## Was ist Informatik

Informatik = Kunstwort aus ”Information” und ”Mathematik” bzw. ”Automatik”.

**Wissenschaft** von den elektronischen Datenverarbeitungsanlagen und den Grundlagen ihrer Anwendung.

Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung

**Theoretische Informatik:**

* **Formale Basis** der Informatik → macht die Informatik zu einer **Wissenschaft**.
* **Grundlage aller anderen Teilgebiete**
* Beispiel für Theoretische Informatik: Konzept der **Turing Maschine** von Alan Turing
* Kernthemen
  + Automatentheorie (Statemaschine)
  + Berechenbarkeit (Turing Maschine)
  + Komplexitätstheorie (können alle Probleme, die in polynomialer Zeit gelöst werden, auch in polynomialer Zeit überprüft werden)
  + Formale Sprachen (regex)
  + Informationstheorie (Zb übertragung von informationen)
  + Logik (Aussagenlogik)

**Technische Informatik**

* **Bau von Rechnern** vom Transistor bis zu vollständigen System und bis zur Vernetzung mehrerer Systeme.
* **Schnittstelle** der Informatik zur Elektrotechnik.
* Kernthemen
  + Hardware
  + Gatter-Logik: Schaltnetze und Schaltwerke
  + Rechnerorganisation und -architektur
  + Mikroprogrammierung
  + Netzwerke
  + Systemnahe Software

**Praktische Information = ”Programmierung”**

* **Prinzipien**, **Methoden** und **Werkzeuge** zur Entwicklung von Software
* Kernthemen
  + Software Engineering (Softwaretechnik)
  + Programmiersprachen
  + Programmierparadigmen (Jedes Paradigma legt fest, wie Programme geschrieben, strukturiert und organisiert werden sollen)
  + Algorithmen und Datenstrukturen
  + Compiler
  + Betriebssysteme (Schnittstelle zur Technischen Informatik)

**Angewandte Informatik**

Anwendung der Konzept der Informatik zur Problemlösung in anderen Fachgebieten.

* Schnittstelle der Informatik zum ”Rest der Welt”.
* Anwendungsgebiete:
  + Datenbanken
  + Computergrafik und virtuelle Realität
  + World Wide Web
  + Automatisierungstechnik
  + Künstliche Intelligenz (KI)
  + Computerspiele
  + Textverarbeitung und Büroautomatisierung
  + Produktionsplanung und -unterstützung
  + Medizintechnik

## 2. Motivation

Fazits aus den ganzen Fällen:

* Nicht nur Software muss sicher sein sondern auch Hardware (eg. Meltdown und Spectre Nutzen Schwachstellen im Prozessor Design aus)
* Cloud hat den Nachteil, dass wenn ein anbieter ein problem hat gleich ganz viele eines haben
* Wichtige dinge wie zugangssysteme sollten evtl nicht am selben system wie der rest laufen
* Bei supply chains muss man vorsichtig sein, was man verwendet, da man oft keine möglichkeit hat, sicherheitslücken von supplyern zu fixen oder diese dazu bringen sie zu fixen (zb billiges china zeug)
* Supply Chains problem oft bei IOT
* Immer Backups machen und auch in der lage sein diese schnell und problemlos wiederherzustellen, generell lösungen für mögliche problemfälle haben und darauf vorbereitet sein
* Passwort manager verwenden

# 3. Schutzziele der Informationssicherheit

## 3.1 Was ist Informationssicherheit? (laut BSI)

**IT-Sicherheit (Computersicherheit)** = IT-Sicherheit bezeichnet einen Zustand, in dem die **Risiken**, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene **Maßnahmen** auf **ein tragbares Maß** reduziert sind.

IT-Sicherheit ist also der Zustand, in dem **Vertraulichkeit, Integrität und Verfügbarkeit** von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

**Informationssicherheit (Information Security)** hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.  
Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Bild, das Text, Screenshot, Schrift, Kreis enthält.

Automatisch generierte Beschreibung

Informationssicherheit ist das Erkennen, Minimieren und – letztlich – bewusste Akzeptieren von Risiken! Es gibt keine 100%ige Sicherheit

## 3.2 Assets

Was sind Assets (Werte) in der Informationssicherheit?

* **Hardware** (Clients, Server, Smartphones, Netzwerkkomponenten, Gebäude/Räume, Verkabelung, ...),
* **Software** (Betriebssysteme, Business Applikationen, Tools, Eigenentwicklungen, ...)

Und

* **Daten** (Dokumente, Fotos, Audios, Videos, E-Mails, ... in jedweder Form).

Die Bedeutung von Assets hängt von der Perspektive des Eigentümers ab. Sie kann abhängig sein von

* monetären Kosten zur (Wieder-)Beschaffung,
* persönlichem Bezug des Eigentümers (z. B. private Fotos/Briefe) und
* zeitlichen Aspekten (z. B. Forschungsergebnisse eines Unternehmens).

## 3.3 Schwachstelle - Bedrohung – Risiko

* **Schwachstelle (Vulnerability):** Schwäche, z. B. im Design oder in der Implementierung eines Systems, welche ausgenutzt werden könnte, um Schaden zuzufügen.
* **Bedrohung (Threat):** Eine mögliche Gefahr, dass, unter bestimmten Umständen und unter Ausnutzung einer oder mehrerer Schwachstellen, durch einen Angriff (Attack) Schaden zugefügt werden könnte.
  + Bedrohungen durch Menschen können
    - ”gutartig” (benign, z. B. Fehler, Unfall) oder bösartig (malicious) sowie
    - ungezielt (random) oder gezielt (targeted) sein.
  + Bedrohungen durch ”höhere Gewalt” umfassen Naturkatastrophen wie Überschwemmungen, Stürme, Brände, Blackouts/Stromausfälle, Ausfälle von Hardware sein
* **Risiko (Risk):** Das Risiko einer Bedrohung ergibt sich aus der Abschätzung der Wahrscheinlichkeit des Eintritts (Risk Likelihood) und dem damit verbundenen Schadensausmaß (Risk Impact).

## 3.4 Schutzziele

Die Informationssicherheit hat das Gewährleisten folgender Schutzziele/Grundwerte zur Aufgabe:

* Vertraulichkeit (Confidentiality),
* Integrität (Integrity),
* Verfügbarkeit (Availability),
* Authentizität (Authenticity) und
* Verbindlichkeit (Accountability)

**Vertraulichkeit**

Schutz vor **unerlaubter Preisgabe** von Daten/Information  
durch die **autorisierte** **Beschränkung** von Informationszugriff und Offenlegung einschließlich Maßnahmen zum Schutz von Privatsphäre

Vertraulichkeit im täglichen Leben, z. B.

* Brief- und Fernmeldegeheimnis
* Amtsverschwiegenheit
* Verschwiegenheitspflichten von Anwälten, Notaren, Ärzten, ...
* Beichtgeheimnis
* Geheimhaltungsvereinbarungen zw. Parteien (Non-Disclosure Agreements, NDAs)

**Integrität**

Schutz vor **unerlaubter Veränderung** von Daten/Information aber auch Systemen   
(und Gewährleistung der Verbindlichkeit / Nicht-Abstreitbarkeit (non-repudiation) und Authentizität von Informationen)

Veränderung kann durch aktive Angriffe oder auch durch z. B. Übertragungs- oder Speicherfehler passieren

Oft werden Integrität, Authentizität und Verbindlichkeit als eine Einheit gesehen (siehe Definition)

**Verfügbarkeit (Availability)**

Die Eigenschaft eines Systems oder einer Systemressource, auf Anfrage einer autorisierten Stelle gemäß den Leistungsspezifikationen für das System zugänglich und nutzbar zu sein.

Verfügbarkeit ist keine binäre Eigenschaft (ja/nein) → Verfügbarkeit muss definiert werden, z. B.

* Verfügbarkeitsklassen 2 (99 %) bis 6 (99,9999 %),
* Fortschritts- bzw. Wartezeiten bei Aufträgen,
* Vorrat an Speicherkapazität, ...

**Authentizität (Authenticity)**

Die Eigenschaft, echt zu sein und überprüfbar und vertrauenswürdig zu sein; Vertrauen in die Gültigkeit einer Übertragung, einer Nachricht oder des Absenders einer Nachricht

* Entity Autenticity = Ich weiß, mit wem ich kommuniziere.
* Data Origin Authenticity = Ich weiß, von wem Daten stammen.
* Authentication = Vorgang, um Authentizität zu erlangen. (Im Deutschen komplizierter)

**Authentisierung vs. Authentifizierung**

Ein Bild, das Text, Diagramm, Entwurf, Screenshot enthält.

Automatisch generierte Beschreibung

**Autorisierung** = Einräumung von Rechten an die authentifizierte Entität im Rahmen der Zugangs-/Zugriffskontrolle (Access Control).

**Verbindlichkeit (Accountability)**

Aktionen einer Entität können eindeutig auf diese Entität zurückgeführt werden.

Verbindlichkeit = Eine Entität kann eine Handlung (z. B. Teilnahme an einer Kommunikation, Zugriff auf eine Ressource, ...) nicht abstreiten.

Daher häufig auch als Nicht-Abstreitbarkeit (Non-Repudiation) bezeichnet.

## 3.5 Sicherheitsmaßnahmen (Controls, Countermeasures)

Wirken gegen Bedrohungen und folglich gegen Risiken

**Arten der Sicherheitmaßnahmen:**

* präventiv (= ein Angriff wird verhindert),
* erschwerend (= ein Angriff wird nicht verhindert aber erschwert),
* abschwächend (= ein Angriff wird nicht verhindert aber der Schaden gemildert),
* erkennend (= ein Angriff wird nicht verhindert aber erkannt) oder
* reaktiv (= ein Angriff wird erkannt und es wird darauf reagiert)

Bei der Wahl von Sicherheitsmaßnahmen muss immer eine Balance zwischen Kosten und Effektivität der Maßnahmen und dem potentiellen Risiko gefunden werden (→ angemessene Maßnahmen)

**Klassen der Sicherheitsmaßnahmen:**

1. **Physische Sicherheitsmaßnahmen** = greifbare, bauliche Sicherheitsmaßnahmen, z. B. Schlösser, Wachen, Brandlöschanlagen, ...

2. **Organisatorische Sicherheitsmaßnahmen** = Richtlinien (Policies, Guidelines), Gesetze und Regulierung, Verträge, Versicherungen, ...

3. **Technische Sicherheitsmaßnahmen** = Hard- und Software wie Firewalls, Zugangs-/Zugriffskontrolle, Verschlüsselung, Intrusion Detection Systeme, ..

Gute Sicherheitskonzepte kombinieren verschiedene, sich oft überlappende Sicherheitsmaßnahmen aus verschiedenen Klassen **(= Defense in Depth**)

# 4. Angriffe und Angreifer

## 4.1 Passive Angriffe

**Eavesdropping**

Ein Bild, das Entwurf, Zeichnung, Diagramm, Lineart enthält.

Automatisch generierte Beschreibung

Hacker hat access zu dem Datentransfer zwischen Alice und  Bob und kann die Nachrichten lesen

**Traffic Analysis**

Ein Bild, das Entwurf, Diagramm, Clipart, Zeichnung enthält.

Automatisch generierte Beschreibung

Hacker hat wie bei 1. access zu dem Datentranfer aber analysiert die Daten genauer die von bob an Alice geschickt werden um Muster zu erkennen die er später nutzen kann

## 4.2 aktive Angriffe

**Masquerade**

Ein Bild, das Entwurf, Zeichnung, Diagramm, Lineart enthält.

Automatisch generierte Beschreibung  
Der hacker sendet eine Nachricht an alice die aussieht als wäre sie von Bob weil er zB zuvor Traffic analysis betrieben hat und durch seine Analyse nun eine ähnliche bilden kann.

**Replaying**

Ein Bild, das Entwurf, Zeichnung, Lineart, Clipart enthält.

Automatisch generierte Beschreibung  
Der hacker fängt einzelne nachrichten von Bob an Alice ab um diese später dann erst an Alice zu schicken.

Replay-Angriffe sind Cyberangriffe, bei denen bereits aufgezeichnete Daten oder Transaktionen erneut abgespielt werden, um unautorisierten Zugriff, Datenmanipulation oder finanzielle Vorteile zu erlangen. Die Ziele sind unter anderem die Wiederverwendung von Authentifizierungsdaten, die Umgehung von Sicherheitskontrollen und die Testung von Schwachstellen. Schutzmaßnahmen wie Verschlüsselung und Zeitstempel sind wichtig, um sich vor Replay-Angriffen zu schützen.

**Modification**

Ein Bild, das Entwurf, Zeichnung, Lineart, Clipart enthält.

Automatisch generierte Beschreibung

Der hacker fängt alle Nachrichten von Bob an Alice ab und ist nun die Verbindungsstelle der beiden. Er kann somit den Datenaustausch frei Bearbeiten nach seinen Wünschen. Nachrichten nach Belieben abfangen, löschen und verändern.

**Denial of Service**

Ein Bild, das Entwurf, Diagramm, Zeichnung, Text enthält.

Automatisch generierte Beschreibung  
  
Bei **DoS** -Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht.

**DDos** Bei der so genannten "verteilte DoS-Attacken" kommt anstelle von einzelnen Systemen eine Vielzahl von unterschiedlichen Systemen in einem großflächig koordinierten Angriff zum Einsatz. Durch die hohe Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam.

## 4.3 Cyber Kill Chain (Phasen eines Angriffs)

1. **Reconnaissance**: Beschaffung von möglichst vielen Informationen  
2. **Weaponization**: Hinzufügen einens Angriffscode (**Exploit**) in eine übertragbare Datei, um heimlich einen Zugang oder eine Hintertür (**Backdoor**) in ein System oder ein Programm zu schaffen  
3. **Delivery**: Überbringung des **weaponized bundles** and das Ziel in der Form von email, web, usb, etc.  
4. **Exploitation**: Ausnutzen einer Schwachstelle um am Ziel code ausführen zu können  
5. **Installation**: Installation der schadsoftware am ziel.  
6. **Command & control**: Command channel einrichten um remote control über das Opfer zu erlangen.  
7. **Actions on Objective**: Man bekommt "hands on keyboard access" der Angreifer hat also sein ursprüngliches Ziel der vollen kontrolle erlangt.

## 4.4. MITRE ATT&CK

MITRE ATT&CK1 ist eine **betreute Wissensdatenbank** und **ein Modell für das Verhalten von Angreifern** (Adversary) in den versch. **Phasen** eines Angriffs.

* MITRE ATT&CK behandelt s. g. APT (Advanced Persistent Threat) Angreifer.
* MITRE ATT&CK folgt dem **Tactics**, **Techniques** and **Procedures** (TTPs) Ansatz:
  + Tactics: das "Warum", taktisches Ziel des Angreifers.
  + (Sub-)Techniques: das "Wie", Vorgehen des Angreifers um das taktische Ziel zu erreichen, Sub-Techniques detaillieren Techniques.
  + Procedures: konkrete Umsetzung von (Sub-)Techniques von Angreifern.
* Die MITRE ATT&CK Matrix bringt Tactics und (Sub-)Techniques in Zusammenhang und ist aktuell für die Bereiche Enterprise, Mobile und ICS (Industrial Control Systems) definiert
* MITRE ATT&CK nimmt **die Perspektive des Angreifers** ein und verwendet dessen Terminologie für Tactics und Techniques.
* Die **Datenbasis** für MITRE ATT&CK bilden Berichte über **reale Vorfälle** (z. B. CTI Reports, Präsentationen auf Konferenzen, Social Media, Blogs, ...).
* MITRE ATT&CK wird stark "**community driven**"(weiter-)entwickelt2.
* MITRE ATT&CK ist deutlich konkreter als allgemeine Modelle wie die Cyber Kill Chain oder Microsoft STRIDE.

<https://attack.mitre.org/resources/versions/>

**Anwendungsgebiete Beispiele:**

* **Red Teaming3**: Vorbereitung von Red-Teaming-Kampagnen (z. B. Emulation eines bestimmten Angreifers oder bestimmter Techniques).
* **Cyber Threat Intelligence** (CTI): Ausgangsbasis/Anreicherung für/von individuelle/n Threat-Intelligence-Daten (z. B. Tactics und Techniques bestimmter Angreifer).
* **SOC4 Maturity Assessment(Beurteilung)**: Untersuchung ob bzw. wie gut ein SOC (Security Operations Center) aufgestellt/vorbereitet ist, um z. B. bestimmten Angreifern oder Techniques zu entdecken, abzuwehren, ...
* **Defensive Gap Assessment**: Finden von Lücken in der Unternehmens-Verteidung (z. B. Tactics und Techniques bestimmter Angreifer)

# 5. Security Design Principles & more

Security prozess: PDCA = Plan -> Do -> Check -> Act

## 5.1 Security Design Principles basierend auf Saltzer und Schroeder’s ”The Protection of Information in Computer Systems”

1. **Economy of Mechanism**  
   Keep it simple! Sicherheitsmechanismen sollten so einfach wie möglich sein (weniger fehleranfällig, Fehler werden leichter gefunden).
2. **Fail-Safe Defaults**

Zugang/Zugriff sollte explizit erlaubt werden müssen (Default: deny = Whitelisting [vs.

Blacklisting]); besser zu argumentieren, was muss zugänglich sein vs. was darf nicht zugänglich sein.

1. **Complete Mediation/Zero Trust Ansatz**

Jeder Zugang/Zugriff muss durch die Zugangs-/Zugriffskontrolle geprüft werden (z. B.

Rechteprüfung beim Öffnen einer Datei, aber auch beim Lesen/Schreiben von/in diese;

systemweite Sicht, nicht nur Betrieb, auch z. B. Außerbetriebnahme).

1. **Open Design**

Das Design eines Sicherheitsmechanismus sollte offen verfügbar sein (z. B. bei

kryptographischen Verfahren [Kerckhoffs’sche Prinzip]); erlaubt Review des

Mechanismus durch Dritte, weit verbreiteter Mechanismus wäre nicht geheim zu halten.

1. **Separation of Privilege**

Wo sinnvoll möglich, sollte Zugang/Zugriff nicht auf Basis einer einzigen Bedingung

gewährt werden (Multifaktor Authentifizierung).

1. **Least Privilege**

Jeder Entität sollten genau die Rechte eingeräumt werden, die diese für die Erledigung

seiner Aufgabe braucht (Need-to-Know-Prinzip).

1. **Least Common Mechanism**

Minimierung der Funktionalitäten, die gleichzeitig für mehrere Benutzer zur Verfügung

stehen.

1. **Psychological Acceptability**

Sicherheitsmechanismen müssen für Benutzer verwendbar sein (Usable Security) und

mit den Vorstellungen des Benutzer in Bezug auf die Sicherheitsziele übereinstimmen.

1. **Layering**

Verwendung mehrerer, überlappender, sich ergänzender Sicherheitsmechnismen, sodass

der Ausfall eines Sicherheitsmechnismus das System nicht schutzlos zurücklässt

(Defense in Depth)

1. **Isolation**

Isolierung von (a) öffentlich zugänglichen von sicherheitskritischen Systemen, (b)

Daten und Prozessen verschiedener Benutzer und (c) Sicherheitsmechnismen selbst.

1. **Modularity**

Sicherheitsmechanismen sollen als unabhängige, geschützte Module entwickelt werden,

die einfach wiederverwendet werden können (z. B. Kryptographie).

1. **Security/Privacy by Design/Default**

Sicherheit und Datenschutz sollen bereits bei der Entwicklung von Systemen

berücksichtigt werden. Default-Einstellungen sollen sicherheits- und

datenschutz-freundlich sein.

## 5.2 Standards und Normen

Standards sind allgemeine Spezifikationen und Richtlinien („Leitlinien“), die z.B. vom Unternehmen definiert werden können (nicht rechtlich gebunden), während Normen spezifische, **verbindliche** Anforderungen nach Stand der Technik sind, wie Sachen bestmöglich umgesetzt werden. (rechtlich gebunden)

Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung