1) IT-Trends - Einleitung / Überblick

Frage: Eine Liste mit mindestens 6 IT-Trends benennen und jeden Begriff kurz erläutern.

- **Cloud Computing** - IT-Ressourcen über das Internet flexibel und skalierbar nutzbar (z. B. Rechenleistung, Speicher). Pay-as-you-go und ortsunabhängig.
- **Industrie 4.0** - Vernetzte, automatisierte Produktion. Maschinen kommunizieren selbstständig (z. B. Predictive Maintenance in Werkstätten).
- **Internet of Things (IoT)** - Vernetzung physischer Geräte (Sensoren, Fahrzeuge, Maschinen). Grundlage für Smart City und Bahninfrastruktur.
- **Big Data** - Verarbeitung riesiger Datenmengen. Erkennt Muster und Trends, z. B. Auslastung von Zügen oder Energieverbrauch.
- **Künstliche Intelligenz (KI)** - Systeme lernen aus Daten (Chatbots, Prognosen, Bilderkennung). Beispiel: Verspätungsprognosen bei der DB.
- **Microservices** - Anwendungen bestehen aus kleinen, unabhängigen Diensten. Jeder Dienst erfüllt eine bestimmte Aufgabe.
- **Edge Computing** - Datenverarbeitung nahe an Sensoren oder Zügen. Reagiert schnell ohne Internetverbindung.

Beispiel Deutsche Bahn: IoT-Sensoren an Zügen senden Daten in Echtzeit an eine Cloud-Plattform, KI bewertet Zustände der Fahrzeuge, Microservices kümmern sich um Wartungs- und Planungsprozesse.

Frage: Unterschied zwischen Cloud Computing und Edge Computing erläutern.

- Cloud: zentrale Verarbeitung in Rechenzentren, hohe Rechenleistung, gut für Analysen und große Datenmengen.
- Edge: dezentrale Verarbeitung vor Ort (z. B. im Zug), geringe Latenz und unabhängig vom Internet.
- Praxis: Edge für Echtzeitdaten (z. B. Bremssensoren), Cloud für langfristige Analyse und KI-Training.

Frage: Anwendungsfälle für KI erläutern.

- Sprach- und Bilderkennung (Chatbots, Ticket-Scanner).
- Prognosen: Auslastung, Energiebedarf, Wartung.
- Automatisierte Text- und Dokumentanalyse.
- Verspätungs- und Fahrplanprognosen bei der DB.

Frage: Grundprinzipien der IT-Sicherheit darstellen.

- CIA-Triade: Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit).
- AAA-Prinzip: Authentication, Authorization, Accounting.
- Zero-Trust-Prinzip: kein Standardvertrauen, alles wird überprüft.
- Defense-in-Depth: mehrere Sicherheitsschichten.
- Praxis DB: Zugriffe per MFA, Verschlüsselung, BSI-Grundschutz.

2) Cloud Computing & REST-Schnittstellen

Frage: Eine REST-Schnittstelle auf der Kommandozeile bedienen.

Beispiel mit curl:

GET - Daten abrufen: curl -i https://api.db.example.com/v1/trains/ICE123 POST - Daten senden: curl -X POST -H "Content-Type: application/json" -d '{"status":"ready"}' https://api.db.example.com/v1/trains Tipp: -i zeigt Header, -v Debug, -sS still mit Fehlern

Frage: Aufbau einer REST-Schnittstelle beschreiben.

- Ressourcenorientiert: eindeutige URLs (z. B. /v1/trains/ICE123).
- HTTP-Methoden: GET, POST, PUT, PATCH, DELETE.
- Antwortformat: meist JSON.
- Statuscodes: 200 OK, 201 Created, 404 Not Found, 500 Error.
- Authentifizierung über Token (Bearer).
- Versionierung über Pfad (z. B. /v1) oder Header.

Frage: Wesentliche Eigenschaften und Vorteile einer REST-Schnittstelle benennen.

- Einheitliche HTTP-Schnittstelle, leicht verständlich.
- Zustandslos (stateless) - einfach skalierbar.
- Cachbar - schnellere Antworten.
- Lose gekoppelt - unabhängige Entwicklung.
- Standardisiert - viele Tools verfügbar.

Frage: Microservice-Architektur von einer Service-orientierten Architektur (SOA) unterscheiden.

- SOA: zentrale Dienste, oft schwerfällig (z. B. ESB).
- Microservices: klein, unabhängig, leicht austauschbar.
- Eigene Datenhaltung je Service.

- Kommunikation über REST oder Messaging.
- Beispiel DB: Buchung, Bezahlung und Benachrichtigung sind getrennte Services.

Frage: Beispiel für eine Anwendung mit Microservice-Architektur und REST-Schnittstelle beschreiben.

- Beispiel: DB-Online-Ticketverkauf.
- Services: Auth-Service, Buchungs-Service, Zahlungs-Service, Benachrichtigungs-Service.
- Kommunikation per REST-API (z. B. POST /tickets).
- Jeder Service hat eigene Datenbank und kann unabhängig aktualisiert werden.

3) Cloud Computing - Einleitung / Überblick

Frage: Cloud definieren.

- Bereitstellung von IT-Ressourcen über das Internet (Rechenleistung, Speicher, Software).
- NIST-Definition: Zugriff auf konfigurierbare Ressourcen, schnell und bedarfsabhängig bereitgestellt.
- Servicemodelle: IaaS, PaaS, SaaS, FaaS.

Frage: Bildliche Darstellung der Cloud-Definition.

- Cloud = IT aus der Steckdose: Nutzung nach Bedarf, Abrechnung nach Verbrauch.
- Anbieter betreibt Hardware, Sicherheit, Skalierung.

Frage: Argumente gegen Cloud-Verwendung.

- Datenschutz / DSGVO / KRITIS-Auflagen.
- Vendor-Lock-in - Anbieterbindung.
- Netzabhängigkeit (Offline-Risiko).
- Kosten bei Dauerlast / Egress-Traffic.
- Komplexität bei Migration alter Systeme.

Frage: Argumente für Cloud-Verwendung.

- Schnelle Bereitstellung und Skalierbarkeit.
- Kostenersparnis durch Pay-as-you-go.
- Weniger Wartungsaufwand durch Managed Services.
- Globale Erreichbarkeit, hohe Ausfallsicherheit.
- Schnelle Innovation durch neue Features.

Frage: Prozess beim Praxispartner, der sich per Cloud verbessern lässt.

- Prozess: Rechnungsfreigabe und Archivierung.
- Cloud-Lösung: automatischer Workflow mit KI-Belegerkennung.
- Audit-Trails, Zugriffskontrolle (MFA), API-Anbindung an ERP.
- Ergebnis: schnellere Abläufe, bessere Nachvollziehbarkeit.

Frage: Beispiel-Services einer Cloud benennen.

- IaaS - Virtuelle Maschinen, Storage, Netzwerke.
- PaaS - Datenbanken, Queues, Serverless-Plattformen.
- SaaS - CRM, Office-Tools, E-Mail-Dienste.
- FaaS - kleine Funktionen auf Abruf (z. B. AWS Lambda).
- Security-Dienste - IAM, WAF, KMS.