



Lernen: Sind die drei elementaren Kriterien, die bei der Schutzbedarfsanalyse gewichtet („normal, hoch, sehr hoch“) und abgesichert werden sollen.



Vertraulichkeit

Nur **autorisierte** Personen haben Zugriff zu den Informationen.

Umsetzung: Passwörter, Zugriffsbeschränkungen, Verschlüsselung.



Integrität

Die Informationen sind **vollständig** und **unverändert**.

Umsetzung: Prüfsummen, Hash-Funktionen.



Verfügbarkeit

Informationen sind zu den gewünschten Zeitpunkten garantiert **verfügbar**

Umsetzung: RAID-Systeme, Notstrom/USV, Backups, redundante Architektur,...



Authentizität (erweitertes Ziel der Integrität)

Die Information/ihr Absender ist **echt/vertrauenswürdig**.

Umsetzung: Digitale Signatur, 2FA, Biometrie, Token

Ziele werden je nach Unternehmen unterschiedlich hoch gewichtet

Beispiel Vertraulichkeit:

Eine Kanzlei nutzt ein System zur E-Mail-Verschlüsselung (z. B. PGP oder S/MIME), bei dem die E-Mail-Inhalte sowohl auf dem Weg vom Absender zum Empfänger als auch bei der Speicherung verschlüsselt werden. Nur der berechtigte Empfänger kann die Nachrichten entschlüsseln und lesen. Damit wird sichergestellt, dass, selbst wenn jemand den Datenverkehr abfängt, die Inhalte nicht lesbar sind. (Technische Maßnahme: Verschlüsselung; organisatorische Maßnahme: Schulung der Mitarbeitenden zur korrekten Nutzung des Mailsystems)

Beispiel Integrität:

Die Hash-Prüfung stellt sicher, dass die Integrität eines Software-Updates gewahrt bleibt, indem der berechnete Hash-Wert des heruntergeladenen Updates mit dem ursprünglich veröffentlichten Hash-Wert verglichen wird, wodurch jede unbemerkte Änderung oder Manipulation der Datei erkennbar wäre.

Beispiel Verfügbarkeit:

Ein E-Commerce Unternehmen verwendet Lastverteilung (Load Balancing) und redundante, geografisch verteilte Server, um sicherzustellen, dass der Onlineshop auch bei hohem Besucheraufkommen oder Serverausfällen erreichbar bleibt.