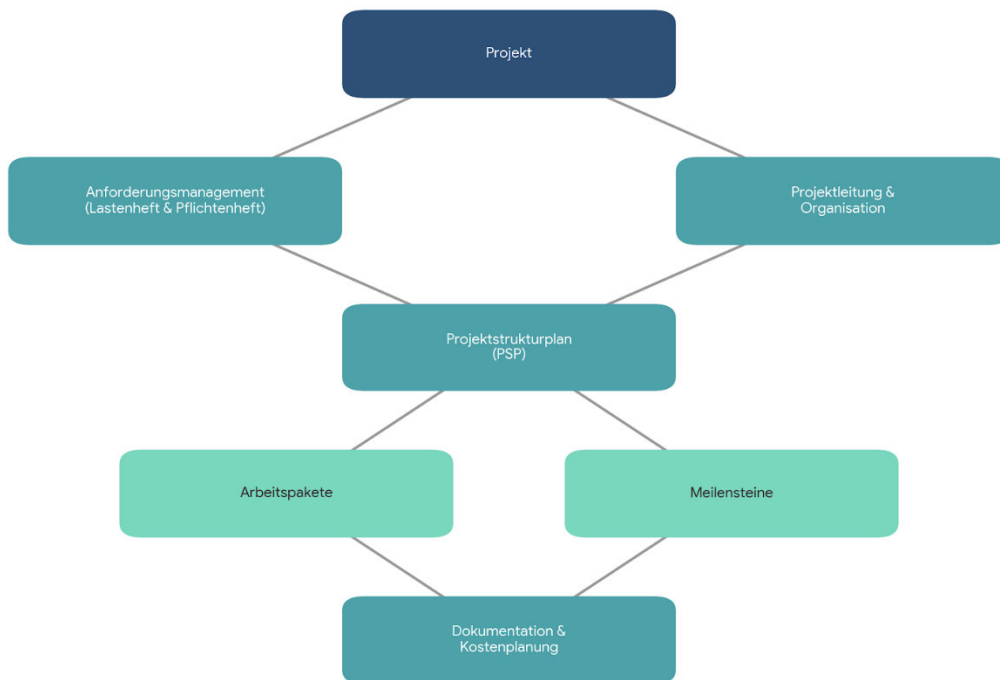


Lastenheft

Projektplanung & Strukturierung

7.1.4 Wesentliche Planungsschritte

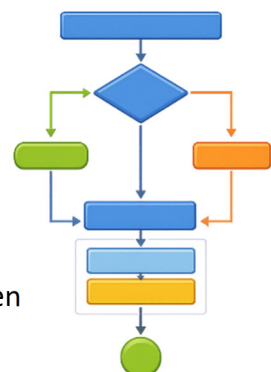
Der Planungsprozess umfasst die Definition der Ziele, die Zerlegung der Aufgaben, die zeitliche Abfolge sowie die Ressourcen- und Kostenplanung.



- **Projektstrukturplan (PSP):** Das „Herzstück“ der Planung. Er gliedert das gesamte Projekt in plan- und kontrollierbare Teilaufgaben und Arbeitspakete.
- **Arbeitspaket:** Die kleinste, nicht weiter zu untergliedende Einheit im Projektstrukturplan, die einem Verantwortlichen zugeordnet wird.
- **Meilenstein:** Ein Ereignis von besonderer Bedeutung (z. B. Abschluss einer Projektphase), das einen überprüfbaren Zwischenzustand markiert.

7.2 Visualisierungstools

- **Struktogramm (Nassi-Shneiderman):** Ein Diagrammtyp zur Darstellung von Programmlogik oder Algorithmen durch Verschachtelung von Blöcken.
- **Ablaufdiagramm (Flowchart):** Eine grafische Darstellung eines Prozesses oder Workflows, die logische Abfolgen und Entscheidungen mittels Symbolen visualisiert.



Organisation & Rollen

7.2.1 Der Projektleiter

- **Aufgaben:** Planung, Steuerung, Überwachung des Fortschritts sowie Führung des Projektteams.
- **Eigenschaften:** Erfordert sowohl Fachkompetenz als auch ausgeprägte Soft Skills wie Kommunikationsfähigkeit, Durchsetzungsvermögen und Konfliktfähigkeit.

7.2.2 Projektorganisation

- **Vorteile:** Klare Verantwortlichkeiten, Fokus auf das Ziel und oft schnellere Entscheidungswege.
- **Nachteile:** Mögliche Konflikte mit der Linienorganisation (Ressourcenstreit) und Unsicherheit der Mitarbeiter nach Projektende.

Dokumentation & Kosten

7.2.3 Projektdokumentation

- **Ziel:** Sicherstellung der Transparenz, Nachvollziehbarkeit von Entscheidungen, Beweissicherung und Wissenssicherung für zukünftige Projekte.



- **Projektkostenplanung:** Die Ermittlung der voraussichtlich anfallenden Kosten für Personal, Material und sonstige Ressourcen über die gesamte Projektlaufzeit.

Ausarbeitung-Themenkatalog

7. Qualitäts- und Projektmanagement

7.2 Projektmethoden, Tools

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

7. Qualitäts- und Projektmanagement	1
7.2 Projektmethoden, Tools.....	1
Projektmethoden & Tools	2
7.2.1 Softwareprozessmodelle	2
Klassische Modelle	2
7.2.2 Aufbau des Wasserfallmodells	2
7.2.3 Probleme beim Wasserfallmodell	3
7.2.4 Aufbau des V-Modells	3
7.2.5 Vor- und Nachteile des V-Modells.....	3
Agiles Projektmanagement (Scrum)	4
7.2.6 Agiles Projektmanagement	4
7.2.7 Scrum Fachbegriffe	4
Softwareentwicklung & Analyse	4
7.2.8 Softwareentwurf (Software Design).....	4
7.2.9 Stadien der Softwareentwicklung (SDLC).....	4
7.2.10 Prototyp.....	5
7.2.11 Soll-Ist-Analyse	5
7.2.12 Versionsverwaltung	5

Projektmethoden & Tools

Projektmethoden sind systematische Vorgehensweisen zur Planung und Durchführung von Projekten.

- **Methoden:** Klassisch (Wasserfall), Agile (Scrum, Kanban) oder Hybrid.
- **Tools:** Software zur Unterstützung wie **Jira** (Task-Management), **Confluence** (Dokumentation), **Trello** (Kanban-Boards) oder **MS Project** (Zeitplanung).

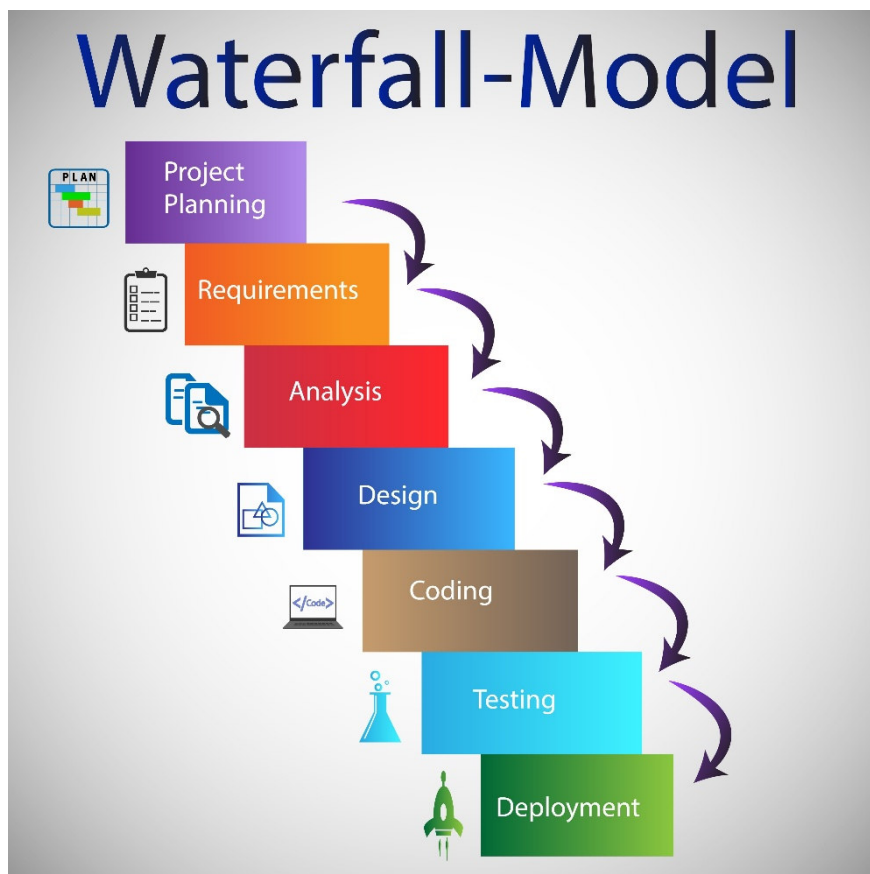
7.2.1 Softwareprozessmodelle

Ein Softwareprozessmodell ist ein abstrakter Entwurf für die Organisation der Softwareentwicklung. Es definiert die notwendigen Aktivitäten, Rollen und Ergebnisse (Artefakte) von der ersten Idee bis zur Wartung der Software.

Klassische Modelle

7.2.2 Aufbau des Wasserfallmodells

Das Wasserfallmodell ist ein **lineares, sequenzielles Vorgehensmodell**. Jede Phase muss vollständig abgeschlossen sein, bevor die nächste beginnt. Ein Rückschritt ist im reinen Modell nicht vorgesehen.

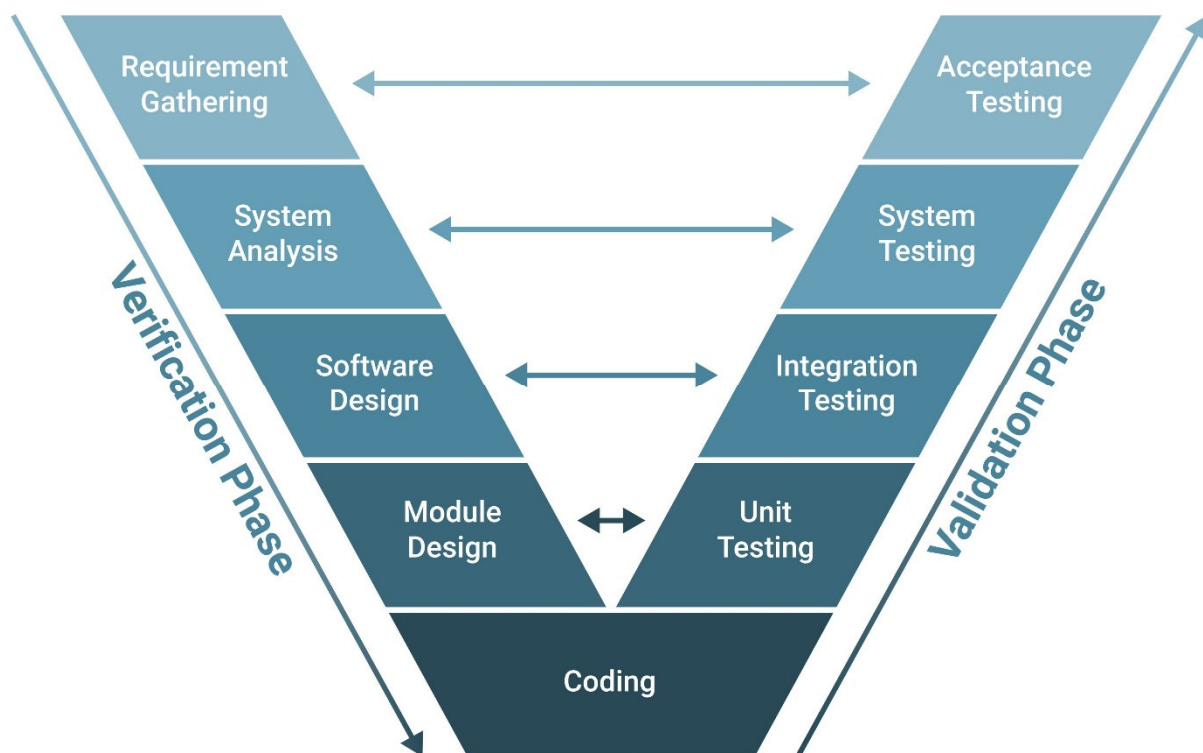


7.2.3 Probleme beim Wasserfallmodell

- **Mangelnde Flexibilität:** Änderungen während der Entwicklung sind teuer und schwer umsetzbar.
- **Spätes Feedback:** Der Kunde sieht das fertige Produkt erst ganz am Ende; Fehlentwicklungen werden spät erkannt.
- **Hohes Risiko:** Wenn die Anforderungen zu Beginn unpräzise sind, scheitert oft das gesamte Projekt.

7.2.4 Aufbau des V-Modells

Das V-Modell ist eine Erweiterung des Wasserfallmodells. Es stellt den Entwicklungsphasen direkt gegenüberliegende **Testphasen** (Verifizierungs- und Validierungsschritte) zur Seite.



7.2.5 Vor- und Nachteile des V-Modells

- **Vorteile:** Hohe Transparenz, klare Qualitätskontrolle durch frühzeitige Testplanung, minimiert Risiken.
 - **Nachteile:** Ebenfalls eher starr und schwerfällig bei sich ändernden Anforderungen; hoher bürokratischer Aufwand.
-

Agiles Projektmanagement (Scrum)

7.2.6 Agiles Projektmanagement

Ein iterativer Ansatz, bei dem Software in kleinen Schritten (Zyklen) entwickelt wird. Fokus liegt auf Flexibilität, Kundenfeedback und Selbstorganisation des Teams statt auf starrer Vorab-Planung.

7.2.7 Scrum Fachbegriffe

- **Scrum Master:** Der "Coach" des Teams. Er sorgt dafür, dass die Scrum-Regeln eingehalten werden und räumt Hindernisse (Impediments) aus dem Weg.
- **Product Owner:** Vertritt die Interessen der Kunden/Stakeholder. Er priorisiert die Aufgaben und entscheidet, **was** gebaut wird.
- **Backlog (Product Backlog):** Eine geordnete Liste aller Anforderungen, Features und Aufgaben, die für das Produkt geplant sind.
- **Sprint:** Ein fester Zeitraum (meist 2–4 Wochen), in dem ein funktionsfähiges Produkt-Inkrement erstellt wird.
- **Daily Scrum / Daily Standup:** Ein tägliches 15-minütiges Meeting, in dem das Team den Fortschritt bespricht und den kommenden Tag plant.
- **Stakeholder:** Alle Personen oder Gruppen, die ein berechtigtes Interesse am Projekt haben (Kunden, Anwender, Management).
- **User Story:** Eine Anforderung aus Sicht des Anwenders (Format: „Als [Rolle] möchte ich [Ziel], um [Nutzen]“).
- **Story Board:** Eine Visualisierung des Arbeitsfortschritts (oft Spalten wie: To Do, In Progress, Testing, Done).

Softwareentwicklung & Analyse

7.2.8 Softwareentwurf (Software Design)

Die Phase, in der die Architektur der Software festgelegt wird (Datenbankdesign, Klassenstrukturen, Schnittstellen), bevor der eigentliche Code geschrieben wird.

7.2.9 Stadien der Softwareentwicklung (SDLC)

1. **Analyse/Planung** (Anforderungen klären)
2. **Entwurf** (Architektur festlegen)
3. **Implementierung** (Programmierung)
4. **Testen** (Fehlersuche & Qualitätssicherung)
5. **Einführung/Wartung** (Release & Support)

7.2.10 Prototyp

Ein vorläufiges, meist vereinfachtes Modell der Software, um Konzepte zu testen oder frühzeitiges Feedback von Nutzern einzuholen.

7.2.11 Soll-Ist-Analyse

Ein Vergleich zwischen dem aktuellen Zustand (**Ist-Zustand**) und dem gewünschten Zielzustand (**Soll-Zustand**). Sie dient dazu, den Handlungsbedarf und die Anforderungen für ein Projekt zu definieren.

7.2.12 Versionsverwaltung

Ein System (z. B. **Git**), das Änderungen am Quellcode protokolliert. Es ermöglicht es, zu älteren Ständen zurückzukehren und die Zusammenarbeit mehrerer Entwickler am selben Code zu koordinieren.

Ausarbeitung-Themenkatalog

8. Qualitätssicherung

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

8. Qualitätssicherung	1
Qualitätssicherung (QS).....	2
8.1 Zweck von Code-Reviews	2
8.2 Fachbegriff: Schreibtischtest.....	2
8.3 Software-Testverfahren	2
8.4 Qualitätsmerkmale der Softwarefunktionalität (nach ISO 25010)	2
8.5 Changemanagement (Änderungsmanagement).....	3
8.6 Versionierung und deren Nutzen	3
8.7 Problemmanagement	3

Qualitätssicherung (QS)

Die Qualitätssicherung umfasst alle geplanten und systematischen Maßnahmen, die sicherstellen, dass ein Softwareprodukt die festgelegten Anforderungen erfüllt. Im Gegensatz zum reinen „Testen“ (das Fehler findet), ist die QS prozessorientiert und versucht, Fehler durch standardisierte Abläufe von vornherein zu **vermeiden**.

8.1 Zweck von Code-Reviews

Ein Code-Review ist eine manuelle Überprüfung des Quellcodes durch andere Entwickler (Vier-Augen-Prinzip).

- **Fehlererkennung:** Logikfehler oder Sicherheitslücken finden, die automatisierte Tests übersehen.
- **Wissenstransfer:** Teammitglieder lernen voneinander und verstehen den Code der anderen.
- **Standardisierung:** Sicherstellen, dass Coding-Guidelines eingehalten werden (Lesbarkeit, Wartbarkeit).

8.2 Fachbegriff: Schreibtischtest

Der Schreibtischtest ist eine manuelle Prüfung eines Algorithmus oder Programmabschnitts ohne Computer. Dabei geht der Entwickler den Code Schritt für Schritt auf dem Papier (oder im Kopf) mit Beispieldaten durch.

- **Ziel:** Die Logik eines Algorithmus frühzeitig validieren, bevor Zeit in die Implementierung investiert wird.

8.3 Software-Testverfahren

Merkmal	Black-Box-Test	White-Box-Test
Kenntnis des Codes	Keine (Sicht nur auf Input/Output).	Vollständiger Einblick in den Quellcode.
Fokus	Erfüllt die Software die funktionale Anforderung?	Sind alle Pfade, Schleifen und Bedingungen korrekt?
Zielgruppe	Meist Tester oder Endanwender.	Meist die Entwickler selbst.

Wesentlicher Unterschied: Beim Black-Box-Test testest du **WAS** die Software macht; beim White-Box-Test testest du, **WIE** sie es intern technisch umsetzt.

8.4 Qualitätsmerkmale der Softwarefunktionalität (nach ISO 25010)

Wichtige Merkmale, die über die reine „Lauffähigkeit“ hinausgehen:

- **Angemessenheit:** Erfüllt die Software genau die Aufgaben, die der Nutzer braucht?
- **Richtigkeit:** Liefert die Software die korrekten Ergebnisse?
- **Sicherheit:** Sind Daten vor unbefugtem Zugriff geschützt?
- **Interoperabilität:** Wie gut arbeitet das System mit anderen Systemen zusammen?

8.5 Changemanagement (Änderungsmanagement)

Ein strukturierter Prozess zur Beantragung, Bewertung, Genehmigung und Umsetzung von Änderungen an der Software oder Infrastruktur.

- **Ziel:** Unkontrollierte Änderungen („Wildwuchs“) verhindern und Risiken für den laufenden Betrieb minimieren.

8.6 Versionierung und deren Nutzen

Versionierung ist die Zuweisung von eindeutigen Nummern oder Namen (z.B. v1.0.2) zu verschiedenen Zuständen einer Software oder Datei.

- **Nutzen:**
 - **Nachvollziehbarkeit:** Wer hat wann was geändert?
 - **Rollback:** Bei Fehlern kann sofort auf einen alten, funktionierenden Stand zurückgegriffen werden.
 - **Parallelität:** Mehrere Entwickler können gleichzeitig an verschiedenen Features arbeiten (Branching).

8.7 Problemmanagement

Während das *Incident Management* versucht, eine Störung schnellstmöglich zu beheben, sucht das **Problemmanagement** nach der **Ursache (Root Cause)**.

- **Ziel:** Wiederkehrende Fehler dauerhaft zu beseitigen und die Stabilität des Systems langfristig zu erhöhen.