IT-Sicherheit 1 (Grundlagen) – Zusammenfassung mit IHK-Bezug

Datensicherheit, Datenschutz, Datensicherung, Risiken, Schutzziele VIVA / CIA

🔐 IT-Sicherheit 1 – Grundlagen

📘 Grundlage: Folien „IT-Sicherheit: Einführung“ (GBS Fachschule, 9 Folien). Die Zusammenfassung folgt der Reihenfolge der Folien.

🧭 So liest du dieses Dokument

- **Fett** gedruckte Begriffe sind Prüfungs-Schlagwörter. Die solltest du erklären können.
- 🎯 Jeder Abschnitt hat eine Zeile „IHK-Relevanz“. Das ist eine eigene Einschätzung, keine amtliche Angabe.
- IT-Sicherheit passt zu diesen Prüfungsteilen (AO 2020):
  - **AP1** („Einrichten eines IT-gestützten Arbeitsplatzes“): Schutzbedarf, Schutzziele, Datenschutz, einfache Schutzmaßnahmen.
  - **AP2 Konzeption und Administration** und **Netzwerke**: Sicherheitskonzepte, Verschlüsselung, Backup, Zugriffsschutz.
  - **WiSo**: Datenschutz (DSGVO) am Rand.
- ✏️ Am Ende jedes Blocks stehen Übungsfragen. Die Lösungen stehen gesammelt am Ende.
- 🔎 „Ergänzung“ = steht nicht auf den Folien, aus Allgemeinwissen ergänzt.

Symbol	Bedeutung
🎯	IHK-Relevanz
💡	Merkhilfe
⚠️	Typischer Fehler / Falle
🔎	Ergänzung (nicht auf den Folien)

🗺️ Block 1: Worum geht es im Fach?

🎯 IHK-Relevanz: gering – Überblick.

Der Themenplan des Fachs:

Thema	Frage dahinter	Schutzziel
Verschlüsselung / Kryptographie	Bleibt Vertrauliches vertraulich?	Vertraulichkeit
Signaturen und Zertifikate	Wurden Daten verändert? Ist die Quelle echt?	Integrität, Authentizität
Backup, USV usw.	Sind Daten und Systeme da, wenn man sie braucht?	Verfügbarkeit
Zugangskontrolle	Kommt kein Unbefugter in Räume oder an Daten?	Vertraulichkeit
Angriffe & Schutzmaßnahmen	Welche Angriffe gibt es, wie schützt man sich?	alle
Datenschutz	Was verlangt die DSGVO?	– (Gesetz)
Sonstiges	Cloud, Tracking, E-Mail, Social Media, Blockchain	–

💡 Fast jedes Thema gehört zu einem Schutzziel (Block 4). Das hilft beim Einordnen.

📖 Block 2: Drei Begriffe, die oft verwechselt werden

🎯 IHK-Relevanz: **hoch** – Begriffe werden gern abgefragt („Grenzen Sie ab …“).

Begriff	Was wird geschützt?	Pflicht?
Datensicherheit	**alle** Daten – vor Verlust, Manipulation, Ausspähen	Ermessen des Einzelnen / Unternehmens
Datenschutz	nur **personenbezogene** Daten	**Gesetz**: DSGVO, „Recht auf informationelle Selbstbestimmung“
Datensicherung	Kopie wichtiger Daten (**Backup**)	eine **Maßnahme** für Datensicherheit

💡 Merksatz: **Datenschutz schützt Menschen, Datensicherheit schützt Daten, Datensicherung ist das Backup.**

⚠️ Falle: Datensicherung ist **kein** Oberbegriff. Sie ist nur **eine** Maßnahme, um Datensicherheit zu erreichen.

🔎 Ergänzung: **Personenbezogene Daten** = alle Angaben, mit denen man eine Person erkennen kann. Beispiele: Name, Adresse, E-Mail, IP-Adresse, Personalnummer.

✏️ Übungsfragen Block 2

Ü2.1 Ein Unternehmen sichert jede Nacht seinen Fileserver auf Band. Ist das Datenschutz, Datensicherheit oder Datensicherung?

Ü2.2 Warum ist eine Kundenliste ein Fall für den Datenschutz, eine Konstruktionszeichnung aber nicht?

⚡ Block 3: Woher kommen Risiken?

🎯 IHK-Relevanz: **mittel bis hoch** – oft als Einstieg in Aufgaben zu Schutzbedarf und Maßnahmen.



Risiken mit und ohne menschliches Eingreifen

Ohne menschliches Eingreifen (niemand hat Schuld): defekte Hardware, Software-Fehler (**Bugs**), Stromausfall, Feuer, Wasser, Naturkatastrophen.

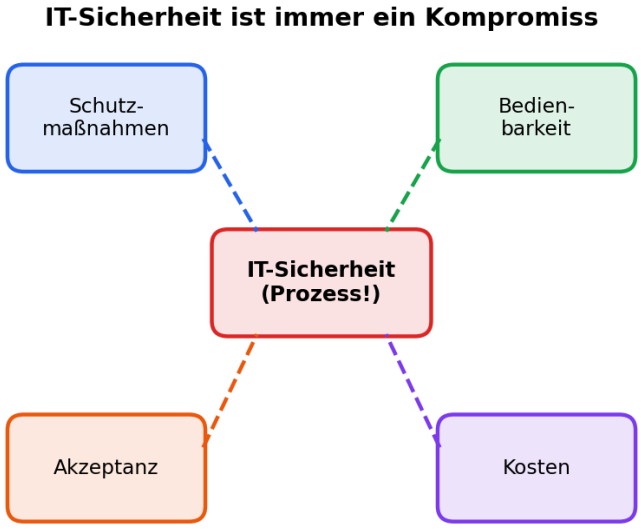
Mit menschlichem Eingreifen – drei Arten:

1. **Unachtsamkeit / Fahrlässigkeit**: falsche Eingaben, Passwort am Monitor, Stecker ziehen, versehentlich löschen, Mail-Anhang öffnen.
2. **Gezielte Angriffe**: Angriffe auf Server, **Schadsoftware**, Diebstahl, Sabotage.
3. **Fehler in der Organisation**: kein Notfallplan, keine Kontrolle, niemand ist zuständig.

💡 Der Mensch ist die größte Schwachstelle. Darum gehören **Schulungen** immer zu den Schutzmaßnahmen.

🔄 Sicherheit ist kein Zustand

- IT-Sicherheit ist ein **Prozess**. Man ist nie „fertig“. Neue Lücken und Angriffe kommen ständig dazu.
- IT-Sicherheit ist immer ein **Kompromiss** zwischen vier Dingen:



Kompromiss

Beispiel: Ein 30-stelliges Passwort, das jede Woche wechselt, ist sehr sicher. Es ist aber unbequem (Bedienbarkeit). Mitarbeiter schreiben es auf einen Zettel (Akzeptanz). Am Ende ist es **unsicherer**.

🔎 Ergänzung: Der Prozess-Gedanke steckt auch im **PDCA-Zyklus** (Plan – Do – Check – Act) und im **BSI IT-Grundschutz**.

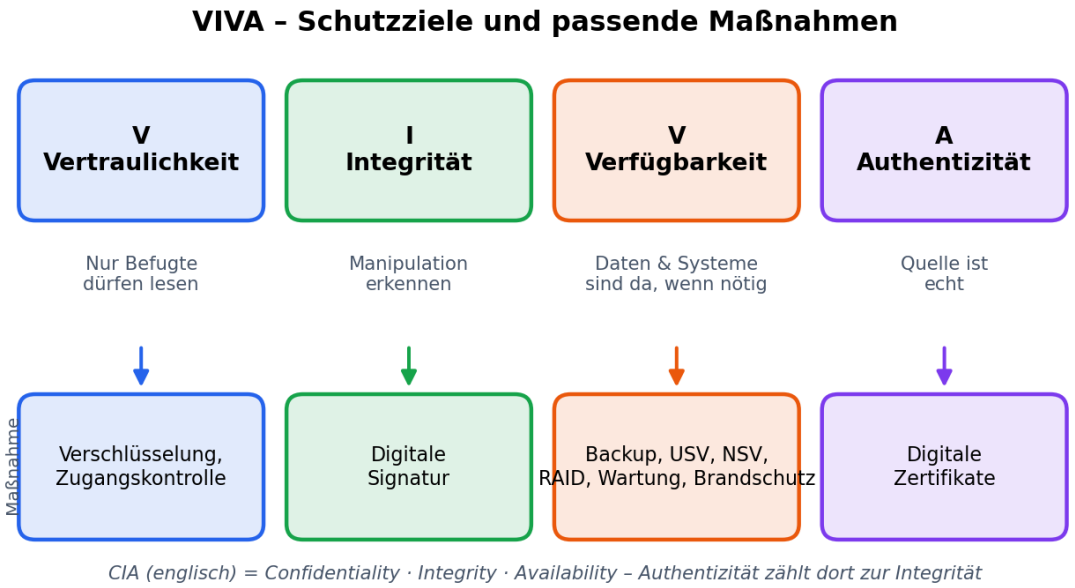
✏️ Übungsfragen Block 3

Ü3.1 Nennen Sie je zwei Risiken mit und ohne menschliches Eingreifen.

Ü3.2 Warum ist „Wir haben 2024 eine Firewall gekauft, also sind wir sicher“ falsch?

🛡️ Block 4: Die Schutzziele – VIVA und CIA

🎯 IHK-Relevanz: **sehr hoch** – kommt in fast jeder Prüfung zum Thema Sicherheit.



VIVA – Schutzziele und Maßnahmen

Schutzziel	Bedeutung	Typische Maßnahme
Vertraulichkeit	Nur Befugte dürfen Daten sehen.	**Verschlüsselung**, Zugangs- und Zugriffskontrolle
Integrität	Daten sind nicht verändert. Manipulation kann man nicht immer verhindern, aber **erkennen**.	**Digitale Signatur** (🔎 auch Hashwerte)
Verfügbarkeit	Daten und Systeme sind da, wenn man sie braucht.	**Backup**, **USV**, NSV, **RAID**, Wartung, Brandschutz
Authentizität	Die Quelle ist echt und überprüfbar.	**Digitale Zertifikate**

Weitere Schutzziele: **Nichtabstreitbarkeit** (Verbindlichkeit), Verlässlichkeit, Anonymität.

CIA – die englische Variante

Englisch	Deutsch
Confidentiality	Vertraulichkeit
Integrity	Integrität
Availability	Verfügbarkeit

Bei **CIA** fehlt die Authentizität. Grund: Signaturen und Zertifikate funktionieren technisch fast gleich. Authentizität gilt hier als **Sonderfall der Integrität**. Manche deutschen Texte nennen sie dann „erweitertes Schutzziel“.

💡 Eselsbrücke: **VIVA** – „Vertraulich, Intakt, Verfügbar, Authentisch“.

🔎 Ergänzung: **USV** = unterbrechungsfreie Stromversorgung (Akku, überbrückt Minuten). **NSV** = Notstromversorgung, meist eine **Netzersatzanlage** (NEA, z. B. Diesel-Aggregat), für längere Ausfälle (Stunden bis Tage).

⚠️ Falle: **RAID ist kein Backup!** RAID schützt vor einem Plattendefekt (Verfügbarkeit). Löscht jemand eine Datei oder kommt Ransomware, ist sie auf allen Platten weg.

✏️ Übungsfragen Block 4

Ü4.1 Ordnen Sie zu: (a) Serverraum mit Chipkarte, (b) tägliches Backup, (c) E-Mail mit Signatur, (d) HTTPS-Zertifikat einer Bank.

Ü4.2 Ein Hacker ändert in einer Datenbank Kontonummern. Welches Schutzziel ist verletzt?

Ü4.3 Wofür steht CIA? Warum fehlt dort die Authentizität?

Ü4.4 Der Chef sagt: „Wir haben RAID 1, ein Backup brauchen wir nicht.“ Was antworten Sie?

✅ Lösungen

Ü2.1 Datensicherung (Backup). Sie ist eine Maßnahme für die Datensicherheit (Verfügbarkeit).

Ü2.2 Die Kundenliste enthält **personenbezogene** Daten (Namen, Adressen) → DSGVO gilt. Die Zeichnung enthält keine Personendaten → Datensicherheit, aber kein Datenschutz.

Ü3.1 Ohne Mensch: Stromausfall, Festplattendefekt, Wasserschaden, Bug. Mit Mensch: versehentliches Löschen, Phishing-Anhang öffnen, Hackerangriff, Diebstahl.

Ü3.2 Sicherheit ist ein Prozess. Neue Lücken und Angriffe entstehen ständig. Die Firewall muss gepflegt, aktualisiert und geprüft werden. Andere Risiken (Mensch, Stromausfall) deckt sie gar nicht ab.

Ü4.1 (a) Vertraulichkeit (Zugangskontrolle) · (b) Verfügbarkeit · (c) Integrität (+ Authentizität) · (d) Authentizität.

Ü4.2 Integrität.

Ü4.3 Confidentiality, Integrity, Availability. Authentizität wird als Sonderfall der Integrität gesehen, weil Signaturen und Zertifikate technisch fast gleich arbeiten.

Ü4.4 RAID schützt nur vor Plattenausfall. Gegen Löschen, Ransomware, Brand oder Diebstahl hilft nur ein Backup, am besten getrennt vom Server gelagert (🔎 3-2-1-Regel: 3 Kopien, 2 Medien, 1 außer Haus).