8.1 Schutzziele und Angriffe

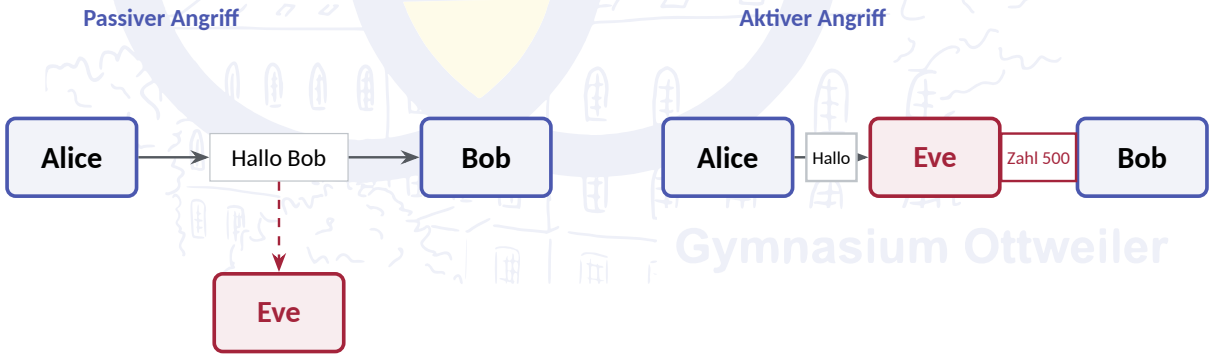
Bevor man ein Verfahren auswählt, muss klar sein, wovor es eigentlich schützen soll. Die IT-Sicherheit unterscheidet drei Grundforderungen.

Schutzziel	Leitfrage	Beispiel für eine Verletzung
Vertraulichkeit	Kann ein Dritter die Nachricht lesen?	Jemand liest im offenen WLAN die Bestellung mit.
Integrität	Ist die Nachricht unverändert angekommen?	Die Kontonummer in einer Überweisung wird unterwegs ersetzt.
Authentizität	Stammt die Nachricht wirklich vom angegebenen Absender?	Eine Mail gibt sich als Nachricht der Schulleitung aus.

Häufig kommt als viertes Ziel die **Verbindlichkeit** hinzu: Der Absender soll später nicht abstreiten können, die Nachricht geschickt zu haben.

Angriffe auf diese Ziele teilt man in zwei Gruppen:

- **Passiver Angriff.** Der Angreifer liest nur mit. Er verletzt die Vertraulichkeit, verändert aber nichts. Solche Angriffe hinterlassen keine Spuren und sind darum kaum zu entdecken – man kann sie nur *verhindern*, indem man den Inhalt unlesbar macht.
- **Aktiver Angriff.** Der Angreifer verändert, wiederholt, verzögert oder unterdrückt Nachrichten oder gibt sich als jemand anderes aus (Maskerade). Solche Angriffe lassen sich nicht verhindern, denn die Leitung gehört dem Angreifer genauso wie uns. Man kann sie nur *erkennbar* machen.



Eve liest mit und ändert nichts. Keine Spur — nur zu *verhindern*, nicht zu erkennen.

Eve ersetzt, wiederholt oder unterdrückt. Nicht zu verhindern — nur *erkennbar* zu machen.

Passiver und aktiver Angriff. Links stiehlt Eve nur Information, rechts greift sie in den Verkehr ein.

Merke

Passive Angriffe muss man verhindern, aktive Angriffe muss man erkennen. Verschlüsselung allein schützt nur die Vertraulichkeit – für Integrität und Authentizität braucht es zusätzliche Werkzeuge (Abschnitt 8.11).

Arbeitsauftrag 1

1. Ordnen Sie zu, welches Schutzziel jeweils verletzt wird: (a) Ein Angreifer schneidet den Netzwerkverkehr mit. (b) Eine Bestellung wird von 1 auf 100 Stück geändert. (c) Ein Erpresser verschlüsselt alle Dateien einer Firma. (d) Eine gefälschte Absenderadresse verschickt Rechnungen.
2. Begründen Sie, warum ein aktiver Angriff meist einen passiven voraussetzt.
3. Nennen Sie für jedes der drei Schutzziele eine Situation aus Ihrem eigenen Alltag, in der Sie sich darauf verlassen.