Prüfungsvorbereitung

Prüfungsvorbereitung für den Teil I der Abschlussprüfung des Jahrgangs IT22 der IHK Koblenz von Niklas Grothe

10. NOVEMBER 2023

Debeka
Debeka Platz 1-5, 56073 Koblenz

1) INHALTSVERZEICHNIS

2) Abbildungen....3
3) Themenübersicht....4
a) Thema 1: Projekte....4
i) Projektmanagement....4
ii) Methoden und Modelle....5
iii) Teamarbeit....6
iv) Changemanagement....6
b) Thema 2: Wirtschaftslehre / Sozialkunde....7
i) Wirtschaftlichkeit....7
ii) Märkte und Bedarf....8
iii) Verträge....8
iv) Kundenberatung/Präsentieren....9
v) Marketing....9
vi) Angebotsvergleich....10
vii) Leistungserbringung....11
c) Thema 3: Hardwarekomponenten....12
i) Hardware....12
ii) Betriebssysteme....13
iii) Multimedia und Berechnungen....14
d) Thema 4: Netzwerke....14
i) Netzwerktechnik....14
ii) Internet....15
e) Thema 5: Softwarekomponenten....16
i) Software....16
ii) Softwareentwicklung....16
iii) Qualitätssicherung....17
f) Thema 6: ITS....18
i) IT-Sicherheit....18
ii) Datenschutz....19
4) Dokumentation....20
a) Projekte....20
i) Projektmanagement....20
ii) Methoden und modelle....20
iii) Teamarbeit....20
iv) Changemanagement....20
b) Wirtschaftslehre / Sozialkunde....20

i) Wirtschaftlichkeit....20
ii) Märkte und Bedarf....20
iii) Verträge....20
iv) Kundenberatung/Präsentieren....20
v) Marketing....20
vi) Angebotsvergleich....20
vii) Leistungserbringung....20
c) Hardwarekomponenten....20
i) Hardware....20
ii) Betriebssysteme....22
iii) Multimedia und Berechnungen....22
d) Netzwerke....23
i) Netzwerktechnik....23
ii) Internet....30
e) Softwarekomponenten....30
i) Software....30
ii) Softwareentwicklung....31
iii) Qualitätssicherung....32
f) ITS....32
i) IT-Sicherheit....32
ii) Datenschutz....46

2) ABBILDUNGEN

Abbildung 1 Struktur einer Schutzbedarfsanalyse.....37
Abbildung 2 Umsetzung einer DMZ mit einer bzw. zwei Firewalls.....46

PRÜFUNGSVORBEREITUNG FI22

3) THEMENÜBERSICHT

A) THEMA 1: PROJEKTE

I) PROJEKTMANAGEMENT

- Nötige Kenntnisse
  - Initiieren, Planen, Steuern, Kontrollieren und Abschließen von Projekten nach aktuell gängigen Projektmanagementstandards
  - Abklären der Rahmenbedingungen unter Berücksichtigung von Datensicherheit und Datenschutz (wirtschaftlich, technisch, rechtlich, terminlich)
- Projekt: zeitlich befristet, relativ innovativ, risikobehaftet, erhebliche Komplexität, erfordert ein Projektmanagement
  - Nach DIN 69901: Vorhaben, das im Wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist
  - Nach PRINCE2: a temporary organization that is created for the purpose of delivering one or more business products according to an agreed Business Case
- Magisches Dreieck: Qualität, Kosten, Zeit
- Qualität: Übereinstimmung der Anforderungen
- SMARTe Ziele: spezifisch, messbar, attraktiv, realistisch, terminiert
- 4-Phasen-Modell
  - Projektdefinition
  - Projektplanung
  - Projektdurchführung und -controlling
  - Projektabschluss
- Kick-Off-Meeting
  - Nach erfolgter Planung vor Start der Projektdurchführung
  - Projektstrukturplan wird erstellt.
- Meilensteine: wichtige Ereignisse des Projekts werden visualisiert und geplant
- Aufgaben/Inhalte/Verbindlichkeit von Lasten-/Pflichtenheften und Angeboten
  - Lastenheft: was/wofür?
  - Pflichtenheft: wie/womit?
- Definieren von Aufgaben, Rollen und Verantwortlichkeiten für alle Projektbeteiligten. Z.B.:
  - Projekt-Auftraggeber
  - Projektleiter
  - Projekt-Steuerkreis
  - Projektmitarbeiter
- Stakeholder: Gruppen oder Personen, die irgendein Interesse am Projekt haben.
- Aufgaben eines Projektleiters: Mitwirkung bei der Zieldefinition Koordination des Teams, Aufgabenverteilung innerhalb des Teams. Überwachung der Projektfortschritte, Kommunikation, Projektcontrolling, Dokumentation, Aufwandschätzung, Vorlage der Ergebnisse beim Lenkungsausschuss, Eskalation von Konfliktsituationen, Erstellen des Projektabschlussberichtes
- Analysieren im Sinne von Erkennen und Einordnen
- Problemlösungsvarianten entwickeln und Probleme beseitigen z.B. durch
  - Situationsanalyse
  - Problemeingrenzung
  - Aufzeigen von Alternativen
  - Auswahl von Lösungen
  - Analysieren der Chancen und Risiken der ausgewählten Lösung anhand vorher definierter Beurteilungskriterien
  - Root-Cause-Analysis
  - 5 Whys

- Kundenkommunikation
- Fehlermanagement, Störungsmanagement
- Supportanfragen, Bearbeitungsstatus, z.B. mittels Ticketsystem
  - Ticketsystem: Verteilung der Aufgaben, Koordination der Beteiligten, Historie, Dokumentation, Auswertungen

II) Methoden und Modelle

- Unterscheiden verschiedener Projektmanagementmethoden und Vorgehensmodelle
  - Projektphasen, z.B. Analyse, Entwurf, Implementierung, Test, Betrieb
  - „klassisch“: Wasserfall, V-Modell, Spiralmodell
  - Agil: Scrum Kanban, Extreme Programming
- Anwendungen von Methoden, Hilfsmitteln, Techniken und Kompetenzen in einem Projekt, z.B.:
  - Projektplan
  - Meilensteine
  - Risikoanalyse
  - Standards und Normen
  - Projektmanagementsysteme
- Projektplanung mit Hilfe von Strukturplan, Netzplan, Gantt-Diagramm
  - Kritischer Pfad: Gesamtpuffer ist 0, bestimmt die gesamte Projektdauer
  - Pufferzeiten
  - Fristgerechte Terminierung
  - Lösungsmöglichkeiten bei Terminproblemen
  - Meilensteine
  - Definieren und Festlegen von Arbeitspaketen und Abhängigkeiten
  - Erleichterung der Planung und der Fortschrittskontrolle durch Aufteilung des Arbeits- bzw. Projektverlaufs in überprüfbare Etappen mit Zwischenzielen
  - Umsetzung der Arbeitspakete in konkrete Handlungen und Messen anhand von Prüfkriterien
  - Ggf. Ableiten einer Prognose für den weiteren Fortschritt bzw. den Endtermin
  - Vollständige Erfassung aller relevanten Tätigkeiten eines Projektes (funktionsorientierte, objektorientierte oder zeitorientierte Gliederung) im Top-down-, Bottom-up- oder Yo-Yo-Ansatz
- Erstellung von Projektstrukturplänen zur Gliederung von Projekten in plan- und kontrollierbare Elemente
  - Statische Sicht
  - Zerlegung des Gesamtprojekts in Teilschritte
  - Top-Down-Verfahren (deduktiv) vs. Bottom-Up-Verfahren (induktiv) vs. Yo-Yo-Verfahren (Gegenstromverfahren)
- Netzplan
  - Dauer der Aktivitäten
  - Zeitliche und logische Abhängigkeiten werden gezeigt
  - Pufferzeiten und der kritische Pfad sind erkennbar
  - Frühester/spätester Anfangszeitpunkt, frühester/spätester Endzeitpunkt, Gesamtpuffer, freier Puffer
- Gantt-Diagramm
  - Zeitliche Reihenfolge der Aktivitäten auf einer Zeitachse (z.B. Kalenderwochen)
  - Parallelität sichtbar
  - Abhängigkeiten können visualisiert werden
- Visualisierung
  - Netzplantechnik
  - Scrum Board
  - Kanban Board
  - Gantt-Diagramme
- Kanban-Bord: WIP-Limit (work in progress), Pull statt Push, Spalten entsprechen Prozessschritten

III) Teamarbeit

- Teambildung und -entwicklung
  - Prozess der Teambildung nach Bruch Tuckman:

        - Forming
        - Storming
        - Norming
        - Performing
        - (Adjourning)
    - Team als soziales Gefüge verstehen („social awareness“)
    - Phasen der Teamentwicklung kennen und anwenden (Konflikt, Kontrakt, Kooperation)
- Reflexion
    - Gemeinsame kritische Analyse der bisherigen Zusammenarbeit und der Ergebnisse („lessons learned“)
    - Offenes Ansprechen von Erfolgen und Problemen
    - Gemeinsame Entwicklung von Maßnahmen zur Verbesserung, z.B. SCRUM-Retrospektive
    - Konstruktive Kritik
    - Retrospektive: Wie kann der Prozess und die Zusammenarbeit im Team verbessert werden?
    - Konstruktive Kritik: konkrete Wahrnehmung schildern (nicht interpretieren, nicht verallgemeinern), Auswirkungen aufzeigen, Ich-Botschaften senden, Wunsch äußern
    - Reflexionsmethoden, z.B. Feedback-Kultur, Lessons learned.
- Adressatengerechte Kommunikation
- Methoden des sachbezogenen Verhandelns kennen und anwenden, Verhandlungen führen
    - Win-win-Strategie: Konfliktlösung ohne Verlierer
    - Havard-Konzept
        - Menschen und Interessen trennen
        - Fokus auf Interessen und nicht auf Positionen
        - Entscheidungsoptionen entwickeln
        - Objektive Beurteilungskriterien anwenden
    - BATNA: Best Alternative to a Negotiated Agreement
    - Communication is what the listener does (Peter Druckner)
- Berücksichtigung der Formen von Arbeitsorganisation, z.B.:
    - Gruppenarbeit
    - Pair Programming
- Betriebsrat
    - Rechte und Pflichten
    - Rechtliche Voraussetzungen
- Kündigung
    - Gesetzliche/vertragliche Fristen
    - Notwendige Unterlagen
- Diversität, Interkulturalität, Fehlerkultur

IV) CHANGEMANAGEMENT

- Basiskenntnisse des Veränderungsmanagements
    - Darstellung der Veränderungsschritte, z.B. anhand der sieben Phasen eines Change-Prozesses
    - Change-Management (Prozess zur Umsetzung von Veränderungen in Unternehmen) z.B. nach Lewin (Unfreeze, Change, Refreeze)
    - Kaizen, Continuous Improvement
- Motivierte Herangehensweise und Betonung der Chancen
    - Hervorhebung der Vorteile und Nutzen-Argumentation
    - Identifizierung und Darstellung von Veränderungsschritten
    - Voranbringen schnell und in geeigneter Weise unterstützen
    - Zielorientierte Vorgehensweise
- Einbeziehung der Mitarbeiter in den Veränderungsprozess
    - Mitarbeiterqualifizierung, z.B. durch BlendedLearning, Multiplikatoren
    - Erkennen von Promoter, Bremser, Skeptiker und Widerständler
    - Fragen beantworten, informieren und zuhören
    - Anreichern mit eigenem Know-how

- Unterstützung bei der Umsetzung von Schulungsangeboten
- Durchführung von Einführungsveranstaltungen (auch begleitende Unterstützung vor Ort)

❖ Ursachen von Widerständen gegen Veränderungen, z.B.
- Angst vor Kompetenzverlust
- Wissenslücken
- Persönliche Historie

B) THEMA 2: WIRTSCHAFTSLEHRE / SOZIALKUNDE

I) WIRTSCHAFTLICHKEIT

❖ Machbarkeitsanalyse: technisch, organisatorisch, wirtschaftlich, zeitlich und rechtlich
❖ Make-or-buy-Entscheidung
❖ Risikoanalyse
❖ Budgetplanung als Teil der Unternehmensplanung
- Budget: die für einen bestimmten Zweck zur Verfügung stehenden Geldmittel

❖ Effektiver und effizienter Ansatz von Arbeits- und Organisationsmitteln
- Effektivität: Die richtigen Dinge tun.
- Effizienz: Die Dinge richtig tun.

❖ Prüfung des Ressourceneinsatzes auf:
- Rechtliche Zulässigkeit
- Technische und organisatorische Machbarkeit
- Ökologische Nachhaltigkeit und Wirtschaftlichkeit

❖ Prüfung der Wirtschaftlichkeit mittels betriebswirtschaftlicher Methoden, z.B.:
- Rentabilitätsrechnung
- Amortisationsrechnung

❖ Betriebswirtschaftliche Kennzahlen, z.B. Umsatz, Gewinn, Deckungsbeitrag
- Umsatz: Absatzmenge * Verkaufspreis
- Gewinn: Erlöse – Kosten
- Deckungsbeitrag: Stückpreis – variable Stückkosten
- Rentabilität: Gewinn / Kapital
- Amortisation: Investition / Ertrag pro Jahr

❖ Ermittlung und Bedeutung von Umsatz/Provision/Deckungsbeitrag/Kosten/Gewinn
❖ Zahlungsverzug
- Definition, Gründe, Konsequenzen
- Rechtsgrundlage/Definition für Zahlungsverzug

❖ Möglichkeiten zum Umgang mit Liquiditätsengpässen
❖ Gemeinkosten auf Kostenstellen verteilen
❖ Kosten für eine Produkteinführung berechnen
❖ Break-Even-Point ermitteln
❖ Gewinn ermitteln
❖ Vor-/Nachteile Kauf/Leasing/Miete
❖ Eigen- und Fremdfinanzierung
❖ Profit-Center-Organisation
❖ Handelskalkulation
❖ Betriebsabrechnungsbogen, Nachkalkulation, Zuschlagskalkulation
❖ Fehler in Lieferschein/Rechnung finden
❖ Gesetzliche Gewährleistungsfrist ermitteln
❖ Umgang mit Mängeln, Mängelrüge
❖ Umgang mit Vertragsstörungen
❖ Zweiseitiger Handelskauf und Rechte/Pflichten
❖ TCO erläutern
❖ Rabatt und Skonto berechnen
❖ Umrechnungen in Zahlensystemen (Dual, Dezimal, oktal, Hexadezimal) -> passt hier nicht ganz rein, sucht neue Heimat

II) MÄRKTE UND BEDARF

- Volkswirtschaftliche Sektoren: primär, sekundär, tertiär
- Betriebliche Grundfunktion: Beschaffung, Produktion, Vertrieb, Finanzierung
- Marktformen, z.B. Monopol, Oligopol, Polypol, Käufer-/Verkäufermarkt, Marktgleichgewicht
- Feststellung des Bedarfs an Waren, Dienstleistungen oder Personal in einer bestimmten Region, einer bestimmten Personengruppe oder in einem bestimmten Zeitraum, z.B.:
  - Zielgruppendefinitionen und -abgrenzungen
  - Kundentypologien
  - Konsumverhalten
- Angebotsbewertung
- Fragetechnik, aktives Zuhören, bedarfs- und adressatengerechte Präsentation
- Eigene Datenerhebung (z.B. Kundenbefragung)
- Auswertung vorhandener Daten (z.B. Anforderung an Büroarbeitsplätze)
- Primär- und Sekundärforschung
- Unterscheiden und Nutzen von Erhebungsmethoden, z.B.:
  - Benchmarking
  - Befragungen
  - Data Mining
- Marktbeobachtung und Marktanalyse mit Marktdaten als Grundlage, z.B.:
  - Preisentwicklungen
  - Struktur der Anbieter
  - Produktqualitäten
- Unternehmens-/Gesellschaftsformen, z.B. AG, GmbH, SE, UG, GbR, OHG, KG, Ltd.
  - Personen- vs. Kapitalgesellschaft
  - Kriterien: Haftung, Kapital, Gesellschafter, juristisch/natürlich, Firma

III) VERTRÄGE

- Vertragsarten
  - Kaufvertrag
  - Lizenzvertrag
  - Servicevertrag
  - Miete vs. Leasing
  - Werkvertrag vs. Dienstvertrag
- Vertragsbestandteile, z.B. Leistungsbeschreibung, Termine, Entgelte, Lasten- und Pflichtenheft, Konventionalstrafen
  - Service Level Agreements (SLA)
- First, Second und Third Level Support
- Verzug
- Ziele: ökologisch, ökonomisch (z.B. prozentuale Marge), sozial
- Kontinuierliche Prüfung der vertraglich vereinbarten Vorgaben
- Aufbewahrung von Archivdaten, gesetzliche Vorgaben, Unterschied zu Backup
- Urheberrecht
  - Von Patenten abgrenzen
  - Creative Commons
- Fernabsatzverträge
- Gewährleistung vs. Garantie
- Werks- vs. Dienstvertrag
- Inhalte von SLAs
- Arbeitsvertrag
  - Inhalte, Rechte/Pflichten
  - Kollektives Arbeitsrecht
- Verschiedene Versicherungen (z.B. Haftpflicht, Berufsunfähigkeit, Krankenversicherung, Rechtsschutz, Hausrat, KFZ, Gebäudeversicherung usw.)

IV) KUNDENBERATUNG/PRÄSENTIEREN

- Präsentationen erstellen → **wichtig, aber nicht Teil von Präsentationen**
- Argumentations- und Präsentationstechniken
  - Zielgruppengerechte und lösungsorientierte Vorstellung von Produkten und Ergebnissen
  - Medien zur Kundenpräsentation und -information, z.B. Kundengespräch via Webinar
- Online-Schulungen
- Website/Homepage
- Kommunikationsmodelle, z.B.
  - Sender-/Empfängermodell
  - Eisbergmodell
  - 4-Ohren-Modell: Sachebene, Appell, Selbstoffenbarung, Beziehung
- Technische und nicht-technische Texte → **wichtig, aber nicht Teil von Präsentationen**
- Digitale Suchabfragen unter Verwendung von Suchoperatoren
- Auswertung von englischen Texten
- Qualitätsmerkmale von Präsentationen
- Medienkompetenz
- Unterschiedliche Quellen nutzen und bewerten, z.B.:
  - Internet und Intranet
  - Fachliteratur
  - Technische Dokumentationen
- Berücksichtigungen der geltenden Compliance-Regelungen, Ethik → **wichtig, aber nicht Teil von Präsentationen** (hierzu auch das Lernportal nutzen). Für die Präsentation nur kurze Definition

V) MARKETING

- Stärken- Schwächen-Analyse (SWOT etc.)
- ABC-Analyse
- Begleiten von IT-Vertriebsprozessen
- Motive und Werte der Kunden
- Kundenzufriedenheit
- Nutzwertanalyse
- Vertriebsformen: direkter Vertrieb, indirekter Vertrieb
- Cross-Selling, Upselling
- Kundenbefragungen
  - Offene/geschlossene Fragen
- Pre-Sales
- Fachbegriffe kennen
  - Marktvolumen, Absatz, Marktanalyse etc.
  - B2B, B2C, B2G
  - Umfrage, Beobachtung, Experiment, Testmarkt, Marktprognose, Panelerhebung
  - Marktdurchdringung, Marktentwicklung, Markterschließung, Produktinnovation, Produktentwicklung, Diversifikation
- AIDA (Attention, Interest, Desire, Action)
- Phasen des Produktlebenszyklus
  - Einführung, Wachstum, Reife, Sättigung, Rückgang, End-of-Life
- Phasen der Technologieadaption
  - Innovators, Early Adopters, Early Majority, Late Majority, Laggards
- Outsourcing (organisatorisch) vs. Offshoring (geografisch)
- Geschäftsmodelle im Internet
  - Freemium, In-Game-Payment

VI) ANGEBOTSVERGLEICH

Hängt sehr stark mit Wirtschaftlichkeit zusammen

- Nötige Kenntnisse
  - Potenziale von IT-Systemen bzw. einem Verbund verschiedener Arten erkennen
  - IT-Systeme anhand ihres wirtschaftlichen Nutzens zum Unternehmenserfolg bewerten → wichtig, aber nicht Teil von Präsentationen
- Angebotsvergleiche
  - Gegenüberstellung Eigenfertigung oder Fremdbezug (Make or buy)
  - Partieller/gewichteter Preisvergleich
  - Qualitativer und quantitativer Angebotsvergleich
  - Auslastung und Anpassungsfähigkeit/Erweiterbarkeit, Zukunftssicherheit → wichtig, aber nicht Teil von Präsentationen
  - Aus den Angeboten verschiedener Lieferanten das am besten geeignete Angebot identifizieren, z.B. mithilfe der Nutzwertanalyse
  - Technische Leistungskriterien verschiedener IT-Systeme vergleichen und bewerten → wichtig, aber nicht Teil von Präsentationen
- Ausschreibung von Leistungen
- Beschreibung von Leistungen, z.B.:
  - Lasten- und Pflichtenheft
  - Leistungsverzeichnis
- Kosten
  - Anschaffungskosten
  - Betriebskosten
  - Variable und fixe Kosten
  - Lizenzkosten
  - Finanzierungskosten
  - Kostenvergleich: Leasing, Kauf, Miete, Pay-per-use
  - Preis-Leistungs-Verhältnis
  - Gegenüberstellen von Kosten/Nutzen
- Kalkulation
  - Handelskalkulation: Listen-, Ziel-, Bareinkaufspreis, Bezugspreis, Selbstkosten, Bar-, Ziel-, Listenverkaufspreis
  - Zuschlagskalkulation: Materialeinzel-, Materialgemein-, Lohneinzel-, Lohngemeinkosten, Herstellkosten, Verwaltungs-, Vertriebsgemeinkosten

VII) LEISTUNGSERBRINGUNG

- Nötige Kenntnisse
  - Abstimmen der zu erwartenden Ergebnisse hinsichtlich betrieblicher und vertraglicher Rahmenbedingungen mit dem Auftraggeber
  - Abstimmen der dokumentierten Vorgaben zur Leistungserbringung während des gesamten Zeitraums mit dem Auftraggeber
  - Kontinuierliche Prüfung der erfolgreichen Umsetzung und Ergebnisse sowie der zeitlichen Einhaltung
  - Dokumentation der angefallenen Kosten anhand einer Kostenaufstellung und der wirtschaftlichen Leistungserbringung erstellen
  - Bewerten und Dokumentieren der erbrachten Leistungen anhand der anfänglichen Abstimmung der betrieblichen und vertraglichen Vereinbarungen
- Kundenvorgaben bei der Leistungserbringung, z.B.
  - Termin und Erfüllungsort
  - Technische Voraussetzungen (z.B. Betriebssystem, Hersteller)
  - Kauf, Miete, Leasing
  - Leistungserbringung vor Ort vs. Remote
  - Berücksichtigung der Stilllegung von Altsystemen und Inbetriebnahme der neuen Systeme
  - Personaleinsatzplanung auf Basis der Arbeits- und Projektzeiterfassung
- Rolloutprozesse
  - Vorbereitung (Kunden-Onboarding, Scope festlegen, Formalitäten)

- Rolloutumsetzung (Integration von Schnittstellen, kundenspezifische Entwicklungen)

❖ Aufbauorganisation: Mehrliniensystem, Einliniensystem, Matrixorganisation, Stabliniensystem
- Organigramm

❖ Handlungs- und Entscheidungsspielräume/Vollmachten
- Unterschriften: i.V., i.A., ppa.
- Prokura, Handlungsvollmacht

❖ Abnahme
- Bedeutung und Moment der Abnahme verdeutlichen
- Vor der Abnahme: Prüfung der Funktionsfähigkeit sowie Installation und Personalschulung
- Abnahmeprotokoll mit Angaben zu Vollständigkeit, Funktionseignung und Schadensfreiheit des geprüften Werks erstellen
- Zusätzlich Aufnahme nicht geprüfter Abnahmekriterien
- Inhalt des Abnahmeprotokolls, z.B.
  - Gegenstand der Abnahme
  - Beteiligte Personen
  - Ort, Datum und Uhrzeit
- Nötige Unterlagen zur Einführung und Umsetzung der Ergebnisse bereitstellen und übergeben, z.B.:
  - Planungsunterlagen
  - Angaben zu genutzten Systemen und Daten

❖ Vollständige Dokumentation der erbrachten Leistung
- Dokumentation der Vereinbarung, z.B. mittels Pflichtenheft oder Anforderungskatalog
- Dokumentation von Arbeits- und Projektzeiten (aktuell, flächendeckend und realistisch)
- Zeiterfassung als Bestandteil des Projektmanagements und Controllings
- Erfüllen oder Abweichen von der Vereinbarung dokumentieren
- Erbrachte Leistungen bestätigen lassen
- Arten der zu übergebenden Dokumentation, z.B.
  - Benutzerdokumentation (Handbuch)
  - Schnittstellendokumentation
  - Programmdokumentation (Source Code)
  - Netzwerkdokumentation
  - Testprotokolle
- Bestätigung erbrachter Leistungen

❖ Mängel und Mängelarten
- Schlechtleistung, z.B. fehlende Funktionalität
- Falschlieferung, z.B. falsche Softwarepakete ausgeliefert
- Minderlieferung, z.B. nur Teile der Software ausgeliefert

❖ Soll-Ist-Vergleich
- Abgleich mit der Sollspezifikation durchführen und protokollieren
- Abweichungsanalyse

❖ Lessons Learned

❖ Doppelte Buchführung

❖ Fort- und Weiterbildung, Umschulung

C) Thema 3: Hardwarekomponenten

I) Hardware

❖ Nötige Kenntnisse
- Funktionale, ökonomische, ökologische, soziale Aspekte bewerten
- Installation und Konfiguration der Hardware

❖ Hardwareprodukte, z.B. CPU, Motherboard, Speicher, Datenspeicher, Netzteile, Grafikkarte, Peripheriegeräte, Netzwerkkomponenten, WLAN
- Ein-/Ausgabegeräte: Drucker, Scanner, Maus, Display, Touchpad, Tastatur
- Arten von Scannern: Flachbett, Handscanner, Trommelscanner, Dokumentenscanner
- Arten von Druckern: Tintenstrahl, Laser, Thermo, Nadel

- Prozessor/CPU, Kühlung
  - Von-Neumann-Architektur
  - ALU
  - Latency Numbers Every Programmer Should Know
- RAM-Arten und Unterschiede
  - Unterschiede Stack/Heap
- Kenngrößen, Leistungsdaten, Funktionsumfang, z.B. BIOS, UEFI, CPU, RAM, Datenspeicher, RAID, Dateisysteme, Grafikkarte, Netzwerkkarte, Router, Switch, LWL, Ethernet-Standards, WLAN-Standards
  - RAM: Dual Channel
- Speichermedien
  - Magnetisch (Festplatten, HDD, Band),
  - Elektrisch (SDD)
  - Optisch (CD, DVD, BluRay)
- Schnittstellen
  - USB, Bluetooth, Firewire
  - DIE, SATA, iSCSI, SAS
  - Video-Schnittstellen: VGA, DVI, HDMI, DisplayPort, übliche Auflösungen, z.B. HD, UHD, 4K, 8K
  - Single-/Multimode Fasers
- Geräteklassen, z.B. Desktops, Notebooks/Laptops, Tablets, Smartphones, Convertible
- Mobile und stationäre Arbeitsplatzsysteme wie PC, Terminals, LAN, WLAN, Dockingstation, Thin Client vs. Fat Client
- WLAN
  - Hotspot, Ad-Hoc, Repeater, Access Point
  - Sicherheit (WPA, WEP, MAC-Filter, WPS)
- Bussysteme, Storage etc.
  - Glasfaser, Fibre Channel, Host-Bus-Adapter
  - Eigenschaften/Unterscheidung/Vor-/Nachteile DAS, SAN und NAS
    - DAS, SAN und NAS: Grafik 1, Grafik 2
- Abkürzungen und Bedeutungen kennen: sATA, AGP, PCI, IDE, iSCSI, SAS, USB, RAID, USV, SSD
  - Veraltet: ISA, SCSI, IDE: Master/Slave, Jumper
- Arten von Druckern und Scannern
  - 3D-Drucker
- Monitore (-arten)
  - VGA, DVI, HDMI, DisplayPort
- USV nach IEC 62040-3: VFI, VI, VFD
  - Mögliche Probleme bei der Stromversorgung: Stromausfall, Über-/Unterspannung, Frequenzabweichung etc.
  - Standby-, Offline-, Online-USV
  - Typen von USVen (z.B. VFI) nach DIN EN 62040-3
    - Voltage Independent, Voltage and Frequency Dependent, Voltage and Frequency Independent
  - Benötigte Scheinleistung für vorgegebene Hardware ermitteln
  - Netzstörung, vor denen USVen schützen
- Bootvorgang eines Computers
  - S.M.A.R.T.
  - P.O.S.T.
  - Bootsektor, Boot Loader
- Barrierefreiheit, z.B. Arbeitsplatz mit zweitem Monitor ausstatten, Lautsprecher/Mikrofon zur Verfügung stellen
- Hot Swapping, Hot Spare erläutern
- Vor-/Nachteile von SSDs
- Power over Ethernet (PoE)
- BYOD
- Elektrotechnik

- Energiegrößen, Wirkungsgrad
- Strom, Spannung, Wirkleistung (P = U * I)
- Leistungsaufnahme (W = P * t)

- Green IT, Energy Star, Recycling, Nachhaltigkeit
- Barcodes, QR-Codes, RFID
  - Asset Tag vs. Service Tag
- Ergonomierichtlinien, Arbeitsstättenverordnung
  - Vorgaben bzgl. Arbeitsplatzergonomie kennen
  - ergonomische Anforderungen an Bildschirme, Drucker, Stühle, Tische, Temperatur, Lichtverhältnisse, Peripherie
  - Nutzen ergonomischer Arbeitsplätze für das Unternehmen

II) Betriebssysteme

- Typen von Multitasking erläutern (kooperativ vs. Präemptiv)
- Prozess vs. Task vs. Thread
- Verschiedene Betriebssysteme kennen (Linux, Windows, Android, iOS, Windows Phone)
- Unterchied Unix/Linux
- Vor-/Nachteile Linux/Windows
  - Dateisysteme (FAT, NTFS, ext)
  - Aufbau des Dateibaums
  - Kommandozeile vs. GUI
- Linux
  - Arbeiten mit der Kommandozeile, Befehlssyntax, Parameter
  - Wichtige Befehle kennen (ls, chmod, chown, ps, grep, mount)
  - Wichtige Verzeichnisse kennen (bin, boot, dev, etc, home, lib, root, sbin, var)
  - Dateirechtesystem erklären (ugw, rwx)
  - Gängige Linux-Distributionen nennen (Debian, Suse, Red Hat, Ubuntu etc.)
  - Wie wird die Hardware angesteuert?
  - Mounten von Laufwerken
- Konsolenbefehle für Dateioperationen und Netzwerktroubleshooting/Namensauflösung
  - Dir, ls, mkdir, alias, del, cp, copy, chmod
  - Ipconfig, ifconfig, getmac, iprouteZ, arp, ping, traceroute, tracert, nslookup, netsh

III) Multimedia und Berechnungen

- Kompression
  - Verlustbehaftet vs. Verlustfrei
    - ZIP
    - Huffman-Code
- Datenraten von verschiedenen Laufwerken: Festplatte (HDD/SSD), CD, DVD, BluRay
- Audiobearbeitung
  - Sampling (-rate, -tiefe)
  - MP3
- Bildbearbeitung
  - Unterschied Raster-/Vektorgrafik
  - Auflösung
  - GIF, JPG/JPEG, TIF, PNG, SVG, MPEG
  - OCR
- Video
  - HD/UltraHD/4k
  - 3D-/HD-TV, BluRay
  - Kompressionsverfahren
- Zeichensätze kennen und Unterschiede aufzeigen
  - ASCII, Unicode, UTF-8 kennen und erklären
- Sinn von Prüfziffern (z.B. EAN, IBAN)

- Längs-/Querparität berechnen
- Mögliche Aufgaben
  - Dateigrößen von Bildern/Audio/Videos berechnen

D) Thema 4: Netzwerke

I) Netzwerktechnik

- Netzwerkkomponenten, z.B. Router, Switch, Access-Point
- Netzwerkhardware (Hub, Bridge, Switch, Router) mit Zuordnung zu ISO-Schichten
  - Switches/Hubs unterscheiden
- Netzwerkprotokolle, z.B. OSI-Modell, DNS, SMB, NFS, SMTP/S, IMAP/S, POP3/S, HTTP/S, IPSEC, IP, TCP, UDP, SSH, DHCP, ARP, TLS, SNMP, LDAP
- ISO/OSI-Modell (7-Schichten) im Vergleich zum TCP/IP-Modell (4 Schichten)
- TCP vs. UDP
  - TCP-Handshake, 3-Way-Handshake
- CSMA/CD, Token
- VLAN
  - statisch/dynamisch, tagged/untagged
- Client/Server vs. P2P
  - File Sharing
- IP-Adressen (IPv4, IPv6)
  - Unterschiede und Vor-/Nachteile von IPv4 vs. IPv6
  - Subnetting, Netzwerkmaske, Broadcast
  - APIPA, SAA (Stateless Address Autoconfiguration)
  - Link-Local-Unicast, Unique Local Unicast, Multicast, Global Unicast
- PoE vs. dLAN
- Quality of Service (QoS)
  - VoIP, SIP
- Server-/Desktop-/Anwendungsvirtualisierung
  - mögliche Arten der Virtualisierung:
    - Hypervisor (Typ 1/2)
    - Bare-Metal
    - Hosted
  - VDI, DaaS
  - Hardwareunterstützung
  - Vor-/Nachteile der einzelnen Verfahren
  - Serverkonsolidierung
- Container (z.B. Docker)
  - Unterschied zu VMs, Einsatzszenarien, Vor-/Nachteile
- Cloud Computing
  - Software as a Service, Infrastructure as a Service, Platform as a Service, Function as a Service
  - vs. On Premises
  - Clouds: Public, Private, Hybrid, Community, Virtual Private, Multi
  - Vorteile u.a.: Skalierbarkeit, Lastverteilung, Ausfallsicherheit
- Internetzugang: DSL (ADSL, VDSL, SDLS), LTE, 5G, UMTS, HSDPA, Edge
  - Datenraten, Technik
- Methoden zur Namensauflösung erklären (DNS, hosts)
  - DNS-Konfiguration
  - DNS-Einträge: A, AAAA, NS, PTR, MX, SOA, CNAME
- DNS, DHCP, WINS, ARP, Subnetting, Topologien
  - Ablauf beim DHCP-Lease (Discover -> Offer -> Request -> Acknowledge)
  - ping (ICMP)
  - MAC vs. IP
- IPv4, IPv6, A/B/C-Klassennetze

  - öffentliche/private IP-Adressen
- Protokolle mit Port-Nummern (HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, SMB, Telnet, SSH)
- Unterschiede IMAP/POP3, SMTP
- Routing
- Firewall
  - Packet Inspection, Port-Forwarding
- FDDI (Lichtwelle)/Ethernet beschreiben
- RDP/ICA/VNC grob unterscheiden

II) Internet

- Aufbau von URL/URI/URN
  - Schema, Benutzer/Passwort, Domain, Pfad, Query, Fragment etc.
- Beispiele für Browser/Webserver/Web-Programmiersprachen/(serverseitige) Scriptsprachen
- Wichtige Protokolle und Ports (HTTP, FTP, SMTP, POP3, IMAP, Telnet, SMB, SSH, NTP)
- Vor-/Nachteile wichtiger Dateiformate (PDF, Bildformate)
- Ablauf beim Aufruf einer Webseite (Kommunikation Client/Server) und Verarbeitung bei PHP
- Grundlegende Kenntnisse von HTML, CSS, PHP
- Responsive Webdesign (mit HTML5 + CSS3)
- Ergonomische Gestaltung von Websites
- Content Management System (CMS)
- Mindestinhalte des Impressums
- Virtuelle Hosts erläutern
- Möglichkeiten zur Unterscheidung von Websites auf einem Host: IP, Hostname, Port
- Funktion von .htaccess erläutern
- JavaScript
  - jQuery und andere Frameworks
- HTML5, CSS3
  - Audio-/Videoeinbettung/-unterstützung

E) Thema 5: Softwarekomponenten

I) Software

- Einteilung und Klassifikation von Anwendungssystemen
  - ERP, CMS, CRM, PSP, CAD, CASE, ECM, DMS, OMS
  - Anwendungssoftware
  - Betriebssysteme
  - Integrierte Entwicklungsumgebung (IDE)
  - Standard- vs. Individualsoftware
  - Branchensoftware
  - Open Source vs. proprietäre Software
  - Benutzeroberfläche
  - Datenbanksysteme
  - Kommunikationssysteme
  - OEM-Software
- Qualitätsmerkmale
  - Anpassbarkeit, Wartbarkeit
  - Schnittstellen, Interoperabilität
  - Kompatibilität
- Intuitive Bedienung
- Bestimmungen der Barrierefreiheit bei der Auswahl sowie der Einrichtung moderner Informations- und Kommunikationstechnik (Hard- und Software) berücksichtigen
  - Einfache Sprache
  - Braille
  - Spracheingabe- und -ausgabe

- Normen, Vorschriften, Zertifikate, Kennzeichnungen
- Installation und Einrichtung von Systemen, z.B. Betriebssysteme, BIOS, UEFI, Partitionierung/Formatierung, Netzwerkanbindungen, IP-Konfiguration, Remotedesktop (RDP, ICA)
- Lizenzarten, z.B. EULA, OEM, GNU
  - Pay by Use
- Konfiguration, Test, Troubleshooting und Dokumentation von Netzwerkverbindungen, z.B. IP-Adressen, DHCP, WLAN-Zugang, Pre shared key/Enterprise
  - VPN: End-to-End, Site-to-Site, End-to-Site
  - L2TP, IPsec
- Bestimmungen zur IT-Sicherheit (IT-Security) bei allen eingesetzten Hardware- und Softwaresystemen bzw. Infrastrukturen für eine Sicherheit der Informationsverarbeitung und auch der Kommunikation (Daten- bzw. Informationssicherheit) kennen und einhalten
- Basiswissen IT-Servicemanagement und darin verwendeter Methoden und Verfahren, z.B.:
  - ITIL
  - CobiT
  - MOF
  - ISO 20000
- Client-Server-Modell

II) SOFTWAREENTWICKLUNG

- Nötige Kenntnisse
  - Vor- und Nachteile verschiedener Programmierparadigmen kennen und Programmiersprachen nach Sprachhöhe unterscheiden
  - Identifikation und Auswahl einer für das jeweilige Realweltproblem" passenden Sprache
  - Softwareentwicklung und Anpassung von Software
  - Basiswissen Softwarelogik und grundlegende Programmelemente
  - Darstellungsformen für Programmabläufe
  - Aussagenlogik
  - Programmstrukturen
  - Algorithmen
  - Compiler, Linker, Interpreter
  - Prozedurale und objektorientierte Herangehensweise
  - Variablen, Datentypen und -strukturen, Zuweisungen
    - primitive Datentypen: byte, short, int, long, float, double, boolean, char
  - Kontrollstrukturen, z.B. Verzweigung, Schleife
  - Prozeduren, Funktionen
  - Objekte, Klassen, Methoden, Attribute
  - Vererbung, Polymorphie
  - Bibliotheken, Frameworks o Skriptsprachen, z.B. Shell-Skript, Macros
  - Debugging, formale und inhaltliche Fehler
- Abbildung der Kontrollstrukturen mittels Struktogramm (Nassi-Shneiderman), PAP oder Pseudocode als didaktisches Hilfsmittel
  - Verzweigungen (if, switch), Wiederholungen (kopf-/fußgesteuert)
- UML: Use Cases, Klassendiagramm
  - Komposition, Aggregation, Assoziation
- Entwurf der Bildschirmausgabemasken (Softwareergonomie, Barrierefreiheit)
  - Mockup, Wireframe
- Anforderungen: funktionale und nicht-funktionale Anforderungen
- Datenbanken
  - Stammdaten und Bewegungsdaten
  - Aufgaben eines DBMS
  - Einfache ER-Modelle mit Entity-Relationship-Modell und Tabellenmodell erstellen
  - SQL: DDL, DOL, DML. TCL DQL

        - SELECT bezogen auf eine Tabelle (inkl. Klauseln wie WHERE, ORDER BY, GROUP BY)
        - Aggregatsfunktionen wie SUM, COUNT, AVG
    - Normalisierung

III) Qualitätssicherung

- Qualitätsbegriff nach ISO 9000
- Modelle und Standards einordnen, z.B.:
    - QS-Normen ISO 9000-9004
    - EFQM
    - (Six Sigma)
- Nutzen der QS-/QM-Systeme im betriebseigenen Umfeld steht hier im Vordergrund
    - an der ständigen Verbesserung des betriebseigenen QS-Systems mitarbeiten
    - Verbesserung der Prozessqualität, der Arbeitsqualität und damit der Produkt- und Dienstleistungsqualität (Stichwort: prozessorientiertes QM-System)
    - vorrangiges Ziel ist die Sicherstellung der vorgegebenen Qualität, ein höherwertiges Ergebnis ist nicht das primäre Ziel
- Zertifizierung, Audit
- Qualitätsplanung, Qualitätsziele (Ist-Zustand ermitteln und Ziel-Zustand festlegen)
- Qualitätslenkung (Umsetzung der Planphase)
- PDCA - Plan, Do, Check, Act als Qualitätsmanagementzyklus
- Kriterien der Softwarequalität: Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Änderbarkeit, Übertragbarkeit
- Siegel: Geprüfte Sicherheit, Blauer Engel
- Testverfahren
    - Black- und White-Box-Test
    - Komponenten-/Modul-/Unit-Tests vs. Integrationstests vs. Systemtests
    - Abnahmetest
    - Lasttest

F) Thema 6: ITS

I) IT-Sicherheit

- Nötige Kenntnisse
    - Nutzen und stetes Anwenden der betriebseigenen Regelungen zur IT-Sicherheit und den Datenschutz
    - Anwenden des organisationsinternen Prozesses zur Gewährleistung der IT-Sicherheit und des Datenschutzes (IT-Sicherheitsmanagement)
- Schutzziele: Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit
- Maßnahmen zur Informationssicherheit
    - Organisatorische Maßnahmen, z.B. IT-Sicherheitsbeauftragter im Betrieb, Erstellung einer IT-Sicherheitsrichtlinie, z.B. Passwort-Policy
    - Technische Maßnahmen, z.B. Virenschutzsystem, Firewall, Anti-Spam
    - Personelle Maßnahmen, Sicherheitsbewusstsein herstellen
    - Passwörter, PINs, TANs, Captchas erklären und Komplexität/Sicherheit berechnen
- Normen und Branchenstandards zur Informationssicherheit, z.B.
    - ISO 27001
    - ISO 27002
    - BSI IT-Grundschutz
- (Anwenden von Vorschriften), z.B.:
    - Basel II und III
    - SOX
- Schutzbedarfsanalyse nach BSI IT-Grundschutz für
    - Anwendungen
    - IT-Systeme
    - Räume

- Kommunikationsverbindungen
- Anwenden von Evaluierungstechniken zur IT-Sicherheit (IT-Grundschutz-Handbuch)
- Schutzbedarfskategorien (normal, hoch, sehr hoch)
  - Erreichen des mittleren, angemessenen und ausreichenden Schutzniveaus, für ID-Systeme durch technische Sicherheitsmaßnahmen und infrastrukturelle, organisatorische und personelle Schutzmaßnahmen
- IT-Sicherheitsmanagementsystem implementieren
  - Betrieblicher IT-Sicherheitsbeauftragter
  - Schaffung eines Sicherheitsbewusstseins bei den Mitarbeitern
  - IT-Sicherheitsmanagement
  - Durch technische, infrastrukturelle, organisatorische und personelle Schutzmaßnahmen
  - Verhindern oder Abwehr von Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes, z.B. durch Etablierung eines IT-Sicherheitsmanagements (ISMS) unter Verwendung von Standards wie IT-Grundschutz, ISO/IEC 27001
- Security by Design, Security by Default
- Datensicherung/Backup-Verfahren
  - Wie erkennt die Software, welche Daten zu sichern sind?
  - Inkrementelles, differenzielles und Vollbackup
  - Generationenprinzip bzw. Großvater/Vater/Sohn
  - Medien nennen und erläutern
    - Kriterien bei der Auswahl von Backupmedien: Lebensdauer, Zugriffsgeschwindigkeit, Kosten, Störanfälligkeit, Kapazität
  - Hot/Cold Backup
  - Was sind sicherungswürdige Daten?
  - Mögliche Gründe für Datenverluste auf Servern erläutern und Gegenmaßnahmen vorschlagen
  - Folgen von Datenverlust, Auswirkungen von Datenverlusten für das Unternehmen erläutern
  - Maßnahmen der Mitarbeiter zur Vermeidung von Datenverlusten erläutern
- Verschrottung von Datenträgern
- Sicherung der Verfügbarkeit, z.B. RAID-Systeme, SAN
  - RAID 0, 1, 5, 6, 01, 10, JBOD erklären
  - Nested RAID levels
- Zugangs- und Zugriffskontrolle
- Grundbegriffe
  - Schadprogramme: Viren, Würmer
  - Rootkits, Botnetze, Trojaner, Malware, Ransomware, Spyware, Adware, Scareware, Hoax, Dialer (veraltet), Keylogger
    - Verbreitung von Viren/Würmer/Trojaner erläutern
  - Hacker (White Hat, Black Hat), Cracker, Script-Kiddies
  - Spam, Phishing, Sniffing, Spoofing, Man-in-the-Middle
  - SQL-Injection, XSS, CSRF, Session Hijacking, DoS, DDoS
  - Backdoor, Exploit, 0-Day-Exploit, Rootkit
- Kryptographie
  - Verschlüsselungstechniken, symmetrische und asymmetrische Verschlüsselung
  - Hashverfahren
  - Cas, Zertifikate, Digitale Signaturen, PKI
  - Techniken wie HTTPS, TLS
- SSH vs. Telnet
- WLAN
  - SSID, Mac-Filter, WPS, Wi-Fi Easy Connect
  - Sicherheitsmethoden: WEP, WPA 1/2/3 (PSK, Enterprise), RADIUS
  - Verschlüsselungsstandards: AES, TKIP, SAE
- Endpoint-Security
  - Virenscanner, Firewall, Application Control, Datenträgerverschlüsselung

- Arten und Funktionsweise von Firewalls
  - Packet Filter, Stateful Packet Inspection, Application Firewall, WAF
- Sinn und Aufbau einer DMZ
  - Port-Forwarding erklären
- Authentifizierung vs. Autorisierung
  - MFA
  - Passwort-Policy

II) Datenschutz

- Datenschutzgesetze – national und auf EU-Ebene, z.B. DSGVO, BDSG
  - Definition von personenbezogenen Daten
  - Maßnahmen des Datenschutzes: Datensparsamkeit, Zweckbindung usw.
  - Betroffenenrechte: Auskunftsrecht, Recht auf Löschung etc.
- Grundsätze des Datenschutzes
  - Gesetzmäßigkeit (Erfordernis der gesetzlichen Grundlage)
  - Verhältnismäßigkeit (Datensparsamkeit und Datenvermeidung (§3a BDSG))
  - Zweckbindung
  - Richtigkeit/Integrität
  - Transparenz gegenüber den betroffenen Personen
  - Informationssicherheit
- Persönlichkeitsrechte
  - Recht am eigenen Bild

4) Dokumentation

A) Projekte

I) Projektmanagement

II) Methoden und Modelle

III) Teamarbeit

IV) Changemanagement

B) Wirtschaftslehre / Sozialkunde

I) Wirtschaftlichkeit

II) Märkte und Bedarf

III) Verträge

IV) Kundenberatung/Präsentieren

V) Marketing

VI) Angebotsvergleich

VII) Leistungserbringung

C) Hardwarekomponenten

I) Hardware

- Nötige Kenntnisse
  - Funktionale, ökonomische, ökologische, soziale Aspekte bewerten
  - Installation und Konfiguration der Hardware
- Hardwareprodukte, z.B. CPU, Motherboard, Speicher, Datenspeicher, Netzteile, Grafikkarte, Peripheriegeräte, Netzwerkkomponenten, WLAN
  - Ein-/Ausgabegeräte: Drucker, Scanner, Maus, Display, Touchpad, Tastatur
  - Arten von Scannern: Flachbett, Handscanner, Trommelscanner, Dokumentenscanner
  - Arten von Druckern: Tintenstrahl, Laser, Thermo, Nadel
- Prozessor/CPU, Kühlung
  - Von-Neumann-Architektur

- ALU
- Latency Numbers Every Programmer Should Know

- RAM-Arten und Unterschiede
  - Unterschiede Stack/Heap
- Kenngrößen, Leistungsdaten, Funktionsumfang, z.B. BIOS, UEFI, CPU, RAM, Datenspeicher, RAID, Dateisysteme, Grafikkarte, Netzwerkkarte, Router, Switch, LWL, Ethernet-Standards, WLAN-Standards
  - RAM: Dual Channel
- Speichermedien
  - Magnetisch (Festplatten, HDD, Band)
  - Elektrisch (SDD)
  - Optisch (CD, DVD, BluRay)
- Schnittstellen
  - USB, Bluetooth, Firewire
  - DIE, SATA, iSCSI, SAS
  - Video-Schnittstellen: VGA, DVI, HDMI, DisplayPort, übliche Auflösungen, z.B. HD, UHD, 4K, 8K
  - Single-/Multimode Fasers
- Geräteklassen, z.B. Desktops, Notebooks/Laptops, Tablets, Smartphones, Convertible
- Mobile und stationäre Arbeitsplatzsysteme wie PC, Terminals, LAN, WLAN, Dockingstation, Thin Client vs. Fat Client
- WLAN
  - Hotspot, Ad-Hoc, Repeater, Access Point
  - Sicherheit (WPA, WEP, MAC-Filter, WPS)
- Bussysteme, Storage etc.
  - Glasfaser, Fibre Channel, Host-Bus-Adapter
  - Eigenschaften/Unterscheidung/Vor-/Nachteile DAS, SAN und NAS
    - DAS, SAN und NAS: Grafik 1, Grafik 2
- Abkürzungen und Bedeutungen kennen: sATA, AGP, PCI, IDE, iSCSI, SAS, USB, RAID, USV, SSD
  - Veraltet: ISA, SCSI, IDE: Master/Slave, Jumper
- Arten von Druckern und Scannern
  - 3D-Drucker
- Monitore (-arten)
  - VGA, DVI, HDMI, DisplayPort
- USV nach IEC 62040-3: VFI, VI, VFD
  - Mögliche Probleme bei der Stromversorgung: Stromausfall, Über-/Unterspannung, Frequenzabweichung etc.
  - Standby-, Offline-, Online-USV
  - Typen von USVen (z.B. VFI) nach DIN EN 62040-3
    - Voltage Independent, Voltage and Frequency Dependent, Voltage and Frequency Independent
  - Benötigte Scheinleistung für vorgegebene Hardware ermitteln
  - Netzstörung, vor denen USVen schützen
- Bootvorgang eines Computers
  - S.M.A.R.T.
  - P.O.S.T.
  - Bootsektor, Boot Loader
- Barrierefreiheit, z.B. Arbeitsplatz mit zweitem Monitor ausstatten, Lautsprecher/Mikrofon zur Verfügung stellen
- Hot Swapping, Hot Spare erläutern
- Vor-/Nachteile von SSDs
- Power over Ethernet (PoE)

BYOD alias bring your own Device ist ein Verfahren eines Betriebes welches den Mitarbeitern ermöglicht ihre eigenen Endgeräte (Notebooks, Tablets, etc.) mit in den Betrieb zu nehmen und mit ihren eigenen Geräten ihr Tagesgeschäft zu erledigen.

- Elektrotechnik
  - Energiegrößen, Wirkungsgrad
  - Strom, Spannung, Wirkleistung (P = U * I)
  - Leistungsaufnahme (W = P * t)
- Green IT, Energy Star, Recycling, Nachhaltigkeit
- Barcodes, QR-Codes, RFID
  - Asset Tag vs. Service Tag
- Ergonomierichtlinien, Arbeitsstättenverordnung
  - Vorgaben bzgl. Arbeitsplatzergonomie kennen
  - ergonomische Anforderungen an Bildschirme, Drucker, Stühle, Tische, Temperatur, Lichtverhältnisse, Peripherie
  - Nutzen ergonomischer Arbeitsplätze für das Unternehmen

II) Betriebssysteme

- Typen von Multitasking erläutern (kooperativ vs. Präemptiv)
- Prozess vs. Task vs. Thread
- Verschiedene Betriebssysteme kennen (Linux, Windows, Android, iOS, Windows Phone)
- Unterchied Unix/Linux
- Vor-/Nachteile Linux/Windows
  - Dateisysteme (FAT, NTFS, ext)
  - Aufbau des Dateibaums
  - Kommandozeile vs. GUI
- Linux
  - Arbeiten mit der Kommandozeile, Befehlssyntax, Parameter
  - Wichtige Befehle kennen (ls, chmod, chown, ps, grep, mount)
  - Wichtige Verzeichnisse kennen (bin, boot, dev, etc, home, lib, root, sbin, var)
  - Dateirechtesystem erklären (ugw, rwx)
  - Gängige Linux-Distributionen nennen (Debian, Suse, Red Hat, Ubuntu etc.)
  - Wie wird die Hardware angesteuert?
  - Mounten von Laufwerken
- Konsolenbefehle für Dateioperationen und Netzwerktroubleshooting/Namensauflösung
  - Dir, ls, mkdir, alias, del, cp, copy, chmod
  - ipconfig, ifconfig, getmac, iprouteZ, arp, ping, traceroute, tracert, nslookup, netsh

III) Multimedia und Berechnungen

- Kompression
  - Verlustbehaftet vs. Verlustfrei
    - ZIP
    - Huffman-Code
- Datenraten von verschiedenen Laufwerken: Festplatte (HDD/SSD), CD, DVD, BluRay
- Audiobearbeitung
  - Sampling (-rate, -tiefe)
  - MP3
- Bildbearbeitung
  - Unterschied Raster-/Vektorgrafik
  - Auflösung
  - GIF, JPG/JPEG, TIF, PNG, SVG, MPEG
  - OCR

- Video
  - HD/UltraHD/4k
  - 3D-/HD-TV, BluRay
  - Kompressionsverfahren
- Zeichensätze kennen und Unterschiede aufzeigen
  - ASCII, Unicode, UTF-8 kennen und erklären
- Sinn von Prüfziffern (z.B. EAN, IBAN)
  - Längs-/Querparität berechnen
- Mögliche Aufgaben
  - Dateigrößen von Bildern/Audio/Videos berechnen

D) NETZWERKE

I) NETZWERKTECHNIK

Zum Übertragen von Daten innerhalb eines Netzwerkes benötigt man diverse **Netzwerkkomponenten**. Innerhalb eines lokalen Netzwerkes, in dem alle Geräte über ein Netzwerkkabel kommunizieren ist ein Switch ausreichend. Der **Switch** arbeitet auf Layer 2 des ISO/OSI-Modelles und verwaltet die Übertragung entsprechend anhand der MAC-Adressen der Geräte. Will man nun drahtlose Geräte hinzufügen, benötigt man ebenfalls einen Access Point, der **Access-Point** wird an den Switch angeschlossen und sendet/empfängt die Daten auch anhand seiner MAC-Adresse. Zusätzlich hat er eine MAC-Adressliste von allen Geräten, die mit ihm verbunden sind, um die Daten auch an das richtige Endgerät weiterzuleiten. Nun wenn du außerhalb deines lokalen Netzwerks kommunizieren möchtest, braucht man dann noch zusätzlich einen **Router**. Dieser wird ebenfalls an den Switch angeschlossen, aber er arbeitet anders als die vorher besprochenen Netzwerkkomponenten, denn er arbeitet auf Layer 3 des ISO/OSI-Modelles. Das heißt er besitzt auch eine MAC-Adresse, damit der Switch Daten an ihn senden kann, aber er selbst leitet diese Daten über IP-Adressen weiter.

Ein **Hub** arbeitet auf Layer 1 des ISO/OSI-Modelles, er empfängt Datenströme und wiederholt diese an allen angeschlossenen Ports, ohne den Datenverkehr zu analysieren oder zu filtern und somit keine getrennte Bandbreite sowie Kollisionsdomänen ermöglicht. **Bridges und Switches** arbeiten gemeinsam auf Layer 2 des ISO/OSI-Modelles. Das bedeutet sie sendet Daten anhand der MAC-Adressen, die sie in einer Geräteliste gespeichert haben und übertragen Daten somit an den richtigen Zielport. Dies ermöglicht die getrennte Bandbreite und Ausführung von Kollisionsdomänen. Ein Router arbeitet auf Layer 3 des ISO/OSI-Modelles und dient zur Datenübertragung zwischen verschiedenen Netzwerken. Er nutzt zur Datenübertragung IP-Adressen, die er in einer Routing-Tabelle gespeichert hat.

- **OSI-Modell:** Modell zur Einteilung von Netzwerkkommunikation in sieben differenzierte Ebenen: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer
- **DNS:** Domain Name System → Protokoll zur Auflösung von les- und schreibbaren Namen in die IP-Adressen der zugehörigen Server
- **SMB:** Server Message Block → Protokoll zur Dateifreigabe im Netzwerk.
- **NFS:** Network File System → Protokoll zur Zugriffskontrolle für Dateien in einem Netzwerk. Dateizugriff anders als FTP, weil Dateien direkt auf dem Server angezeigt oder geändert werden ohne vorherigen Download.
- **SMTP/S:** Simple Mail Transfer Protocol / Secure → Protokoll zum übertragen von E-Mails. Secure steht dann für eine verschlüsselte Verbindung durch SSL/TLS
- **IMAP/S:** Internet-Mail Access Protocol / Secure → Protokoll zum Anzeigen und Verwalten von E-Mails auf dem Mail-Server. Secure steht dann für eine verschlüsselte Verbindung durch SSL/TLS

- **POP3/S:** Post Office Protocol 3 / Secure → Protokoll zum Herunterladen von E-Mails vom Mail-Server zur Anzeige und Verwaltung von E-Mails im lokalen Mail-Programm. Secure steht dann für eine verschlüsselte Verbindung durch SSL/TLS
- **HTTP/S:** Hyper Text Transfer Protocol / Secure → Protokoll zur Übertragung von Inhalten im „World Wide Web“. Secure steht dann für eine verschlüsselte Verbindung durch SSL/TLS
- **IPsec:** Internet Protocol Secure → Protokoll für die globale Netzwerkkommunikation über IP-Adressen.
- **IP:** Internet Protocol → Protokoll für die globale Netzwerkkommunikation über IP-Adressen.
- **TCP:** Transfer Control Protocol → Protokoll für die Datenübertragung mit blockierenden Zugriff. Dieses Protokoll nutzt einen 3-Way-Handshake zur Sicherstellung, dass alle Daten komplett und in richtiger Reihenfolge gesendet werden. → Formularübertragung, Dateitransfer, etc.
- **UDP:** User Datagram Protocol → Protokoll für die Dateiübertragung ohne blockierenden Zugriff. Dieses Protokoll nutzt keinen Handshake, sondern überträgt Daten ohne Überprüfung der Vollständigkeit und Reihenfolge. → Streaming von Inhalten
- **SSH:** Secure Shell → Protokoll für den gesicherten Zugang zu anderen Netzwerkgeräten wie Netzwerkkomponenten, Endgeräte im Netzwerk, etc. Gesichert wird der Zugang durch einen asynchronen Verschlüsselungsalgorithmus.
- **DHCP:** Dynamic Host Configuration Protocol → Protokoll zur automatischen Zuweisung von IP-Adressen an die Endgeräte
- **ARP:** Address Resolution Protocol → Protokoll zur Auflösung von IP-Adressen in die les- und schreibbaren Namen der zugehörigen Server
- **TLS:** Transport Layer Security → Protokoll zur Verschlüsselung von Datenverkehr im Netzwerk oder Fremdnetzwerke. End-To-End Verschlüsselung. Gesichert wird der Zugang durch einen asynchronen Verschlüsselungsalgorithmus.
- **SNMP:** Simple Network Management Protocol → Protokoll zum Monitoring, Verwalten und Konfigurieren von Netzwerkgeräten
- **LDAP:** Lightweight Directory Access Protocol → Protokoll zur Speicherung von Daten im „LDAP“-Verzeichnis und Zugriffskontrolle auf das Verzeichnis mit Nutzer-Authentifizierung

ISO/OSI-Modell	TCP/IP-Modell
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Access Layer
Physical Layer	

TABELLE 1 ISO/OSI GEGEN TCP/IP-MODELL

TCP nutzt zur Gewährleistung eines zuverlässigen Datenaustauschs den TCP-Handshake oder besser bekannt als 3-Way-Handshake, der dazu dient, eine konstante Verbindung zwischen Sender und Empfänger zu sichern.

- Schritt 1 (SYN):
  - Der Client sendet ein SYN (Synchronize)-Paket an den Server, um eine Verbindung anzufordern.
- Schritt 2 (SYN-ACK):
  - Der Server antwortet mit einem SYN-ACK (Synchronize-Acknowledge) -Paket, um die Anforderung zu akzeptieren und die Verbindung zu bestätigen.
- Schritt 3 (ACK):
  - Der Client sendet ein ACK (Acknowledge)-Paket als Bestätigung an den Server.

UDP nutzt keine konstante Verbindung. Die Datenübertragung bei UDP funktioniert folgendermaßen:

- Sender sendet UDP-Paket:
  - Der Sender erstellt ein UDP-Paket und sendet es an die Zieladresse und den Zielport.

- Empfänger empfängt UDP-Paket:
  - Der Empfänger lauscht auf dem Zielport und empfängt die UDP-Pakete, die an diesen Port gesendet werden

CSMA/CD steht für Carrier Sense Multiple Access with Collision Detection und ist ein Zugriffsverfahren welchen in Ethernet-Netzwerken fungiert. Es dient, um Kollisionen in einem gemeinsam genutzten Medium zu erkennen und zu behandeln.

- Carrier Sense (**Trägerprüfung**): Ein Gerät lauscht auf dem Übertragungsmedium, um zu prüfen, ob es aktuell in Benutzung ist.
- Multiple Access (**Mehrzugriff**): Wenn das Medium frei ist, kann das Gerät versuchen, Daten zu senden. Wenn jedoch mehrere Geräte gleichzeitig senden, kann es zu einer Kollision kommen.
- Collision Detection (**Kollisionsdetektion**): Im Falle einer Kollision versucht jedes beteiligte Gerät, die Kollision zu erkennen. Sobald eine Kollision erkannt wird, stoppen die sendenden Geräte sofort die Übertragung und starten einen Backoff-Algorithmus, bevor sie erneut versuchen, Daten zu senden.

In einem **Token-basierten Netzwerk** wird ein "Token" als Kontrollmechanismus verwendet, um den Zugriff auf das Übertragungsmedium zu regeln. Nur das Gerät, das im Besitz des Tokens ist, hat die Berechtigung, Daten zu senden.

Der **Token** wird in einem **logischen Ring** durch das Netzwerk weitergegeben. Wenn ein Gerät Daten senden möchte, wartet es auf den Empfang des Tokens. Nach dem Senden der Daten gibt das Gerät den Token weiter, und das nächste Gerät in der Reihe hat dann die Berechtigung zum Senden.

VLANs (Virtual Local Area Networks) sind logische Netzwerke, die innerhalb eines physischen Netzwerks erstellt werden, um den Datenverkehr zu segmentieren. Sie erlauben es, verschiedene Gruppen von Geräten in separate, isolierte Netzwerke zu teilen, um Sicherheit und Leistung zu verbessern.

VLANs können statisch oder dynamisch konfiguriert sein. Statische VLANs erfordern manuelle Zuordnungen von Ports zu VLANs, während dynamische VLANs Ports basierend auf bestimmten Merkmalen wie der MAC-Adresse automatisch in VLANs organisieren.

Innerhalb von VLANs können Datenpakete markiert (tagged) oder unmarkiert (untagged) sein. Markierte Pakete enthalten zusätzliche Informationen im Datenpaket-Header, die es Switches ermöglichen, zu wissen, welchem VLAN sie gehören. Untagged Pakete enthalten keine spezifischen VLAN-Informationen und werden normalerweise verwendet, wenn der Datenverkehr innerhalb desselben VLANs bleibt.

Beim **Client/Server Prinzip** laden Nutzer ihre Daten auf einen Server hoch, damit andere Nutzer sie vom Server herunterladen können. Dies verhindert, dass der Client des Uploaders auf den Client des Downloaders zugreifen kann.

Beim **Peer-to-Peer** Prinzip, lädt sich der Downloader-Client die Daten direkt vom Uploader-Client, dabei besteht zwischen den beiden Clients eine direkte Verbindung.

- **IPv4**
  - Verwendet **32-Bit-Adressen**, was zu Adressknappheit führt. Es erfordert oft **NAT** für die Adressverteilung. IPv4 hat eine Fragmentierung auf Router-Ebene und benötigt **DHCP** für die Adresskonfiguration.
  - **Subnetting** ist die Praxis, ein großes Netzwerk in kleinere, logisch isolierte Netzwerkabschnitte (Subnetze) aufzuteilen. Mit dem Zweck, eine effiziente Nutzung von IP-Adressen, Organisieren von Netzwerken und Begrenzen der Rundsende-Domänen zu ermöglichen.
  - Die **Netzwerkmaske** definiert den Netzwerk- und Hostanteil einer IPv4-Adresse. Zum Beispiel: In der Form einer 32-Bit-Adresse (z. B. 255.255.255.0 für ein 24-Bit-Subnetz), wobei die 1er-Bits den Netzwerkanteil und die 0er-Bits den Hostanteil kennzeichnen.

- **Broadcasting** ist ein Paket, das an alle Geräte in einem Netzwerk gesendet wird. Zum Beispiel: Verwendung der speziellen Broadcast-Adresse (z. B. 192.168.1.255 in einem 24-Bit-Netzwerk), um Daten an alle Geräte im Netzwerk zu übertragen.
- **APIPA** ist eine Funktion in IPv4, die es einem Gerät ermöglicht, automatisch eine private IP-Adresse im 169.254.x.x-Bereich zuzuweisen, wenn kein DHCP-Server verfügbar ist. Es ermöglicht Geräten, eine vorübergehende IP-Adresse für die lokale Kommunikation zu erhalten.
- **Link-Local-Unicast** (IPv4): Dies sind IP-Adressen, die nur in einem bestimmten lokalen Netzwerksegment gültig sind. Sie werden für die Kommunikation innerhalb desselben Netzwerks verwendet, beispielsweise für Geräte im selben Subnetz. Ein bekanntes Beispiel für eine Link-Local-Unicast-Adresse in IPv4 ist die IPv4-Adresse im Bereich von 169.254.0.0/16, die bei der automatischen Adresszuweisung ohne DHCP zum Einsatz kommt (APIPA - Automatic Private IP Addressing).
- **Unique Local Unicast** (IPv4): Diese Art von Adresse ähnelt den IPv4-Adressen im privaten Adressbereich (wie z. B. 192.168.x.x oder 10.x.x.x), die für den privaten Gebrauch innerhalb eines Unternehmensnetzwerks oder privaten Netzwerks bestimmt sind. Unique Local Unicast-Adressen bieten eine Möglichkeit, Adressen zu nutzen, die global eindeutig sind und gleichzeitig für lokale Kommunikation innerhalb eines privaten Bereichs reserviert sind.

❖ **IPv6**

- Verwendet **128-Bit-Adressen**, die praktisch unbegrenzte Adressen bieten. IPv6 hat einen optimierten Header, unterstützt Autoconfiguration und eliminiert die Notwendigkeit von NAT.
- **Subnetting** wird durch Präfixe und Präfixlängen durchgeführt, um Netzwerke in kleinere Bereiche zu unterteilen.
- IPv6 verwendet **keine herkömmlichen Netzwerkmasken** wie IPv4. Die Netzwerkidentifikation erfolgt durch Präfixe und Präfixlängen.
- Es gibt **keine dedizierte Broadcast-Adresse** in IPv6. Multicast wird für ähnliche Funktionalitäten wie Broadcasting in IPv4 verwendet.
- **SAA** (Stateless Address Autoconfiguration) ist ein Merkmal von IPv6, das Geräten die automatische Konfiguration von IPv6-Adressen ohne die Notwendigkeit eines DHCP-Servers ermöglicht. Mit SAA können Geräte basierend auf ihrem Interface-Identifier und dem Präfix des lokalen Routers automatisch eine gültige IPv6-Adresse erhalten.
- **Link-Local-Unicast** (IPv6): Diese Art von Adresse ist ähnlich wie bei IPv4 und wird für die Kommunikation innerhalb desselben Netzwerksegments verwendet. IPv6-Link-Local-Adressen werden normalerweise automatisch generiert und haben einen speziellen Bereich (fe80::/10) und sind typischerweise auf ein einzelnes Netzwerksegment beschränkt.
- **Unique Local Unicast** (IPv6): Dies sind IPv6-Adressen, die für private oder lokale Kommunikation bestimmt sind und ähnlich wie bei IPv4 für den internen Gebrauch in Organisationen oder privaten Netzwerken verwendet werden. Im Gegensatz zu Global Unicast-Adressen sind sie nicht für das Routing im gesamten Internet bestimmt. Das spezielle Präfix für Unique Local Unicast-Adressen ist fc00::/7.
- **Global Unicast** (IPv6): Dies sind die IPv6-Adressen, die global im gesamten Internet eindeutig sind. Sie ermöglichen die Kommunikation zwischen Geräten über das Internet und sind für das Routing im globalen Internet bestimmt. Global Unicast-Adressen haben normalerweise eindeutige Präfixe und Identifikatoren, die eine weltweite Eindeutigkeit gewährleisten.

❖ **Gemeinsamkeit**

- Multicast (IPv6 und IPv4): Multicast-Adressen ermöglichen die Übertragung von Daten an eine Gruppe von Zielen. Geräte, die an einer bestimmten Multicast-Gruppe teilnehmen, können Datenpakete empfangen, die an diese spezielle Gruppenadresse gesendet werden. Multicast wird für Anwendungen wie Streaming-Medien, Online-Gaming und bestimmte Arten von Kommunikationsprotokollen verwendet.

PoE ermöglicht es, angeschlossene Geräte über das Ethernet-Kabel mit Strom zu versorgen. Dies ist nützlich für verschiedene Geräte, die über das Netzwerkkabel mit Daten verbunden sind, wie beispielsweise IP-Telefone,

Überwachungskameras oder WLAN-Zugangspunkte. Es vereinfacht die Installation, da separate Stromkabel vermieden werden können. PoE kann auch für Geräte genutzt werden, die nicht ständig in Betrieb sind, aber trotzdem über das Netzwerk angesprochen werden müssen.

dLAN nutzt das vorhandene Stromnetz im Gebäude, um Daten zwischen verschiedenen Adaptern zu übertragen. Ein Adapter wird an eine Steckdose angeschlossen und über ein Ethernet-Kabel mit dem DSL-Modem oder Router verbunden. Andere Adapter, die in Steckdosen an verschiedenen Orten im Gebäude eingesteckt sind, können dann über Ethernet-Kabel mit Endgeräten wie Computern oder Smart-TVs verbunden werden. Diese Methode nutzt die Stromleitung des Gebäudes, um Daten zu übertragen, und kann praktisch sein, wenn das Verlegen von Netzwerkkabeln schwierig ist oder WLAN nicht zuverlässig ist.

- **Quality of Service (QoS)**
  - **VoIP, SIP**
- **Server-/Desktop-/Anwendungsvirtualisierung**
  - **mögliche Arten der Virtualisierung:**
    - **Hypervisor (Typ 1/2)**
    - **Bare-Metal**
    - **Hosted**
  - **VDI, DaaS**
  - **Hardwareunterstützung**
  - **Vor-/Nachteile der einzelnen Verfahren**
  - **Serverkonsolidierung**
- **Container (z.B. Docker)**
  - **Unterschied zu VMs, Einsatzszenarien, Vor-/Nachteile**
- **Cloud Computing**
  - **Software as a Service, Infrastructure as a Service, Platform as a Service, Function as a Service**
  - **vs. On Premises**
  - **Clouds: Public, Private, Hybrid, Community, Virtual Private, Multi**
  - **Vorteile u.a.: Skalierbarkeit, Lastverteilung, Ausfallsicherheit**
- **Internetzugang: DSL (ADSL, VDSL, SDLS), LTE, 5G, UMTS, HSDPA, Edge**
  - **Datenraten, Technik**

Es gibt verschiedene Arten zur **Namensauflösung** in IP-Adressen, die erste Möglichkeit ist es über Eintragungen in der **hosts-Datei** auf seinem Endgerät, dort kann man direkt eine IP zu einem Host-Name zuweisen und dann auch direkt abrufen. Der Vorteil davon ist es, dass man auch ohne DNS-Server Zugang zu seinen Ressourcen behält und je nach Anwendungsfall auch den DNS-Server überschreiben kann, um mit „öffentlichen“ Domains auf seine privaten Ressourcen zuzugreifen. Jedoch werden Einträge nicht automatisch angepasst, wenn sich die IP-Adresse vom Server ändert.

Möglichkeit Nummer zwei wäre es, die Namensauflösung von einem **DNS-Resolver** durchführen zu lassen. Dabei werden die **DNS-Server** angesprochen. Ein DNS-Server, dient als öffentliche Ressource, in die alle Domain-Namen und die zugehörigen IP-Adressen eingetragen werden können. DNS-Server agieren pro Zone. Sprich jeder „.“ dient als Trennpunkt einer Zone

Hostname Subdomain Second-Level-Domain SLD Top-Level-Domain TLD Rootpunkt

Der Resolver durchläuft dann rekursiv jede Zone, um am Ende die richtige IP-Adresse aufzulösen. Der Vorteil dabei ist, die automatisierte Aktualisierung.

- A („Address“)
  - IPv4-Adresse
- AAAA
  - IPv6
- MX („MaileXchanger“)
  - Mailserver
- NS (Nameserver)
  - DNS-Server
- SOA (Start of Authority)
  - Informationen über die primäre Autorität für die Zone.
- CNAME (Canonical Name)
  - Alias-Eintrag mit Zuweisung auf andere Domains oder Hosts
- PTR (Pointer)
  - Verweist auf ein Objekt: den Domain-Namen. Dadurch wird das Reverse DNS (rDNS) bzw. ein Reverse Lookup möglich.

- **DNS, DHCP, WINS, ARP, Subnetting, Topologien**
  - **Ablauf beim DHCP-Lease (Discover -> Offer -> Request -> Acknowledge)**
  - **ping (ICMP)**
  - **MAC vs. IP**
- **IPv4, IPv6, A/B/C-Klassennetze**
  - **öffentliche/private IP-Adressen**

- **HTTP:** Hyper Text Transfer Protocol → Protokoll zur Übertragung von Inhalten im World Wide Web. Port 80
- **HTTPS:** Hyper Text Transfer Protocol Secure → Protokoll zur verschlüsselten Übertragung von Inhalten im World Wide Web. Port 443
- **FTP:** File Transfer Protocol → Protokoll zum Dateiaustausch mit einem Webserver. Port 20
- **SMTP:** Simple Mail Transfer Protocol → Protokoll für den Mail-Transfer. Port 587
- **POP3:** Post Office Protocol version 3 → Protokoll zum Mail-Transfer von einem Mailserver aufs lokale Gerät. Port 110
- **IMAP:** Internet Message Access Protocol → Protokoll zur E-Mail-Verwaltung auf einem Mailserver. Port 143
- **DNS:** Domain Name System → Protokoll zur Auflösung von les- und schreibbaren Namen in die IP-Adressen der zugehörigen Server. Port 53
- **SMB:** Server Message Block: → Protokoll zur Dateifreigabe im Netzwerk. Port 445
- **Telnet** → Protokoll zur Verbindung mit einer virtuellen Maschine. Port 23
- **SSH:** Secure Shell → Protokoll zur verschlüsselten Verbindung mit einer virtuellen Maschine. Port 22

IMAP ist für die E-Mail-Verwaltung auf einem Mailserver zuständig. Man meldet sich mit einem Mail-Client auf dem Server an und hat dann Zugang auf die Mails zum Lesen und Bearbeiten. Übertragen werden von dem Protokoll also nur die Information, was der Server mit der Mail tun soll oder was er dem Client anzeigen soll. Der Vorteil hiervon ist, die Synchronisation zwischen Mail-Client und Server.

POP3 ist für die E-Mail-Verwaltung auf dem lokalen Gerät. Das heißt, das Protokoll ist dafür zuständig die Maildaten von dem Server auf den lokalen Mail-Client herunterzuladen. Der Vorteil hiervon ist, dass man auch Zugang zu seinen Mails hat, während man Offline ist. Jedoch muss man jede Aktualisierung selbständig auf den Mailserver synchronisieren.

SMTP ist dann schließlich das Protokoll, was den E-Mail Transfer ausführt. Dieses Protokoll ist dafür zuständig, die Mail von einem Mail-Server zum nächsten zu senden.

Routing ist der Prozess, bei dem ein Router Datenpakete von einer Quelle zum Ziel in einem Netzwerk leitet. Der Router entscheidet, welchen Weg die Pakete nehmen, indem er Informationen in Routing-Tabellen verwendet, die er über bekannte Netzwerke und die besten Pfade zwischen ihnen hat. Diese Informationen werden durch Protokolle wie OSPF oder BGP aktualisiert. Der Router wählt dann den besten Pfad basierend auf Kriterien wie der kürzesten Route oder der geringsten Latenz, um die Pakete an ihr Ziel zu bringen.

Eine **Firewall** ist eine Sicherheitskomponente eines Netzwerkes. Es gibt diese In drei Ausführungen, z.B. Nummer eins im Betriebssystem des Endgerätes integriert. Von dort aus kann sie mit privilegierten Rechten über das eigene System scannen ob Programme versteckt Daten empfangen oder senden, sowie ein Register darüber führen welche Programme von der Firewall den Datenstrom verwehrt bekommen sollen. Nummer zwei ist dann als Zusatzsoftware von einem Anbieter, der sich auf Firewall Algorithmen spezialisiert hat, in der Regel erhält diese Software über den Installer ebenfalls privilegierte Rechte über das Endgerät und kann dort den gesicherten Netzwerkverkehr gewährleisten. Option drei ist zusätzlich eine Hardware-Firewall, die als externes Gerät den gesamten Netzwerkverkehr scannt und dort Geräteübergreifend die Sicherheit der Netzwerkkommunikation sicherstellt.

Eine Firewall kümmert sich um verschiedene Aufgaben zur Gewährleistung der Sicherheit wie zum Beispiel die „Packet Inspection“, diese Überprüft anhand des TCP-Handshakes oder anderer Verbindungsanfragen ob die gesendeten Pakete überhaupt angefragt wurden. Falls dies nicht der Fall ist, werden die Pakete einfach als ungültig markiert und verworfen.

Port-Forwarding ist eine Methode, um externen Benutzern Zugang zu Ressourcen in der DMZ zu ermöglichen. Der Vorgang sorgt dafür das Anfragen an die Netzadresse mit einem angegebenen Port an die entsprechende Ressource in der DMZ weitergeleitet werden. Beispiel: Netzadresse 16.32.64.128 → Anfrage auf 16.32.64.128:80 → Anfrage wird auf die interne IP-Adresse des Web-Servers weitergeleitet. So kann der externe Nutzer auf den Web-Server zugreifen, ohne direkt im Netzwerk verbunden zu sein.

Ein **FDDI-Netzwerk** besteht aus zwei Token Rings. Dabei ist ein Ring als Backup gedacht, falls der primäre ausfällt. Der primäre Ring liefert bis zu 100 Mbps. Wird der sekundäre Ring nicht als Backup benötigt, lassen sich darüber ebenfalls Daten übertragen. So erhöht sich die Kapazität auf 200 Mbps. Die Verwendung eines einzelnen Rings erhöht die maximale Distanz. Ein Dual-Ring kann bis zu 100 Kilometer abdecken.

Ethernet basiert auf der Idee, dass die Teilnehmer eines LANs Nachrichten durch Hochfrequenz übertragen, allerdings nur innerhalb eines gemeinsamen Leitungsnetzes. Jede Netzwerkschnittstelle hat einen global eindeutigen 48-Bit-Schlüssel, der als MAC-Adresse bezeichnet wird. (Tatsächlich werden MAC-Adressen teilweise mehrfach ausgegeben, aber die Hersteller versuchen durch geografische Trennungen lokale Kollisionen zu vermeiden.) Da MAC-Adressen modifizierbar sind, muss man darauf achten, keine doppelten Adressen im selben Netz zu verwenden, da es sonst zu Fehlern kommt. Ethernet überträgt die Daten auf dem Übertragungsmedium im sogenannten Basisbandverfahren und in digitalem Zeitmultiplex.

RDP (Remote Desktop Protocol): Ein von Microsoft entwickeltes Protokoll, das die Remote-Verwaltung von Windows-Computern ermöglicht, indem es den Benutzern erlaubt, eine grafische Benutzeroberfläche auf einem entfernten Computer zu steuern.

ICA (Independent Computing Architecture): Ein von Citrix entwickeltes Protokoll, das Remote-Desktop-Dienste anbietet und es Benutzern ermöglicht, von entfernten Standorten aus auf Anwendungen und Desktops zuzugreifen, unabhängig von der Plattform oder dem Betriebssystem.

VNC (Virtual Network Computing): Ein Protokoll, das Remote-Desktop-Funktionalitäten bietet, indem es die Benutzer in die Lage versetzt, die grafische Benutzeroberfläche eines entfernten Computers zu steuern. VNC ist plattformunabhängig und ermöglicht den Zugriff auf verschiedene Betriebssysteme.

Alle drei Protokolle, RDP, ICA und VNC, bieten Remote-Desktop-Funktionalitäten, unterscheiden sich jedoch in ihren Entwicklern, der Plattformunabhängigkeit und den Einsatzgebieten. RDP ist speziell für Windows-Plattformen von Microsoft entwickelt, während ICA von Citrix plattformübergreifend und flexibel für den Zugriff auf Anwendungen gestaltet ist. VNC hingegen ist plattformunabhängig und erlaubt den Fernzugriff auf verschiedene Betriebssysteme, aber im Vergleich zu den proprietären Protokollen könnte es etwas langsamer sein.

II) INTERNET

- **Aufbau von URL/URI/URN**
  - **Schema, Benutzer/Passwort, Domain, Pfad, Query, Fragment etc.**
- **Beispiele für Browser/Webserver/Web-Programmiersprachen/(serverseitige) Script-sprachen**
- **Wichtige Protokolle und Ports (HTTP, FTP, SMTP, POP3, IMAP, Telnet, SMB, SSH, NTP)**
- **Vor-/Nachteile wichtiger Dateiformate (PDF, Bildformate)**
- **Ablauf beim Aufruf einer Webseite (Kommunikation Client/Server) und Verarbeitung bei PHP**
- **Grundlegende Kenntnisse von HTML, CSS, PHP**
- **Responsive Webdesign (mit HTML5 + CSS3)**
- **Ergonomische Gestaltung von Websites**
- **Content Management System (CMS)**
- **Mindestinhalte des Impressums**
- **Virtuelle Hosts erläutern**
- **Möglichkeiten zur Unterscheidung von Websites auf einem Host: IP, Hostname, Port**
- **Funktion von .htaccess erläutern**
- **JavaScript**
  - **jQuery und andere Frameworks**
- **HTML5, CSS3**
  - **Audio-/Videoeinbettung/-unterstützung**

E) SOFTWAREKOMPONENTEN

I) SOFTWARE

- **Einteilung und Klassifikation von Anwendungssystemen**
  - **ERP, CMS, CRM, PSP, CAD, CASE, ECM, DMS, OMS**
  - **Anwendungssoftware**
  - **Betriebssysteme**
  - **Integrierte Entwicklungsumgebung (IDE)**
  - **Standard- vs. Individualsoftware**

- **Branchensoftware**
- **Open Source vs. proprietäre Software**
- **Benutzeroberfläche**
- **Datenbanksysteme**
- **Kommunikationssysteme**
- **OEM-Software**

❖ **Qualitätsmerkmale**
- **Anpassbarkeit, Wartbarkeit**
- **Schnittstellen, Interoperabilität**
- **Kompatibilität**

❖ **Intuitive Bedienung**

❖ **Bestimmungen der Barrierefreiheit bei der Auswahl sowie der Einrichtung moderner Informations- und Kommunikationstechnik (Hard- und Software) berücksichtigen**
- **Einfache Sprache**
- **Braille**
- **Spracheingabe- und -ausgabe**

❖ **Normen, Vorschriften, Zertifikate, Kennzeichnungen**

❖ **Installation und Einrichtung von Systemen, z.B. Betriebssysteme, BIOS, UEFI, Partitionierung/Formatierung, Netzwerkanbindungen, IP-Konfiguration, Remotedesktop (RDP, ICA)**

❖ **Lizenzarten, z.B. EULA, OEM, GNU**
- **Pay by Use**

❖ **Konfiguration, Test, Troubleshooting und Dokumentation von Netzwerkverbindungen, z.B. IP-Adressen, DHCP, WLAN-Zugang, Pre shared key/Enterprise**
- **VPN: End-to-End, Site-to-Site, End-to-Site**
- **L2TP, IPsec**

❖ **Bestimmungen zur IT-Sicherheit (IT-Security) bei allen eingesetzten Hardware- und Softwaresystemen bzw. Infrastrukturen für eine Sicherheit der Informationsverarbeitung und auch der Kommunikation (Daten- bzw. Informationssicherheit) kennen und einhalten**

❖ **Basiswissen IT-Servicemanagement und darin verwendeter Methoden und Verfahren, z.B.:**
- **ITIL**
- **CobiT**
- **MOF**
- **ISO 20000**

❖ **Client-Server-Modell**

II) SOFTWAREENTWICKLUNG

❖ Nötige Kenntnisse
- Vor- und Nachteile verschiedener Programmierparadigmen kennen und Programmiersprachen nach Sprachhöhe unterscheiden
- Identifikation und Auswahl einer für das jeweilige Realweltproblem" passenden Sprache
- Softwareentwicklung und Anpassung von Software
- Basiswissen Softwarelogik und grundlegende Programmelemente
- Darstellungsformen für Programmabläufe
- Aussagenlogik

- Programmstrukturen
- Algorithmen
- Compiler, Linker, Interpreter
- Prozedurale und objektorientierte Herangehensweise
- Variablen, Datentypen und -strukturen, Zuweisungen
  - primitive Datentypen: byte, short, int, long, float, double, boolean, char
- Kontrollstrukturen, z.B. Verzweigung, Schleife
- Prozeduren, Funktionen
- Objekte, Klassen, Methoden, Attribute
- Vererbung, Polymorphie
- Bibliotheken, Frameworks o Skriptsprachen, z.B. Shell-Skript, Macros
- Debugging, formale und inhaltliche Fehler

- Abbildung der Kontrollstrukturen mittels Struktogramm (Nassi-Shneiderman), PAP oder Pseudocode als didaktisches Hilfsmittel
  - Verzweigungen (if, switch), Wiederholungen (kopf-/fußgesteuert)
- UML: Use Cases, Klassendiagramm
  - Komposition, Aggregation, Assoziation
- Entwurf der Bildschirmausgabemasken (Softwareergonomie, Barrierefreiheit)
  - Mockup, Wireframe
- Anforderungen: funktionale und nicht-funktionale Anforderungen
- Datenbanken
  - Stammdaten und Bewegungsdaten
  - Aufgaben eines DBMS
  - Einfache ER-Modelle mit Entity-Relationship-Modell und Tabellenmodell erstellen
  - SQL: DDL, DOL, DML. TCL DQL
    - SELECT bezogen auf eine Tabelle (inkl. Klauseln wie WHERE, ORDER BY, GROUP BY)
    - Aggregatsfunktionen wie SUM, COUNT, AVG
  - Normalisierung

III) QUALITÄTSSICHERUNG

- Qualitätsbegriff nach ISO 9000
- Modelle und Standards einordnen, z.B.:
  - QS-Normen ISO 9000-9004
  - EFQM
  - (Six Sigma)
- Nutzen der QS-/QM-Systeme im betriebseigenen Umfeld steht hier im Vordergrund
  - an der ständigen Verbesserung des betriebseigenen QS-Systems mitarbeiten
  - Verbesserung der Prozessqualität, der Arbeitsqualität und damit der Produkt- und Dienstleistungsqualität (Stichwort: prozessorientiertes QM-System)
  - vorrangiges Ziel ist die Sicherstellung der vorgegebenen Qualität, ein höherwertiges Ergebnis ist nicht das primäre Ziel
- Zertifizierung, Audit
- Qualitätsplanung, Qualitätsziele (Ist-Zustand ermitteln und Ziel-Zustand festlegen)
- Qualitätslenkung (Umsetzung der Planphase)
- PDCA - Plan, Do, Check, Act als Qualitätsmanagementzyklus
- Kriterien der Softwarequalität: Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Änderbarkeit, Übertragbarkeit
- Siegel: Geprüfte Sicherheit, Blauer Engel
- Testverfahren
  - Black- und White-Box-Test

- Komponenten-/Modul-/Unit-Tests vs. Integrationstests vs. Systemtests
- Abnahmetest
- Lasttest

F) ITS

I) IT-SICHERHEIT

Schutzziele sind fundamentale Grundsätze der Informationssicherheit, die darauf abzielen, die Sicherheit von Informationen und Systemen zu gewährleisten.

- Vertraulichkeit: Sicherstellung, dass Informationen nur von autorisierten Personen eingesehen werden können.
- Integrität: Gewährleistung, dass Daten korrekt, unverändert und zuverlässig bleiben.
- Authentizität: Sicherstellung, dass die Identität und Herkunft von Daten oder Personen überprüfbar und echt sind.
- Verfügbarkeit: Garantie, dass Informationen jederzeit zugänglich und nutzbar sind, wenn sie benötigt werden.

Maßnahmen zur Informationssicherheit umfassen strategische Schritte und Mittel, die ergriffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten sowie die Systeme und Daten vor unbefugtem Zugriff oder Schäden zu schützen.

- Organisatorische Maßnahmen: Dies beinhaltet die Entwicklung und Umsetzung von Richtlinien, Verfahren und Organisationsstrukturen, um Sicherheitsstandards festzulegen. Dazu gehören die Ernennung von Sicherheitsverantwortlichen wie einem IT-Sicherheitsbeauftragten, die Erstellung von Sicherheitsrichtlinien wie einer Passwort-Policy und die Etablierung von Prozessen zur Sicherheitsüberwachung.
- Technische Maßnahmen: Hierunter fallen der Einsatz von technologischen Lösungen wie Virenschutzsystemen, Firewalls, Anti-Spam-Software und anderen Sicherheitswerkzeugen, um Netzwerke, Systeme und Daten vor Bedrohungen zu schützen.
- Personelle Maßnahmen: Das Ziel ist es, das Sicherheitsbewusstsein und die Sensibilisierung der Mitarbeiter für Sicherheitsrisiken zu stärken. Schulungen, Workshops und Sensibilisierungskampagnen sind hierfür entscheidende Instrumente.
- Passwörter, PINs, TANs, Captchas: Diese sind Sicherheitsmechanismen zur Zugangskontrolle oder zur Verifizierung von Identitäten. Passwörter sind Zeichenkombinationen, PINs sind Identifikationsnummern, TANs dienen zur Autorisierung von Transaktionen und Captchas sollen zwischen Menschen und Maschinen unterscheiden. Die Sicherheit und Komplexität dieser Mechanismen ist entscheidend, um unautorisierten Zugriff zu verhindern.

Normen und Branchenstandards sind Referenzpunkte, die Organisationen dabei unterstützen, bewährte Praktiken zur Informationssicherheit zu implementieren. Hier sind einige Beispiele:

Die ISO 27001 ist ein international anerkannter Standard für Informationssicherheitsmanagement-systeme (ISMS). Er legt Anforderungen fest, die Unternehmen und Organisationen dabei unterstützen, angemessene Sicherheitsmaßnahmen zum Schutz ihrer sensiblen Informationen zu etablieren, zu implementieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

- **Ziele:** Die ISO 27001 zielt darauf ab, einen systematischen Ansatz zur Verwaltung von vertraulichen Informationen zu bieten, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.
- **Risikobasiertes Denken:** Der Standard basiert auf einem risikobasierten Ansatz, der Organisationen dazu ermutigt, Risiken zu identifizieren, zu bewerten und angemessene Kontrollen einzurichten, um diese Risiken zu minimieren.

- **Plan-Do-Check-Act (PDCA)-Zyklus:** Die ISO 27001 folgt dem PDCA-Zyklus, was bedeutet, dass Organisationen einen kontinuierlichen Verbesserungsprozess implementieren, um ihre Informationssicherheit zu optimieren.
- **Rahmenbedingungen:** Sie definiert eine Reihe von Rahmenbedingungen, wie zum Beispiel die Festlegung von Sicherheitsrichtlinien, Risikobewertungen, Schulungen für Mitarbeiter und die Notfallvorsorge.
- **Zertifizierung:** Organisationen können ihre Konformität mit der ISO 27001 durch externe Prüfungen und Zertifizierungen nachweisen, was das Vertrauen von Kunden und Geschäftspartnern in die Sicherheitspraktiken stärken kann.

Die Implementierung der ISO 27001 erfordert ein starkes Engagement der Organisation, klare Prozesse zur Risikobewertung und Sicherheitskontrollen sowie regelmäßige Überprüfungen und Anpassungen, um mit sich verändernden Bedrohungen und Technologien Schritt zu halten.

Die ISO 27002 ist eng mit der ISO 27001 verbunden und bietet konkrete Leitlinien und Kontrollen für die Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) gemäß der ISO 27001. Hier sind einige wichtige Informationen zur ISO 27002:

- **Kontrollen und Maßnahmen:** Die ISO 27002 definiert eine umfassende Sammlung von Kontrollen und Maßnahmen, die Organisationen dabei unterstützen, die Anforderungen der ISO 27001 umzusetzen. Diese Kontrollen decken verschiedene Aspekte der Informationssicherheit ab, einschließlich physischer Sicherheit, Zugriffskontrolle, Verschlüsselung, Inzident Management, usw.
- **Detaillierte Richtlinien:** Im Gegensatz zur ISO 27001, die sich auf die Prozesse und Prinzipien konzentriert, bietet die ISO 27002 detaillierte Empfehlungen und Best Practices für spezifische Sicherheitsmaßnahmen. Es ist eine Art Handbuch für die Umsetzung der Anforderungen der ISO 27001.
- **Flexibilität und Anpassung:** Die ISO 27002 bietet einen Rahmen, der Organisationen erlaubt, die empfohlenen Kontrollen und Maßnahmen an ihre individuellen Risiken, Bedürfnisse und Umgebungen anzupassen. Es ist kein starres Regelwerk, sondern ein Leitfaden zur Sicherstellung einer angemessenen Informationssicherheit.
- **Korrelation mit anderen Standards:** Die ISO 27002 kann in Verbindung mit anderen Sicherheitsstandards und -rahmenwerken verwendet werden. Sie bietet eine umfassende Liste von Kontrollen, die mit anderen Standards wie COBIT, NIST oder ITIL korrelieren.
- **Kontinuierliche Verbesserung:** Ähnlich wie bei der ISO 27001 betont die ISO 27002 die Bedeutung der kontinuierlichen Verbesserung. Organisationen sollten regelmäßig ihre Informationssicherheitspraktiken überprüfen, um sicherzustellen, dass sie wirksam sind und sich an Veränderungen in der Bedrohungslandschaft anpassen.

Die ISO 27002 ist ein wertvolles Werkzeug für Organisationen, die die Richtlinien der ISO 27001 implementieren möchten, da sie konkrete Empfehlungen und Kontrollen bietet, um ein robustes Informationssicherheitsmanagementsystem zu etablieren und aufrechtzuerhalten.

Der BSI IT-Grundschutz ist ein Rahmenwerk des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Deutschland. Es bietet eine strukturierte und praxisnahe Methode zur Informationssicherheit und Risikomanagement für Organisationen. Hier sind einige relevante Informationen darüber:

- **Modularer Ansatz:** Der IT-Grundschutz verwendet einen modularen Ansatz, der sich auf verschiedene Aspekte der Informationssicherheit konzentriert. Es bietet eine Sammlung von Bausteinen (sogenannte "Bausteine") für verschiedene Bereiche wie Netzwerksicherheit, Infrastruktursicherheit, Datensicherheit usw.
- **Risikoorientierung:** Ähnlich zur ISO 27001 basiert der IT-Grundschutz auf einer risikobasierten Vorgehensweise. Organisationen bewerten Risiken und setzen dann die entsprechenden Bausteine ein, um diese Risiken zu minimieren.

- **Praktische Umsetzung:** Der IT-Grundschutz bietet konkrete Handlungsanleitungen und Empfehlungen in Form von Bausteinen. Diese enthalten Maßnahmen, um typische Schwachstellen und Risiken zu adressieren, und können je nach Bedarf und Risikoprofil der Organisation angepasst werden.
- **Vorgegebene Sicherheitsmaßnahmen:** Im Gegensatz zur ISO 27002, die allgemeinen Kontrollen und Empfehlungen anbietet, bietet der IT-Grundschutz konkrete Maßnahmen und Techniken zur Umsetzung von Sicherheitsstandards.
- **Zertifizierung und Anerkennung:** Eine Zertifizierung nach dem BSI IT-Grundschutz kann in Deutschland für Organisationen eine hohe Relevanz haben. Es dient als anerkannter Standard und kann das Vertrauen von Kunden, Partnern und anderen Stakeholdern stärken.

Der BSI IT-Grundschutz ist besonders in Deutschland weit verbreitet und wird oft von öffentlichen Institutionen und Unternehmen genutzt, um Informationssicherheit zu gewährleisten. Es ist ein praxisorientiertes Rahmenwerk, das Organisationen dabei unterstützt, Schutzmaßnahmen umzusetzen, die auf spezifische Risiken und Anforderungen zugeschnitten sind.

Diese Standards dienen als Rahmen für die Entwicklung, Implementierung und Aufrechterhaltung von Informationssicherheitsmaßnahmen und helfen Organisationen, ihre Systeme und Daten zu schützen.

Bei den Vorschriften Basel II und III handelt es sich um internationale Vereinbarungen, die von der Basel Committee on Banking Supervision (BCBS) entwickelt wurde. Die Basel Committee on Banking Supervision ist eine Einrichtung der Bank for International Settlements (BIS).

Basel II wurde 2004 beschlossen und ist die Erweiterung von Basel I. Grund für die Entwicklung von Basel II ist, die Schwächen von Basel I zu überwinden. Das Ziel von Basel II ist das Risikomanagement und die Verbesserung von Eigenkapitalanforderungen für Banken. Basel II besteht aus drei Hauptkomponenten, die auch als “drei Säulen“ bezeichnet werden:

Säule 1: Mindesteigenkapitalanforderungen: Basel II führt eine differenzierte Methode zur Berechnung der Mindestkapitalanforderungen ein. Sinn dahinter soll sein, dass die Kapitalanforderungen besser den Risiken entsprechen, denen eine Bank ausgesetzt ist. Es werden Risiken wie Kredit-, Marktpreis- und operationelle Risiken berücksichtigt.

Säule 2: Bankaufsichtlicher Überprüfungsprozess: Aufsichtsbehörden sollen die Qualität und Quantität der von den Banken bereitgestellten Informationen überwachen. Dieser Pfeiler legt den Fokus auf die aufsichtsrechtliche Überprüfung und die Anpassung der Kapitalanforderungen, um spezifische Risikoprofile der Banken zu berücksichtigen.

Säule 3: Erweiterte Offenlegung / Marktdisziplin: Basel II fördert eine transparentere Darstellung der Risikopositionen und der Kapitalausstattung der Banken. Dies soll die Marktdisziplin stärken, indem potenziellen Anlegern, Gläubigern und anderen Marktteilnehmern mehr Informationen zur Verfügung gestellt werden.

Als Nachfolger von Basel II dient Basel III.

Basel III wurde im Dezember 2010 vom Basler Ausschuss für Bankenaufsicht in einer vorläufigen Endfassung veröffentlicht. Ziel von Basel III ist es, die Stabilität des internationalen Finanzsystems zu stärken und die Risiken im Bankensektor zu reduzieren. Basel III ist der Nachfolger von Basel I und Basel II. Seit 2013 wird Basel II von Basel III schrittweise abgelöst. Hauptsächlich wurde Basel III geschaffen, nachdem die Finanz- und Wirtschaftskrise 2007-2008 Schwächen des internationalen Bankensystems offengelegt hatte. Folgend werden die wichtigsten Merkmale und Bestimmungen genannt:

Eigenkapitalanforderungen: Basel III legt strengere Anforderungen an das Eigenkapital der Banken fest. Banken müssen einen höheren Anteil ihres Gesamtkapitals als hartes Kernkapital halten, um besser gegen finanzielle Schocks geschützt zu sein.

Einführung einer Verschuldungsquote (Leverage Ratio): Eingeführt wurde dies, um sicherzustellen, dass Banken nicht übermäßig hohe Fremdkapitalhebel nutzen. Dies soll die Stabilität des Bankensystems durch die Begrenzung des Verhältnisses von Fremdkapital zu Eigenkapital verbessern. Dadurch soll dem Bankensektor geholfen werden, sich vor einer übermäßigen Verschuldung zu bewahren.

Einführung eines Liquiditätsrisikostandards: Basel III legt strengere Anforderungen an die Liquidität von Banken fest, um sicherzustellen, dass sie in der Lage sind, ihren kurzfristigen Verpflichtungen nachzukommen.

Einführung von Gegenparteirisikostandards: Basel III setzt Standards für die Kontrolle und Begrenzung von Gegenparteirisiken, insbesondere im Zusammenhang mit derivativen Finanzinstrumenten.

Berücksichtigung systematischer Risiken: Basel III legt strengere Vorschriften für als systemisch wichtig eingestufte Finanzinstitute fest, um sicherzustellen, dass diese Banken aufgrund ihrer Größe und Bedeutung für das Finanzsystem zusätzliche Vorsichtsmaßnahmen ergreifen.

SOX steht für Sarbanes-Oxley Act, ein US-amerikanisches Bundesgesetz, das im Jahr 2002 verabschiedet wurde. Der offizielle Name des Gesetzes ist Sarbanes-Oxley Act of 2002, benannt nach den US-Senatoren Paul Sarbanes und Michael Oxley, die eine Schlüsselrolle bei seiner Entstehung spielten. Das Gesetz wurde als Reaktion auf verschiedene Bilanzskandale großer Unternehmen eingeführt, darunter Enron und WorldCom, um die Transparenz und Integrität von Finanzberichten zu verbessern und das Vertrauen der Anleger in die Finanzmärkte zu stärken.

Finanzberichterstattung und Transparenz: SOX verlangt von Unternehmen, transparente und genaue Finanzberichte zu erstellen und sicherzustellen, dass die Informationen in den Berichten korrekt sind.

Interne Kontrollen: Eine wesentliche Komponente von SOX ist die Verstärkung der internen Kontrollen in Unternehmen. Unternehmen müssen sicherstellen, dass sie effektive interne Kontrollsysteme implementieren, um finanzielle Unregelmäßigkeiten zu verhindern.

CEO und CFO-Zertifizierung: Gemäß SOX müssen CEOs (Chief Executive Officers) und CFOs (Chief Financial Officers) persönlich für die Genauigkeit ihrer Finanzberichte bürgen und eine schriftliche Bestätigung der Wirksamkeit der internen Kontrollen unterzeichnen.

Unabhängige Prüfung: Unternehmen unterliegen einer unabhängigen Prüfung ihrer internen Kontrollen und Finanzberichte durch externe Prüfungsfirmen.

Strafverfolgung für Fehlinformationen: SOX sieht strafrechtliche Konsequenzen für Unternehmen und Führungskräfte vor, die absichtlich falsche oder irreführende Informationen in Finanzberichten veröffentlichen.

Whistleblower-Schutz: Das Gesetz enthält Bestimmungen zum Schutz von Whistleblowern, die Missstände oder Verstöße gegen SOX-Maßnahmen melden.

Dokumentenretention und Prüfung: SOX enthält Anforderungen an die Aufbewahrung von Unterlagen und verlangt, dass Unternehmen wichtige Geschäftsdokumente für einen bestimmten Zeitraum aufbewahren.

Audit Committees: SOX schreibt vor, dass Unternehmen unabhängige Audit Committees einrichten, um die Unabhängigkeit der Prüfung und die Integrität der Finanzberichterstattung zu gewährleisten.

Die Einhaltung der SOX-Anforderungen betrifft vor allem öffentlich gehandelte Unternehmen in den Vereinigten Staaten. Unternehmen, die unter die Regelungen von SOX fallen, müssen erhebliche Anstrengungen unternehmen, um sicherzustellen, dass ihre Finanzberichterstattung und interne Kontrollen den gesetzlichen Anforderungen entsprechen. Die SOX-Compliance hat sich zu einem integralen Bestandteil der Unternehmensführung und Corporate Governance entwickelt.

Die Schutzbedarfsanalyse im Rahmen des BSI IT-Grundschutzes ist ein strukturierter Prozess zur Bewertung der Sicherheitsanforderungen von verschiedenen Bereichen in einem Unternehmen oder einer Organisation.

- **Anwendungen:** Diese Analyse konzentriert sich auf die Identifizierung von Sicherheitsanforderungen für Softwareanwendungen, um potenzielle Schwachstellen oder Risiken zu erkennen und angemessene Sicherheitsmaßnahmen zu definieren.
- **IT-Systeme:** Hierbei wird der Schutzbedarf von Informationstechnologiesystemen, einschließlich Hardware, Betriebssystemen und Datenbanken, analysiert, um Sicherheitslücken zu erkennen und geeignete Schutzmaßnahmen zu bestimmen.
- **Räume:** Diese Analyse bewertet den Sicherheitsbedarf von physischen Räumlichkeiten, um potenzielle Sicherheitsrisiken zu identifizieren und Schutzmaßnahmen für Gebäude, Serverräume oder andere wichtige Bereiche festzulegen.
- **Kommunikationsverbindungen:** Hierbei wird der Schutzbedarf von Netzwerkverbindungen und Kommunikationssystemen untersucht, um potenzielle Sicherheitslücken zu identifizieren und Sicherheitsmaßnahmen für die Netzwerkinfrastruktur festzulegen.

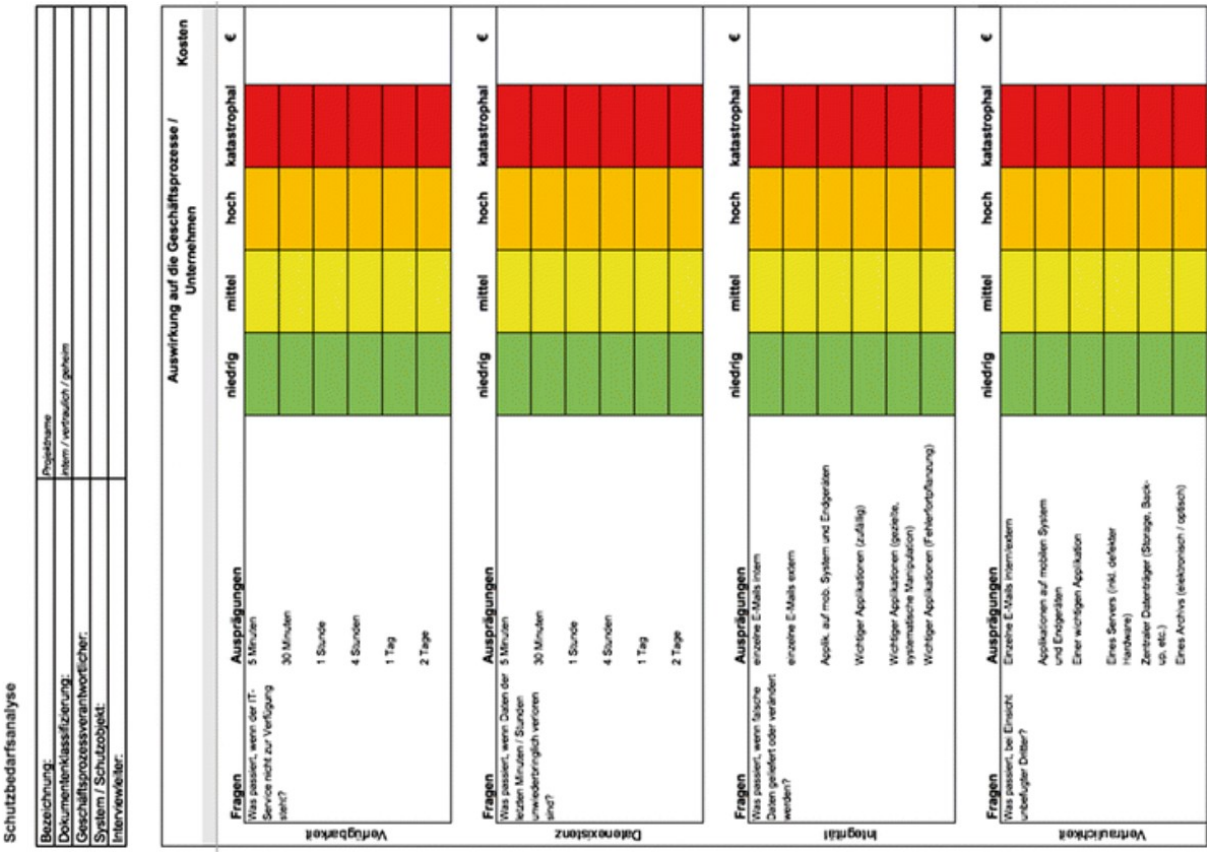

ABBILDUNG 1 STRUKTUR EINER SCHUTZBEDARFSANALYSE

Das Anwenden von Evaluierungstechniken zur IT-Sicherheit, wie es im IT-Grundschutz-Handbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) beschrieben wird, beinhaltet die systematische Bewertung von Sicherheitsmaßnahmen und -prozessen, um deren Wirksamkeit zu überprüfen. Hier sind einige wichtige Punkte dazu:

Ziel der Evaluierung: Die Evaluierungstechniken dienen dazu, die Effektivität der implementierten Sicherheitsmaßnahmen zu bewerten und Schwachstellen aufzudecken. Dies geschieht in regelmäßigen Abständen oder in Reaktion auf veränderte Bedrohungen oder Umgebungen.

Methoden und Werkzeuge: Das IT-Grundschutz-Handbuch bietet verschiedene Methoden und Werkzeuge zur Evaluierung der IT-Sicherheit. Dazu gehören beispielsweise Checklisten, Audits, Penetrationstests und Risikobewertungen.

Praktische Anwendbarkeit: Die Evaluierungstechniken im IT-Grundschutz-Handbuch sind darauf ausgerichtet, praxisnah zu sein. Sie ermöglichen es Organisationen, ihre Sicherheitsmaßnahmen zu überprüfen und auf Basis der Ergebnisse Verbesserungen vorzunehmen.

Kontinuierliche Verbesserung: Ähnlich wie bei anderen Sicherheitsstandards betont der IT-Grundschutz die Bedeutung der kontinuierlichen Verbesserung. Die Ergebnisse der Evaluierung werden genutzt, um das Sicherheitsniveau zu erhöhen und den sich ändernden Bedrohungen anzupassen.

Richtlinienkonformität: Die Evaluierungstechniken zielen darauf ab sicherzustellen, dass die implementierten Sicherheitsmaßnahmen den Richtlinien des IT-Grundschutz-Handbuchs entsprechen und den erwarteten Schutz bieten.

Die Anwendung von Evaluierungstechniken gemäß dem IT-Grundschutz-Handbuch ermöglicht es Organisationen, ihre Sicherheitsvorkehrungen zu überprüfen, zu validieren und zu verbessern. Sie spielen eine wichtige Rolle dabei, sicherzustellen, dass die Informationssicherheit kontinuierlich auf einem angemessenen Niveau bleibt und auf neue Bedrohungen und Entwicklungen reagiert werden kann.

Schutzbedarfskategorien sind ein Konzept der Informationssicherheit und werden insbesondere in Deutschland im Rahmen des IT-Grundschutzes nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verwendet. Die Kategorien Normal, Hoch und sehr Hoch helfen dabei, den Schutzbedarf von Informationen und IT-Systemen zu bewerten.

Schutzbedarfskategorie Normal: Informationen und IT-Systeme mit dem Schutzbedarf „Normal“ erfordern ein durchschnittliches Schutzniveau. Hierbei handelt es sich um Standardinformationen und -systeme, bei deren Verlust, Beeinträchtigung oder Offenlegung keine erheblichen Schäden zu erwarten sind.

Schutzbedarfskategorie Hoch: Informationen und Systeme mit erhöhtem Schutzbedarf sind sensibler Natur. Ein Schaden durch Verlust, Beeinträchtigungen oder Offenlegung könnte für die Organisation erhebliche Konsequenzen haben. Hierzu gehören beispielsweise personenbezogene Daten oder geschäftskritische Informationen.

Schutzbedarfskategorie sehr Hoch: Informationen und IT-Systeme mit hohem Schutzbedarf sind von besonderer Bedeutung für die Organisation. Ein Schaden könnte schwerwiegende Folgen haben, sowohl finanziell als auch im Hinblick auf das Ansehen der Organisation. Hierzu zählen beispielsweise geheime Forschungsergebnisse oder Informationen zu nationalen Sicherheitsbelangen.

Um ein mittleres, angemessenes oder ausreichendes Schutzniveau für Identifikationssysteme zu erreichen, sind sowohl technische Sicherheitsmaßnahmen als auch infrastrukturelle, organisatorische und personelle Schutzmaßnahmen erforderlich. Dies beinhaltet die Implementierung von geeigneten Sicherheitsmechanismen wie Zugriffskontrollen, Verschlüsselungstechniken oder Sicherheitsrichtlinien sowie die Entwicklung und Umsetzung organisatorischer Verfahren und die Sensibilisierung der Mitarbeiter für Sicherheitsrisiken. Durch diese kombinierten Maßnahmen soll ein adäquates Schutzniveau erreicht werden, das den spezifischen Schutzanforderungen für Identifikationssysteme gerecht wird.

- IT-Sicherheitsmanagementsystem implementieren
  - Betrieblicher IT-Sicherheitsbeauftragter
  - Schaffung eines Sicherheitsbewusstseins bei den Mitarbeitern
  - IT-Sicherheitsmanagement
  - Durch technische, infrastrukturelle, organisatorische und personelle Schutzmaßnahmen

- Verhindern oder Abwehr von Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes, z.B. durch Etablierung eines IT-Sicherheitsmanagements (ISMS) unter Verwendung von Standards wie IT-Grundschutz, ISO/IEC 27001

❖ Security by Design, Security by Default

Security by Design ist ein Sicherheitskonzept in der Informationssicherheit, das Sicherheitsaspekte von Anfang an in den Entwicklungsprozess von Systemen, Anwendungen oder Produkten integriert. Dieses Prinzip betont die proactive Integration von Sicherheitsmaßnahmen während des gesamten Lebenszyklus eines Systems, beginnend mit der Konzeption und Planung bis hin zur Implementierung und Wartung. Es strebt danach, Sicherheit als grundlegenden Bestandteil der IT- und Produktentwicklung zu etablieren.

Sicherheitsaspekte werden von Beginn an in den Entwicklungsprozess eingebunden. Das bedeutet, dass Sicherheitsüberlegungen nicht als nachträgliche Ergänzung betrachtet warden, sondern von Anfang an als integraler Bestandteil des Designs.

Eine gründliche Risikobewertung wird durchgeführt, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Auf Grundlage dieser Analyse warden angemessene Sicherheitsmaßnahmen entwickelt und implementiert.

Die Grundprinzipien der Sicherheit, wie die Prinzipien der geringsten Rechte, müssen bei der Entwicklung berücksichtigt werden Dies bedeutet, dass Benutzer, Anwendungen oder Systeme nur die minimal erforderlichen Rechte und Zugriffe erhalten.

Entwickler und Projektbeteiligte werden in Sicherheitsfragen geschult, um ein Bewusstsein für Sicherheitsrisiken und bewährte Sicherheitspraktiken zu schaffen. Dies fördert eine Kultur der Sicherheit im gesamten Entwicklungsprozess.

Die Sicherheitsaspekte werden kontinuierlich überprüft und aktualisiert, um auf neue Bedrohungen und Entwicklungen in der Sicherheitslandschaft reagieren zu können. Dies schließt regelmäßige Sicherheitsaudits und -überprüfungen ein.

Alle Sicherheitsentscheidungen und -maßnahmen werden dokumentiert. Dies ermöglicht eine transparente Nachverfolgung der Sicherheitsentscheidungen und erleichtert die Zusammenarbeit zwischen verschiedenen Teams und Stakeholdern.

Bei **Security by Default** handelt es sich um ein Sicherheitsprinzip, welches ein angemessenes Maß an Sicherheit zu gewährleisten hat, indem standardmäßig sichere Konfigurationen und Einstellungen für Systeme, Anwendungen oder Produkte verwendet werden. Bei der Umsetzung dieses Prinzips sollen die voreingestellten Konfigurationen so gestaltet sein, dass sie ein solides Sicherheitsniveau bieten, ohne dass Benutzer zusätzliche Anpassungen vornehmen müssen.

Das Ziel ist es, Benutzer vor potenziellen Sicherheitsrisiken zu schützen, ohne dass sie aktiv Sicherheitseinstellungen ändern müssen. Die Standardeinstellungen und Konfigurationen von Systemen oder Anwendungen werden so entworfen, dass sie bereits ein angemessenes Sicherheitsniveau bieten. Dies beinhaltet den Einsatz sicherer Protokolle, den Zugriff auf Dienste und Funktionen sowie die Verwendung sicherer Standardpasswörter.

Durch die Auswahl von sicheren Standardkonfigurationen wird die Angriffsfläche, also die Menge potenziell angreifbarer Komponenten, minimiert. Unnötige Dienste oder Funktionen werden standardmäßig deaktiviert, um das Risiko von Sicherheitslücken zu reduzieren.

"Security by Default" orientiert sich an etablierten Sicherheitsrichtlinien und -standards. Diese können von anerkannten Organisationen wie dem National Institute of Standards and Technology (NIST) oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) stammen.

Automatisierte Tools und Mechanismen werden eingesetzt, um sicherheitsrelevante Konfigurationen automatisch durchzuführen. Dies minimiert menschliche Fehler und stellt sicher, dass die Sicherheitsstandards konsistent eingehalten werden.

- Datensicherung/Backup-Verfahren
  - Wie erkennt die Software, welche Daten zu sichern sind?
  - Inkrementelles, differenzielles und Vollbackup
  - Generationenprinzip bzw. Großvater/Vater/Sohn
  - Medien nennen und erläutern
    - Kriterien bei der Auswahl von Backupmedien: Lebensdauer, Zugriffsgeschwindigkeit, Kosten, Störanfälligkeit, Kapazität
  - Hot/Cold Backup
  - Was sind sicherungswürdige Daten?
  - Mögliche Gründe für Datenverluste auf Servern erläutern und Gegenmaßnahmen vorschlagen
  - Folgen von Datenverlust, Auswirkungen von Datenverlusten für das Unternehmen erläutern
  - Maßnahmen der Mitarbeiter zur Vermeidung von Datenverlusten erläutern

Die ordnungsgemäße **Verschrottung von Datenträgern** ist ein wichtiger Schritt zur Sicherstellung der IT-Sicherheitsmaßnahmen, dass sensible Informationen nicht in die falschen Hände geraten. Hier sind einige Schritte, die bei der Verschrottung von Datenträgern unter Einhaltung der Datenschutzgesetze und IT-Sicherheitsmaßnahmen berücksichtigt werden sollten:

1. Dateninventur und Klassifizierung
2. Datenlöschung
3. Physische Zerstörung
4. Zertifizierte Dienstleister
5. Dokumentation
6. Umgebungssicherheit
7. Umweltschutz
8. Überprüfung und Audit

Vor der Verschrottung sollte eine umfassende Inventur aller Datenträger durchgeführt werden, um sicherzustellen, dass keine wichtigen Daten übersehen werden. Sensible Daten sollten entsprechend ihrer Klassifizierung identifiziert werden, um angemessene Maßnahmen für die sichere Entsorgung zu treffen.

Bevor Datenträger verschrottet werden, ist es wichtig, alle Daten darauf sicher zu löschen. Dies kann durch spezielle Software oder Hardware erfolgen, die sicherstellt, dass alle Daten unwiderruflich gelöscht werden. In einigen Fällen kann auch die physische Zerstörung der Datenträger eine Option sein.

Die physische Zerstörung von Datenträgern ist eine effektive Methode, um sicherzustellen, dass die darauf gespeicherten Daten nicht wiederhergestellt werden können. Dies kann durch Schreddern, Zertrümmern oder andere zerstörerische Methoden erfolgen. Es ist wichtig sicherzustellen, dass die Zerstörung nach anerkannten Standards erfolgt.

Unternehmen sollten Dienstleister wählen, die auf die sichere Entsorgung von Datenträgern spezialisiert sind und entsprechende Zertifizierungen besitzen. Dies gewährleistet, dass die Verschrottung nach etablierten Standards und Datenschutzgesetzen erfolgt.

Jeder Schritt im Verschrottungsprozess sollte dokumentiert werden. Dies umfasst die Inventur, den Löschprozess und die physische Zerstörung. Die Dokumentation ist wichtig, um die Einhaltung von Datenschutzbestimmungen nachweisen zu können.

Während des Verschrottungsprozesses ist es wichtig sicherzustellen, dass die Umgebung sicher ist. Dies bedeutet, dass nur autorisiertes Personal Zugang zu den Datenträgern hat und dass angemessene Sicherheitsmaßnahmen getroffen werden, um Diebstahl oder unbefugten Zugriff zu verhindern.

Bei der physischen Zerstörung von Datenträgern sollte auch auf die umweltgerechte Entsorgung geachtet werden. Elektronische Komponenten enthalten oft gefährliche Materialien, die ordnungsgemäß entsorgt werden müssen.

Nach der Verschrottung sollte eine Überprüfung und ein Audit des Prozesses durchgeführt werden, um sicherzustellen, dass alle Schritte korrekt umgesetzt wurden. Dies dient nicht nur der Sicherstellung der Datensicherheit, sondern auch der kontinuierlichen Verbesserung des Datenschutzprozesses.

Die Einhaltung dieser Schritte gewährleistet, dass die Verschrottung von Datenträgern den Datenschutzgesetzen entspricht und die Vertraulichkeit sensibler Informationen gewährleistet ist.

- Sicherung der Verfügbarkeit, z.B. RAID-Systeme, SAN
  - RAID 0, 1, 5, 6, 01, 10, JBOD erklären
  - Nested RAID levels

RAID (Redundant Array of Independent Disks) bezieht sich auf verschiedene Techniken zur Organisation von Festplattenlaufwerken in einem System, um Leistung, Redundanz oder beides zu verbessern. Hier sind Erläuterungen zu den gängigen RAID-Leveln:

- RAID 0 (Striping):
  - Merkmale:
    - Daten werden über mehrere Laufwerke verteilt (Striping).
    - Keine Redundanz, daher kein Schutz vor Datenverlust bei Ausfall eines Laufwerks.
  - Vorteile:
    - Hohe Leistung durch paralleles Schreiben/Lesen auf mehreren Laufwerken.
    - Effiziente Nutzung des verfügbaren Speichers.
  - Nachteile:
    - Keine Redundanz, Ausfall eines Laufwerks führt zum Datenverlust.
- RAID 1 (Mirroring):
  - Merkmale:
    - Daten werden auf zwei Laufwerken identisch gespiegelt.
    - Hohe Redundanz und Datensicherheit.
  - Vorteile:
    - Hohe Lesegeschwindigkeiten, da Daten von beiden Laufwerken gleichzeitig gelesen werden können.
    - Ausfallsicherheit bei einem Laufwerksausfall.
  - Nachteile:
    - Hohe Kosten, da die Hälfte des Speichers für die Spiegelung verwendet wird.
- RAID 5 (Striping mit verteilter Parität):
  - Merkmale:
    - Daten werden über mehrere Laufwerke verteilt (Striping) und Paritätsinformationen werden ebenfalls verteilt gespeichert.
    - Bietet Redundanz durch Paritätsinformationen, ermöglicht den Betrieb auch bei Ausfall eines Laufwerks.
  - Vorteile:
    - Gute Kombination aus Leistung und Datensicherheit.
  - Nachteile:
    - Schreibvorgänge können langsamer sein, da Paritätsinformationen aktualisiert werden müssen.
- RAID 6 (Striping mit doppelter verteilter Parität):
  - Merkmale:
    - Ähnlich wie RAID 5, aber mit doppelter Parität.
    - Bietet höhere Redundanz und Schutz vor dem Ausfall von zwei Laufwerken.
  - Vorteile:
    - Erhöhte Ausfallsicherheit im Vergleich zu RAID 5.
  - Nachteile:

- Schreibvorgänge können langsamer sein als bei RAID 5.

❖ RAID 01 (Mirror of Stripes):
  - ➢ Merkmale:
    - Kombiniert RAID 0 (Striping) und RAID 1 (Mirroring).
    - Stripes werden gespiegelt.
  - ➢ Vorteile:
    - Hohe Leistung und hohe Datensicherheit durch Spiegelung.
  - ➢ Nachteile:
    - Hoher Speicherplatzbedarf durch Spiegelung.

❖ RAID 10 (Striping über Mirrors):
  - ➢ Merkmale:
    - Kombiniert RAID 0 (Striping) und RAID 1 (Mirroring).
    - Daten werden gestriped und dann gespiegelt.
  - ➢ Vorteile:
    - Hohe Leistung und hohe Datensicherheit durch Kombination von Striping und Mirroring.
  - ➢ Nachteile:
    - Hoher Speicherplatzbedarf durch Spiegelung.

❖ JBOD (Just a Bunch Of Disks):
  - ➢ Merkmale:
    - Einfache Anordnung von unabhängigen Laufwerken ohne RAID-Konfiguration.
    - Jedes Laufwerk wird einzeln genutzt.
  - ➢ Vorteile:
    - Einfache Konfiguration und flexible Nutzung der verfügbaren Kapazität.
  - ➢ Nachteile:
    - Keine Redundanz oder Leistungssteigerung.

Die Auswahl des geeigneten RAID-Levels hängt von den spezifischen Anforderungen an Leistung, Datensicherheit und Speichereffizienz ab.

Nasted RAID levels kombinieren mehrere RAID-Levels, um bestimmte Eigenschaften zu optimieren, wie Leistung, Redundanz oder eine Kombination aus beidem. Hier sind einige der gängigsten Nested RAID-Levels:

RAID 01 (auch als RAID 0+1 bekannt):

Merkmale:

Kombiniert RAID 0 (Striping) und RAID 1 (Mirroring).

Stripes werden gespiegelt.

Vorteile:

Hohe Leistung durch Striping.

Hohe Datensicherheit durch Mirroring.

Nachteile:

Hoher Speicherplatzbedarf durch Spiegelung.

RAID 10 (auch als RAID 1+0 bekannt):

Merkmale:

Kombiniert RAID 0 (Striping) und RAID 1 (Mirroring).

Daten werden gestriped und dann gespiegelt.

Vorteile:

Hohe Leistung durch Striping.

Hohe Datensicherheit durch Mirroring.

Nachteile:

Hoher Speicherplatzbedarf durch Spiegelung.

RAID 50:

Merkmale:

Kombiniert RAID 5 (Striping mit verteilter Parität) und RAID 0 (Striping).

Striping auf höherer Ebene über Striping auf niedrigerer Ebene.

Vorteile:

Gute Kombination aus Leistung und Datensicherheit.

Redundanz durch Paritätsinformationen.

Nachteile:

Komplexere Konfiguration im Vergleich zu einfachen RAID-Levels.

RAID 60:

Merkmale:

Kombiniert RAID 6 (Striping mit doppelter verteilter Parität) und RAID 0 (Striping).

Striping auf höherer Ebene über Striping auf niedrigerer Ebene.

Vorteile:

Höhere Ausfallsicherheit als RAID 50.

Gute Leistung durch Striping. Nachteile:

Komplexere Konfiguration.

RAID 100:

Merkmale:

Kombiniert RAID 1 (Mirroring) und RAID 0 (Striping) auf höherer Ebene über RAID 0 auf niedrigerer Ebene.

Stripes werden gespiegelt. Vorteile:

Hohe Leistung durch Striping.

Hohe Datensicherheit durch Mirroring. Nachteile:

Hoher Speicherplatzbedarf durch Spiegelung.

Die Auswahl eines Nested RAID-Levels hängt von den spezifischen Anforderungen an Leistung, Datensicherheit und Speichereffizienz ab. Es ist wichtig zu beachten, dass die Implementierung von Nested

RAID-Levels zusätzliche Komplexität mit sich bringen kann, und die Wahl sollte daher sorgfältig basierend auf den spezifischen Anforderungen und Zielen erfolgen.

Die **Zugangs- und Zugriffskontrolle** im Bereich der IT-Sicherheit bezieht sich auf Maßnahmen, die sicherstellen, dass nur autorisierte Benutzer auf bestimmte IT-Ressourcen zugreifen können und dass diese Zugriffe entsprechend ihren Berechtigungen gesteuert werden.

Angenommen, ein Unternehmen hat sensible Kundendaten in seiner Datenbank gespeichert. Die Zugangskontrolle würde sicherstellen, dass nur autorisierte Mitarbeiter durch eine geeignete Authentifizierungsmethode, wie Benutzername und Passwort, Zugang zu den IT-Systemen des Unternehmens erhalten. Nach erfolgreicher Zugangskontrolle würde die Zugriffskontrolle sicherstellen, dass der Mitarbeiter nur auf die für seine Rolle notwendigen Daten in der Datenbank zugreifen kann. Diese Zugriffsberechtigungen werden präzise festgelegt und überwacht, um sicherzustellen, dass kein unberechtigter Zugriff auf sensible Informationen erfolgt. Durch diese differenzierten Kontrollmechanismen wird das Risiko unbefugter Zugänge und Zugriffe minimiert, und die Integrität sowie Vertraulichkeit der Daten bleiben gewährleistet.

Grundbegriffe der IT-Sicherheit:

- Schadprogramme
  - Viren: Computerprogramme, welche sich unbemerkt auf dem PC einschleusen, sich an andere Programme anhängen, um sich selber zu reproduzieren und sich dann auf andere Geräte durch den Austausch von Dateien verbreiten. Viren infizieren Computerprogramme und zählen als Malware.
  - Würmer: Schadsoftware, die sich selbst reproduzieren und über Netzwerke verbreiten. Der Unterschied zu Viren ist, dass Würmer keine Hostdatei zur Reproduzierung benötigen, da sie dies selbst tun. Ein Wurm befällt den PC selbst.
  - Rootkits: Sammlung von Schadsoftware, die sich auf verschiedenen Berechtigungsebenen des Computers einnisten, um so den Zugang zum Computer zu vereinfachen. Es verschleiert Schadsoftware vor z.B. Virenscannern.
  - Botnetze: Zusammenschluss befallener internetfähiger Endgeräte, die ferngesteuert als Schwarm agieren. Diese werden z.B. zum Lahmlegen von Webdiensten missbraucht.
  - Trojaner: Schadsoftware, welche sich als legitime Software oder Datei ausgibt, um somit einen Computer zu infiltrieren. Ein Trojaner kann sich nicht wie Würmer oder Viren reproduzieren.
  - Malware: Schadsoftware, welche unerwünscht und unbemerkt auf Computer gelangen, um dort bösartige Aktionen auszuführen.
  - Ransomware: Schadsoftware, welche den Zugriff auf Daten und Systeme blockieren und ein Lösegeld fordern, um diese wieder zugänglich zu machen.
  - Spyware: Programme, welche unbemerkt und ohne Zustimmung auf den Computer gelangen, um private Daten abzugreifen.
  - Adware: Schadsoftware, welche sich auf einem Gerät verbirgt, um durch die Überwachung des Nutzerverhaltens gezielte Werbung einzublenden.
  - Scareware: Software, welche versucht den Benutzer zu erschrecken oder in Panik zu versetzen, damit dieser unüberlegt die eigentliche Schadsoftware installiert oder Geld bezahlt. Dies kann z.B. mit Popup-Alerts passieren, dass der Nutzer einen Virus auf seinem Gerät hat.
  - Hoax: Falschmeldungen, die im Internet kursieren.
  - Dialer: Bösartiges Programm, welches mithilfe der Wählfunktion versucht andere Nummern anzurufen.
  - Keylogger: Hard- oder Software, welches die Tastenanschläge des Nutzers aufzeichnet.
- Hacker, Cracker und Scriptkiddies
  - Blackhat-Hacker
    - Blackhat-Hacker sind kriminelle Hacker, welche versuchen, in Systeme einzudringen. Ihr Ziel ist oft der Diebstahl von sensiblen Daten wie Kreditkarteninformationen, Dokumenten und Passwörtern. Alternativ schleusen sie Malware in die Systeme ein. Ihre Absichten sind in der Regel darauf ausgerichtet, Schaden anzurichten oder Geld zu erlangen.
  - Whitehat-Hacker

        - Whitehat-Hacker stehen im Gegensatz zu Blackhat-Hackern. Sie setzen sogenannte Pentest-Tools ein, um Schwachstellen in einem System zu identifizieren. Diese Tätigkeiten erfolgen legal und mit Zustimmung des Eigentümers des Systems, mit dem Ziel die Sicherheit des Systems zu verbessern.
    - Cracker
        - Der Begriff Cracker wird oft synonym mit Hacker verwendet, obwohl es Unterschiede gibt. Cracker sind darauf spezialisiert, Schutzmechanismen von Software zu umgehen, um beispielsweise illegale Kopien zu erstellen oder Lizenzschlüssel zu generieren. Im Vergleich zu Hackern liegt der Fokus mehr auf der Umgehung von Schutzmaßnahmen als auf dem Eindringen in Systeme.
    - Script-Kiddies
        - Script-Kiddies sind unerfahrene Personen, welche vorgefertigte Skripte oder Tools verwenden, um Cyberangriffe durchzuführen. Im Gegensatz zu professionellen Hackern fehlt ihnen oft das Verständnis für die zugrunde liegende Technik. Ihr Handeln basiert auf Nachahmung und nicht auf tiefem Verständnis der Systeme, die sie angreifen.
- Netzwerkangriffe und Täuschungstechniken
    - Spam
        - Unerwünschte Massen-E-Mails oder Nachrichten, die an eine große Anzahl von Empfängern gesendet werden. Das Hauptziel ist oft Werbung, aber es kann auch schädlichen Code oder betrügerische Inhalte enthalten.
    - Phishing
        - Betrügerische Methode, bei der Angreifer vorgeben, legitime Entitäen zu sein, um persönliche Informationen wie Benutzernamen, Passwörter oder Finanzdaten von ahnungslosen Opfern zu stehlen. Dies geschieht oft über gefälschte E-Mails oder Websites.
    - Sniffing
        - Abfangen und Überwachen von Netzwerkdatenverkehr. Dies kann dazu verwendet werden, sensible Informationen wie Benutzernamen und Passwörter zu erfassen. Sniffing ist besonders gefährlich in ungesicherten Netzwerken.
    - Spoofing
        - Manipulation von Datenpaketen oder Identitätsinformationen, um vorzutäuschen, dass sie von einer vertrauenswürdigen Quelle stammen. Spoofing kann bei E-Mails, IP-Adressen oder Webseiten auftreten und dient oft dazu, betrügerische Aktivitäten zu verschleiern.
    - Man-in-the-Middle-Angriff
        - Ein Angriff, bei dem ein Angreifer den Datenverkehr zwischen zwei Parteien abfängt und möglicherweise manipuliert, ohne dass die Kommunikationspartner dies bemerken. Dies kann zu Diebstahl von sensiblen Informationen führen.
- Webanwendungsangriffe und Netzwerküberlastungen
    - SQL-Injection
        - Injektion schädlicher SQL-Codefragmente in Anwendungen, um auf Datenbanken zuzugreifen oder diese zu manipulieren.
    - XSS (Cross-Site Scripting)
        - Einschleusen von bösartigem Scriptcode in Webseiten, der dann von anderen Benutzern ausgeführt wird.
    - CSRF (Cross-Site Request Forgery)
        - Manipulation von Nutzeranfragen, um ungewollte Aktionen im Namen des authentifizierten Benutzers durchzuführen.
    - Session Hijacking
        - Übernahme einer laufenden Benutzersitzung, um unberechtigten Zugriff auf geschützte Bereiche zu erhalten.
    - DOS (Denial of Service)
        - Gezielte Überlastung eines Systems, um die Verfügbarkeit für legitime Benutzer zu beeinträchtigen.
    - DDOS (Distributed Denial of Service)

        - Koordination von Angriffen aus verschiedenen Quellen, um die Ressourcen eines Systems zu überlasten und es unzugänglich zu machen.
- Sicherheitsbedrohungen und Exploits
    - Backdoor
        - todo
    - Exploit
        - todo
    - 0-Day-Exploit
        - todo
    - Rootkit
        - todo

Kryptographie ist ein zentrales Konzept für die Sicherheit von Daten und Kommunikation.

- Verschlüsselungstechniken: Symmetrische Verschlüsselung nutzt denselben Schlüssel zum Verschlüsseln und Entschlüsseln von Daten. Asymmetrische Verschlüsselung verwendet ein Schlüsselpaar: einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln.
- Hashverfahren: Diese Technik wandelt Eingabedaten in eine feste Zeichenfolge (Hash) um. Es ist unumkehrbar und dient zur Integritätsprüfung von Daten, da eine geringfügige Änderung der Eingabe den gesamten Hash drastisch verändert.
- Cas, Zertifikate, Digitale Signaturen, PKI: Certification Authorities (CAs) geben Zertifikate aus, die die Identität von Entitäten im Internet überprüfen. Digitale Signaturen verwenden asymmetrische Verschlüsselung, um die Authentizität von Daten oder Dokumenten zu bestätigen. Public Key Infrastructure (PKI) ist ein System zur Erstellung, Verwaltung und Widerrufung von digitalen Zertifikaten.
- Techniken wie HTTPS, TLS: HTTPS (Hypertext Transfer Protocol Secure) ist ein verschlüsseltes HTTP-Protokoll, das durch SSL/TLS (Secure Sockets Layer/Transport Layer Security) gesichert wird. TLS ist eine Verschlüsselungstechnologie, die die Kommunikation zwischen Webbrowsern und Servern schützt, um die Vertraulichkeit und Integrität von Daten zu gewährleisten.

Telnet ist ein älteres Netzwerkprotokoll, das dazu dient, eine Verbindung zwischen Computern über das Internet oder ein lokales Netzwerk herzustellen. Es erlaubt einem Benutzer, eine Remote-Verbindung zu einem anderen Computer herzustellen und Befehle auszuführen, Dateien zu übertragen oder Daten zu lesen und zu schreiben.

Allerdings hat Telnet ein großes Sicherheitsproblem: Es sendet Daten, einschließlich Passwörtern, im Klartext, was bedeutet, dass sie ohne Verschlüsselung übertragen werden. Das macht es anfällig für Abhören und potenziellen Missbrauch durch Angreifer.

Hier kommt SSH ins Spiel. Secure Shell (SSH) ist ein Verschlüsselungsprotokoll, das entwickelt wurde, um die Sicherheitsprobleme von Telnet zu lösen. Es bietet eine sichere Methode, um auf entfernte Systeme zuzugreifen, indem es eine verschlüsselte Verbindung zwischen den Computern herstellt. SSH verschlüsselt die gesamte Kommunikation zwischen Client und Server, einschließlich der übertragenen Befehle, Dateien und Passwörter. Dies stellt sicher, dass sensible Informationen während der Übertragung geschützt sind und nicht von Unbefugten abgefangen werden können.

SSH verwendet verschiedene Verschlüsselungsmethoden, darunter symmetrische und asymmetrische Verschlüsselung sowie Hashing-Algorithmen, um die Sicherheit der übertragenen Daten zu gewährleisten. Es ist heute eines der am häufigsten verwendeten Protokolle für sichere Remote-Verbindungen und wird in vielen Bereichen wie Systemadministration, Datenübertragung und Cloud-Services eingesetzt.

- SSID (Service Set Identifier)
    - Beschreibung: Die SSID ist der Name des WLAN-Netzwerks. Jedes WLAN-Gerät, das eine Verbindung zu einem Netzwerk herstellen möchte, muss die SSID kennen.
    - Funktion: identifiziert das WLAN-Netzwerk und ermöglicht es Geräten, sich damit zu verbinden.
- Mac-Filter (Media Access Control)

    - Beschreibung: Mac-Filter ermöglichen die Steuerung des Zugriffs auf ein WLAN-Netzwerk basierend auf den physischen Adressen der Netzwerkadapter (MAC-Adressen) der Geräte.
    - Funktion: Erlaubt oder blockiert den Zugriff von Geräten auf das WLAN basierend auf deren MAC-Adresse.
- WPS (Wi-Fi Protected Setup)
    - Beschreibung: WPS ist eine Methode zur vereinfachten Einrichtung von sicheren WLAN-Verbindungen zwischen Geräten, ohne dass manuelle Eingaben von Netzwerkschlüsseln erforderlich sind.
    - Funktion: Einfache Konfiguration von WLAN-Geräten durch Drücken einer Taste oder Scannen eines QR-Codes.
- Wi-Fi Easy Connect
    - Beschreibung: Auch als DPP (Device Provisioning Protocol) bekannt, ermöglicht Wi-Fi Easy Connect die einfache Einrichtung von WLAN-Verbindungen zwischen Geräten durch Scannen von QR-Codes.
    - Funktion: Vereinfacht die Konfiguration von WLAN-Geräten, indem es die Notwendigkeit von manuellen Eingaben minimiert.

Diese Funktionen tragen zur Verwaltung und Sicherheit von WLAN-Netzwerken bei. Es ist wichtig, sie entsprechend den Sicherheitsanforderungen und den Bedürfnissen des Netzwerkadministrators zu konfigurieren. Beachte, dass Sicherheitspraktiken wie die Verwendung sicherer Passwörter und regelmäßige Überprüfungen der Netzwerkkonfiguration ebenfalls entscheidend sind, um ein sicheres WLAN zu gewährleisten.

- WEP (Wired Equivalent Privacy)
    - Beschreibung: Ist das ehemalige Standard-Verschlüsselungsprotokoll für WLAN. Es sollte sowohl den Zugang zum Netz regeln als auch die Vertraulichkeit und Integrität der Daten sicherstellen, entwickelt, um eine drahtgebundene Äquivalenz zu bieten.
    - Merkmale:
        - Schwache Verschlüsselung (64 oder 128 Bit), anfällig für Sicherheitslücken.
        - In der Regel nicht mehr als sicher angesehen und wird nicht mehr empfohlen.
- WPA (Wi-Fi Protected Access) - Versionen 1 und 2
    - WPA1 (PSK und Enterprise):
        - PSK (Pre-Shared Key): Ein gemeinsamer Schlüssel wird zwischen den Benutzern geteilt.
        - Enterprise (WPA-Enterprise): Nutzt einen Authentifizierungsserver (z. B. RADIUS).
    - WPA2 (PSK und Enterprise):
        - Verbesserte Verschlüsselung und Sicherheitsfunktionen im Vergleich zu WPA1.
        - PSK: Verwendet einen vorab geteilten Schlüssel für die Authentifizierung.
        - Enterprise (WPA2-Enterprise): Nutzt einen Authentifizierungsserver, oft basierend auf RADIUS.
- WPA3
    - Beschreibung:
        - Die neueste Version von Wi-Fi Protected Access (WPA).
        - Bietet verbesserte Sicherheit und Funktionen im Vergleich zu WPA2.
    - Einzelheiten können umfassen:
        - Schutz gegen Brute-Force-Angriffe.
        - Individuelle Verschlüsselung für jeden Benutzer (Individualized Data Encryption).
- RADIUS (Remote Authentication Dial-In User Service)
    - Beschreibung: Ein Protokoll und ein System zur Authentifizierung, Autorisierung und Buchführung (AAA).
    - Funktionen:
        - Authentifizierung von Benutzern gegenüber einem zentralen Server (RADIUS-Server).
        - Verwendung in Unternehmensumgebungen, um den Zugriff auf das Netzwerk zu steuern.
        - Kann in Verbindung mit WPA-Enterprise zur sicheren WLAN-Authentifizierung verwendet werden.

Diese Sicherheitsmethoden sind entscheidend für die Gewährleistung der Integrität und Vertraulichkeit von WLAN-Kommunikation. Bei der Implementierung sollte darauf geachtet werden, dass die neuesten und sichersten Protokollversionen verwendet werden, und es ist ratsam, komplexe und starke Passwörter oder Schlüssel zu wählen, um die Sicherheit weiter zu verbessern.

Endpoint-Security bezieht sich auf Sicherheitsmaßnahmen, die auf einzelnen Endgeräten wie Computern, Laptops, Smartphones oder anderen vernetzten Geräten implementiert werden, um sie vor Bedrohungen zu schützen.

- Virenscanner: Software, die das System nach Viren, Malware und anderen schädlichen Programmen durchsucht, erkennt und entfernt. Sie überwacht Dateien, E-Mails und Webseiten, um Bedrohungen zu identifizieren.
- Firewall: Eine Firewall auf Endgeräten überwacht den ein- und ausgehenden Netzwerkverkehr, um unerwünschte Zugriffe zu blockieren und das System vor potenziellen Angriffen zu schützen.
- Application Control: Steuert, welche Anwendungen auf einem Endgerät ausgeführt werden dürfen. Sie überwacht und kontrolliert den Zugriff auf bestimmte Anwendungen, um potenziell schädliche oder nicht autorisierte Programme zu verhindern.
- Datenträgerverschlüsselung: Verschlüsselt die Daten auf den Datenträgern oder Speichermedien des Endgeräts, sodass selbst bei physischem Diebstahl der Datenzugriff erschwert oder verhindert wird.

Diese Komponenten sind essenziell, um Endgeräte vor verschiedenen Arten von Bedrohungen zu schützen und die Sicherheit in einem Netzwerkumfeld zu gewährleisten.

Firewalls sind Sicherheitsvorrichtungen, die dazu dienen, Netzwerke vor unautorisiertem Zugriff, Datenlecks und anderen Bedrohungen zu schützen. Es gibt verschiedene Arten von Firewalls, die unterschiedliche Ansätze zur Kontrolle und Überwachung des Datenverkehrs in einem Netzwerk verfolgen. Hier sind einige häufige Arten von Firewalls und ihre Funktionsweisen:

Die Funktionsweise einer **Paketfilter-Firewall** beruht auf dem Prinzip des Paketfilterns auf Netzwerkebene. Diese Art von Firewall analysiert den Datenverkehr auf Basis von vordefinierten Regeln und Entscheidungen, ob ein Datenpaket durchgelassen oder blockiert wird. Hier sind die grundlegenden Schritte und Prinzipien:

- Überwachung des Datenverkehrs: Die Paketfilter-Firewall überwacht den ein- und ausgehenden Datenverkehr im Netzwerk. Dies erfolgt auf der Basis von IP-Adressen, Ports und Protokollen.
- Definition von Regelwerken: Administratoren legen vorab Regeln fest, die bestimmen, welche Arten von Datenpaketen erlaubt oder abgelehnt werden sollen. Diese Regeln basieren auf verschiedenen Parametern wie Quell- und Ziel-IP-Adressen, Ports, Protokollen usw.
- Vergleich mit Regeln: Jedes Datenpaket wird mit den vordefinierten Regeln verglichen. Die Firewall prüft, ob die Eigenschaften des Datenpakets mit den erlaubten oder gesperrten Bedingungen übereinstimmen.
- Entscheidungsfindung: Auf Grundlage des Vergleichs entscheidet die Firewall, ob das Datenpaket durchgelassen oder blockiert wird. Wenn ein Datenpaket den Kriterien der erlaubten Regeln entspricht, wird es passieren; andernfalls wird es blockiert.
- Protokollierung: Viele Paketfilter-Firewalls bieten Protokollierungsfunktionen, um den Netzwerkverkehr zu überwachen. Diese Protokolle können für Sicherheitsanalysen und Fehlersuche genutzt werden.
- Stateless Filtering: Paketfilter-Firewalls sind oft stateless, was bedeutet, dass sie Entscheidungen für jedes einzelne Datenpaket basierend auf den vordefinierten Regeln treffen, ohne den Zustand der Netzwerkverbindung zu berücksichtigen.
- Anwendung auf Netzwerkebene: Die Paketfilter-Firewall agiert auf Netzwerkebene, analysiert also den Header der Datenpakete, einschließlich IP-Adresse, Portnummer und Protokollinformationen. Inhaltsinspektion auf Anwendungsebene ist jedoch nicht vorgesehen.

Die **Stateful Packet Inspection** (SPI) ist eine fortschrittlichere Form der Paketfilterung, die nicht nur den Header eines Datenpakets analysiert, sondern auch den Status (oder Zustand) der Netzwerkverbindung berücksichtigt. Durch die Aufrechterhaltung eines Zustandskontexts kann die Stateful Packet Inspection den

Datenverkehr auf Anwendungsebene überwachen und somit zusätzliche Sicherheitsfunktionen bieten. Hier ist die Funktionsweise von Stateful Packet Inspection:

- Überwachung des Datenverkehrs: Stateful Packet Inspection überwacht den ein- und ausgehenden Datenverkehr auf Netzwerkebene. Dies beinhaltet die Analyse der Headerinformationen, einschließlich IP-Adressen, Portnummern und Protokollinformationen.
- Aufrechterhaltung des Verbindungszustands: Im Gegensatz zu Stateless Packet Filtering behält die Stateful Packet Inspection den Status jeder Netzwerkverbindung im Gedächtnis. Sie erstellt einen sogenannten "Verbindungszustandstisch" (Connection State Table), in dem die aktuellen und aktiven Netzwerkverbindungen gespeichert sind.
- Vergleich mit Verbindungszustandstisch: Jedes eintreffende Datenpaket wird nicht nur mit vordefinierten Regeln verglichen, sondern auch mit dem Verbindungszustandstisch. Dadurch wird überprüft, ob das Paket zu einer bereits bestehenden und autorisierten Netzwerkverbindung gehört.
- Dynamische Regelanpassung: Auf Basis der Analyse der Verbindungszustände kann die Stateful Packet Inspection dynamisch und kontextbezogen entscheiden, ob ein Datenpaket durchgelassen oder blockiert wird. Diese adaptive Entscheidungsfähigkeit ermöglicht eine bessere Sicherheit, da sie den Kontext des Datenverkehrs berücksichtigt.
- Inspektion auf Anwendungsebene: Durch das Wissen um den Verbindungszustand kann die Stateful Packet Inspection auf Anwendungsebene inspizieren. Dies ermöglicht eine genauere Kontrolle des Datenverkehrs und die Identifikation von unerwünschten oder schädlichen Inhalten.
- Berücksichtigung von Netzwerkprotokollen: Stateful Packet Inspection unterstützt verschiedene Netzwerkprotokolle, einschließlich TCP, UDP und ICMP. Diese Unterstützung erlaubt eine detailliertere Analyse und Kontrolle des Datenverkehrs.
- Berücksichtigung von Netzwerkzuständen: Die Stateful Packet Inspection kann verschiedene Netzwerkzustände wie den Aufbau (Handshake) und das Beenden (Termination) von Verbindungen berücksichtigen. Dies verbessert die Fähigkeit, spezifische Angriffsmuster zu erkennen.

Eine **Application Firewall**, auch als Web Application Firewall (WAF) bezeichnet, ist darauf ausgerichtet, Webanwendungen vor verschiedenen Sicherheitsbedrohungen zu schützen. Im Gegensatz zu traditionellen Firewalls, die auf Netzwerkebene agieren, arbeitet eine Application Firewall auf Anwendungsebene und bietet erweiterte Funktionen zur Überwachung und Kontrolle des Webverkehrs. Hier ist die Funktionsweise einer Application Firewall:

- Deep Packet Inspection: Eine Application Firewall führt eine tiefgehende Paketinspektion durch, um den gesamten Datenverkehr zwischen Webbrowsern und Webservern zu analysieren. Dies schließt den gesamten Inhalt der Datenpakete mit ein.
- Analyse auf Anwendungsebene: Im Gegensatz zu herkömmlichen Firewalls analysiert eine Application Firewall den Datenverkehr auf Anwendungsebene. Sie inspiziert den HTTP- und HTTPS-Verkehr und betrachtet den Inhalt von Anfragen und Antworten.
- Schutz vor Angriffen auf Anwendungsebene: Eine der Hauptfunktionen einer Application Firewall ist der Schutz vor Angriffen auf Webanwendungen. Dazu gehören SQL-Injektionen, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) und andere Angriffe, die auf Schwachstellen in der Anwendung abzielen.
- Erkennung von Anomalien und Mustern: Die Firewall analysiert den normalen Verkehr und erstellt Profile für erlaubten Verkehr. Bei Abweichungen von diesen Profilen können Anomalien erkannt und als potenzielle Angriffe behandelt werden.
- Whitelisting und Blacklisting: Administratoren können erlaubte (Whitelisting) und gesperrte (Blacklisting) Inhalte, IP-Adressen oder URLMuster festlegen, um den Zugriff auf die Webanwendung zu steuern.
- Verschlüsselte Dateninspektion: Einige Application Firewalls können den verschlüsselten Datenverkehr (HTTPS) inspizieren, um potenziell schädliche Aktivitäten zu erkennen.
- Protokollierung und Berichterstellung: Application Firewalls bieten Protokollierung und Berichterstellungsfunktionen, um Angriffe zu dokumentieren, Sicherheitsereignisse zu überwachen und Berichte für Compliance-Anforderungen zu erstellen.

- Schutz vor DDoS-Angriffen: Einige Application Firewalls verfügen über Funktionen zur Erkennung und Abwehr von Distributed Denial of Service (DDoS)-Angriffen.
- Integration mit Sicherheitsinformationen und Ereignismanagement (SIEM): Application Firewalls können in SIEM-Systeme integriert werden, um Sicherheitsinformationen zu zentralisieren und eine umfassende Analyse von Sicherheitsereignissen zu ermöglichen.

Die Funktionsweise einer Application Firewall ist darauf ausgerichtet, Webanwendungen zu schützen, indem sie den Datenverkehr auf Anwendungsebene analysiert, verdächtige Aktivitäten erkennt und proaktiv Maßnahmen ergreift, um Angriffe zu verhindern.

Die **DMZ** ist wie eine Pufferzone zwischen dem Internet und einem privaten Netzwerk. Sie beherbergt öffentliche Server wie Websites oder E-Mail-Server, aber mit etwas Abstand zum privaten Netzwerk. Durch diese Zone werden potenziell gefährliche Daten aus dem Internet gefiltert, bevor sie ins interne Netzwerk gelangen. Das schafft mehr Sicherheit, indem es das interne Netzwerk vor möglichen Angriffen oder Bedrohungen aus dem Internet schützt.

- **Firewalls:** um den Datenverkehr zwischen dem öffentlichen Internet und der DMZ sowie zwischen der DMZ und dem internen Netzwerk zu kontrollieren und zu filtern.
- **Proxy-Server:** Diese Server handhaben den Datenverkehr von außen nach innen und können als Zwischenstation fungieren, um bestimmte Arten von Anfragen zu überprüfen und zu filtern, bevor sie das interne Netzwerk erreichen.
- **Reverse Proxies:** Sie arbeiten ähnlich wie Proxy-Server, aber sie stehen auf der Seite des internen Netzwerks und helfen dabei, den eingehenden Datenverkehr zu überprüfen und zu filtern, bevor er die internen Server erreicht.
- **Öffentliche Server:** Webserver, E-Mail-Server, DNS-Server oder andere Dienste, die für den externen Zugriff bereitgestellt werden und in der DMZ platziert sind.

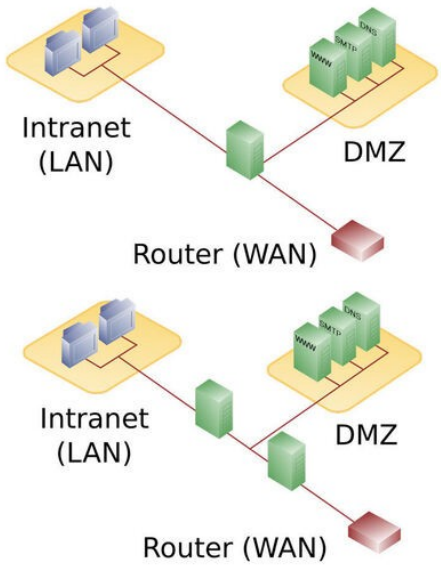

ABBILDUNG 2 UMSETZUNG EINER DMZ MIT EINER BZW. ZWEI FIREWALLS

Port-Forwarding ist eine Methode, um externen Benutzern Zugang zu Ressourcen in der DMZ zu ermöglichen. Der Vorgang sorgt dafür das Anfragen an die Netzadresse mit einem angegebenen Port an die entsprechende Ressource in der DMZ weitergeleitet werden. Beispiel: Netzadresse 16.32.64.128 → Anfrage auf 16.32.64.128:80 → Anfrage wird auf die interne IP-Adresse des Web-Servers weitergeleitet. So kann der externe Nutzer auf den Web-Server zugreifen, ohne direkt im Netzwerk verbunden zu sein.

Multi-Factor Authentication (MFA) ist ein Sicherheitsmechanismus, bei dem mehrere Authentifizierungsfaktoren erforderlich sind, um die Identität eines Benutzers zu bestätigen. Im Gegensatz zur herkömmlichen Ein-Faktor-Authentifizierung, bei der lediglich Benutzername und Passwort benötigt werden, erfordert MFA mindestens zwei der folgenden Faktoren:

- Etwas, das der Benutzer weiß (**Wissensfaktor**): Dies kann beispielsweise ein Passwort, eine PIN oder eine Antwort auf eine geheime Frage sein.
- Etwas, das der Benutzer hat (**Besitzfaktor**): Hierbei handelt es sich um physische Geräte oder Token wie Smartcards, Sicherheitstoken oder Mobiltelefone, die einen generierten Code bereitstellen.
- Etwas, das der Benutzer ist (**Identitätsfaktor**): Dies bezieht sich auf biometrische Merkmale wie Fingerabdrücke, Retina-Scans oder Gesichtserkennung.

Die Kombination mehrerer Faktoren erhöht die Sicherheit erheblich, da selbst wenn ein Faktor kompromittiert wird, der Angreifer dennoch den Zugriff auf das Konto verwehrt bleibt, solange die anderen Faktoren intakt sind.

Eine **Passwort-Policy** ist eine Sammlung von Regeln und Anforderungen, die festlegen, wie Benutzer Passwörter erstellen, verwenden und verwalten sollen. Diese Richtlinien werden implementiert, um die Sicherheit von Benutzerkonten und damit verbundenen Systemen zu erhöhen, indem bestimmte Anforderungen an die Passwörter gestellt werden. Eine effektive Passwort-Policy berücksichtigt bewährte Sicherheitspraktiken und zielt darauf ab, die Wahrscheinlichkeit von erfolgreichen Angriffen, wie beispielsweise Brute-Force-Angriffen oder Passwortdiebstahl, zu minimieren.

- **Länge und Komplexität:** Festlegung von Mindestlängen für Passwörter und Anforderungen an die Komplexität, z. B. die Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- **Passwortänderung:** Bestimmung der Häufigkeit, mit der Benutzer ihre Passwörter ändern müssen, um die Sicherheit zu erhöhen.
- **Wiederverwendung von Passwörtern:** Verhinderung der Verwendung von zuvor verwendeten Passwörtern, um sicherzustellen, dass Benutzer regelmäßig neue und einzigartige Passwörter erstellen.
- **Sperrmechanismen:** Implementierung von Kontosperrungen nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche, um vor Brute-Force-Angriffen zu schützen.
- **Biometrische Authentifizierung:** Festlegung von Anforderungen für biometrische Authentifizierungsfaktoren, wenn verfügbar.
- **Passwortrichtlinien für Administratoren:** Verschärfte Anforderungen für Passwörter von Administratoren oder anderen privilegierten Benutzern.
- **Sensibilisierung der Benutzer:** Schulung der Benutzer in Bezug auf bewährte Praktiken für die Passwortnutzung und Sensibilisierung für Phishing-Angriffe.
- **Verschlüsselung und sichere Speicherung:** Anforderungen für die sichere Speicherung von Passwörtern, einschließlich der Verwendung von sicheren Hash-Algorithmen.

II) DATENSCHUTZ

In Deutschland gelten viele Datenschutzgesetze wie zum Beispiel: Die Datenschutz-Grundverordnung (DSGVO), welche Europaweit in durchgesetzt wird und über den jeweiligen nationalen Datenschutzgesetzen steht. Das Bundesdatenschutzgesetz (BDSG), welches für öffentliche Stellen des Bundes (Bundesverwaltung), nicht-öffentliche Bereiche (Wirtschaftsunternehmen und Vereine) und die öffentliche Hand, wenn diese im Wettbewerb stehen, gilt. Die Richtlinie 2002/58/EG besser bekannt als ePrivacy-Richtlinie, diese dient als Grundlage vom Telekommunikationsgesetz (TKG), vom Telemediengesetz (TMG), vom Kreditwesengesetz (KWG), vom Geldwäschegesetz (GwG), von der Telekommunikationsüberwachungsverordnung (TKÜV), usw. Die Landesdatenschutzgesetze, diese gelten ebenfalls unter der DSGVO und dem BDSG und dienen der Regelung der Datenverarbeitung von Verwaltungen und Behörden. Das Gesetz über den Kirchlichen Datenschutz (KDG) findet in der Kirche und kirchlichen Institutionen Anwendung. Das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) als Ergänzung der Vorgaben des TKG und TMG. Und das

Patientendaten-Schutz-Gesetz (PDSG), welches unter anderem die Verarbeitung von Personenbezogenen Daten in digitalen Angeboten wie E-Rezept oder der elektronischen Patientenakte regelt.

Personenbezogene Daten

- „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“ – Artikel 4 der DSGVO
- “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)” - §46 Abs. 1 des BDSG
  - Natürliche Personen
    - Lebende Personen unabhängig ihrer Herkunft
    - Keine Gesellschaften, Vereine oder Stiftungen
    - Keine verstorbenen Personen
  - Identifizierte / Identifizierbare Personen
    - Eine Person gilt als identifiziert, wenn die Zuordnung von Daten ohne Umweg möglich ist und ein direkter Bezug hergestellt werden kann.
    - Ist dies nicht direkt, jedoch mit Zusatzwissen möglich, handelt es sich um eine identifizierbare Person. Dieses Zusatzwissen müssen Sie nicht zwangsweise selbst besitzen, es kann auch von Drittpersonen kommen.
- Welche Daten zählen dazu?
  - Name
  - Adresse
  - Telefonnummer
  - Kreditkarten- und Personalnummer
  - Autokennzeichen
  - Kontodaten
  - Online-Daten wie IP-Adresse oder Standortdaten
  - Physische Daten wie Aussehen, etc.

Datenschutz Rechte für Betroffene einer Datenerhebung

- Auskunftsrecht
  - Das Recht einer Person, von einer Organisation oder einem Unternehmen Informationen darüber zu erhalten, ob und welche personenbezogenen Daten von ihr verarbeitet werden und zu welchem Zweck.
- Recht auf Löschung (Recht auf Vergessenwerden)
  - Das Recht einer Person, die Löschung ihrer personenbezogenen Daten zu verlangen, wenn diese Daten nicht mehr erforderlich sind, unrechtmäßig verarbeitet wurden oder die betroffene Person ihre Einwilligung zurückzieht.
- Recht auf Berichtigung
  - Das Recht einer Person, unrichtige oder unvollständige personenbezogene Daten zu korrigieren oder zu vervollständigen, die von einer Organisation oder einem Unternehmen verarbeitet werden.
- Widerspruchsrecht
  - Das Recht einer Person, aus bestimmten Gründen gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen, insbesondere wenn diese Verarbeitung auf berechtigten Interessen oder für Direktmarketingzwecke erfolgt.
- Recht auf Datenübertragbarkeit
  - Das Recht einer Person, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten gegebenenfalls an eine andere Organisation zu übertragen.

Die Grundsätze des Datenschutzes sind die Gesetzmäßigkeit, d.H. die Einhaltung gesetzlicher Regelungen zum Schutz der Privatsphäre und personenbezogenen Daten der Benutzer. Verhältnismäßigkeit, was so viel bedeutet wie, es sind nur die Daten zu sichern die man für seine Geschäftsprozesse benötigt um bei einem Datenverlust der Schutz der Nutzer größtmöglich erhalten bleibt. Die Zweckbindung, was mit der Verhältnismäßigkeit einhergeht. Die Richtigkeit und Integrität, was dafür steht das die Daten so gespeichert werden, wie der

Anwender sie angibt. Und vor Veränderung von dritten und Invalidität geschützt werden. Transparenz gegenüber den betroffenen Personen, indem man dem Nutzer direkt mitteilt welche Daten man gesichert hat, oder ihm die Option der Datenauskunftsanfrage anbietet. Und zu guter Letzt Informationssicherheit, was sich auf den Schutz der Verarbeitung der Information bezieht.

Die Persönlichkeitsrechte sind im Allgemeinen die Rechte eines Individuums auf die freie Entfaltung und Achtung seiner Persönlichkeit. Entsprechend finden sich die Persönlichkeitsrechte z.B. im strafrechtlichen Ehrschutz, im zivilrechtlichen Schutz des Namens, im Recht am eigenen Bild, im Urheberrecht oder im Recht auf informelle Selbstbestimmung wieder.

Das Persönlichkeitsrecht ist ein Grundgesetz, welches jeden Teil einer Person, der für sie charakteristisch ist, schützt. Zum Beispiel den Namen, die Stimme oder das Aussehen. Zusätzlich schützt es auch die Ehre sowie die Privatsphäre eines Menschen.