

1.1 Datensicherheit – Grundlagen, TOMs und Zugriffsrechte

Überblick

Datensicherheit ist ein Zusammenspiel aus Technik, Organisation und bewusstem Verhalten. Diese Lernseite behandelt Schutzziele, Kontrollen und Berechtigungen.

So lernst du: Beantworte jede Frage zuerst selbst und klappe anschließend die Musterantwort auf.

Grundlagen und Schutzziele

1. Was versteht man unter Datensicherheit?

Maßnahmen, die Daten gegen Verlust, unerlaubte Veränderung und unberechtigte Nutzung schützen. Dazu gehören beispielsweise Sicherungskopien, Berechtigungen und Verschlüsselung.

2. Welche drei grundlegenden Schutzziele gibt es?

- **Vertraulichkeit:** Nur Berechtigte können Informationen einsehen.
- **Integrität:** Informationen bleiben korrekt und vollständig; unerlaubte Veränderungen werden verhindert oder erkannt.
- **Verfügbarkeit:** Informationen und Dienste sind zum benötigten Zeitpunkt nutzbar.

3. Ordne zu: Kundendaten werden veröffentlicht, Rechnungen manipuliert, ein Server fällt aus.

Veröffentlichung → **Vertraulichkeit**. Manipulation → **Integrität**. Serverausfall → **Verfügbarkeit**. Ein Vorfall kann mehrere Schutzziele gleichzeitig beeinträchtigen.

4. Was unterscheidet Datenschutz und Datensicherheit?

Datenschutz betrifft den Umgang mit personenbezogenen Informationen und den Schutz der betroffenen Menschen. Datensicherheit schützt Daten unabhängig davon, ob sie einen Personenbezug haben. Beide Bereiche überschneiden sich.

Technische und organisatorische Maßnahmen

5. Was sind TOMs? Nenne technische und organisatorische Beispiele.

Technische und organisatorische Maßnahmen. Technisch: Verschlüsselung, Firewall, MFA. Organisatorisch: Schulungen, geregelte Rechtevergabe, dokumentierte Backup-Verantwortung und Notfallabläufe.

6. Wie unterscheiden sich Zutritts-, Zugangs- und Zugriffskontrolle?

- **Zutritt:** Wer darf in den Serverraum?
- **Zugang:** Wer darf sich am System anmelden?
- **Zugriff:** Wer darf eine bestimmte Datei lesen, ändern oder löschen?

Merksatz: Raum → System → Daten.

7. Wozu dienen Weitergabe- und Eingabekontrolle?

Weitergabekontrolle: Informationen bei Übermittlung und Weitergabe schützen, etwa durch verschlüsselte Verbindungen. **Eingabekontrolle:** Änderungen nachvollziehbar machen, beispielsweise über Protokolle mit Benutzer, Zeitpunkt und Aktion.

8. Was bedeuten Auftragskontrolle, Verfügbarkeitskontrolle und Datentrennung?

Auftragskontrolle: Verarbeitung gemäß festgelegten Vorgaben. **Verfügbarkeitskontrolle:** Ausfälle und Verlust abfangen. **Datentrennung:** Bestände für unterschiedliche Zwecke oder Mandanten getrennt halten.

Identität und Berechtigungen

9. Was unterscheidet Authentifizierung und Autorisierung?

Authentifizierung: Identität prüfen – „Wer bist du?“ **Autorisierung:** Berechtigung prüfen – „Was darfst du?“ Ein erfolgreicher Login erlaubt nicht automatisch den Zugriff auf alle Daten.

10. Welche Authentifizierungsfaktoren gibt es?

- **Wissen:** Passwort oder PIN.
- **Besitz:** Sicherheitsschlüssel oder registriertes Gerät.
- **Sein:** biometrisches Merkmal, etwa Fingerabdruck.

11. Sind Passwort und PIN zusammen eine Zwei-Faktor-Authentifizierung?

Nein. Beide gehören zur Kategorie Wissen. MFA kombiniert unabhängige Faktoren verschiedener Kategorien, zum Beispiel Passwort und Sicherheitsschlüssel.

12. Wie unterscheiden sich RBAC, ABAC und ACL?

- **RBAC:** Rechte folgen Rollen, etwa „Buchhaltung“.
- **ABAC:** Regeln werten Attribute aus, etwa Abteilung, Schutzklasse und Gerät.
- **ACL:** Eine Zugriffsliste legt Berechtigte und erlaubte Aktionen für ein Objekt fest.

13. Was bedeuten Least Privilege und Need-to-know?

Least Privilege: Nur die für eine Aufgabe notwendigen Rechte vergeben. **Need-to-know:** Informationen nur bei fachlichem Bedarf zugänglich machen. Ein Mitarbeiter benötigt beispielsweise Leserechte für einen Bericht, aber keine Löschrechte auf dem gesamten Laufwerk.

14. Warum müssen Rechte regelmäßig überprüft werden?

Aufgaben und Zuständigkeiten ändern sich. Nicht mehr benötigte Berechtigungen werden entzogen; bei Austritt wird der Zugang gesperrt. Sonst sammeln sich überflüssige Rechte an.

15. Was bedeutet Funktionstrennung?

Kritische Arbeitsschritte werden auf mehrere Personen verteilt. Beispiel: Eine Person legt einen Zahlungsempfänger an, eine andere genehmigt die Zahlung. Das erschwert Missbrauch und reduziert Fehler.

Merksatz

Schutzziel bestimmen → passende Kontrolle auswählen → Wirksamkeit prüfen.

Prüfungshinweis

Nenne bei Maßnahmen immer den Zweck. „Verschlüsselung schützt bei verlorenen Datenträgern die Vertraulichkeit“ ist aussagekräftiger als nur „Verschlüsselung“.

Quellen und Einordnung

Themenrahmen: [FI-Wiki – Datensicherheit](#). Die Fragen, Beispiele und Musterantworten sind eigenständig als Lernhilfe formuliert; keine offiziellen IHK-Prüfungsfragen.

Vertiefung zu Berechtigungen: [OWASP – Authorization Cheat Sheet](#).
