# D. Grundbegriffe und ihre Systematik

1. Schutzziele
2. Schwachstelle und Verwundbarkeit
3. Insbesondere: Exploit
4. Gefährdungsfaktoren
5. Bedrohung vs. Risiko
6. Angriff


**die Systematik dieser Begriffe wirkt in verschiedenen Quellen mitunter etwas chaotisch und unterscheidet sich von Autor zu Autor ein wenig…**

# D.1. Schutzziele

- Authentizität (glaubwürdige Daten, vom richtigen Subjekt) - und auch Möglichkeit der Nachverfolgung eventueller Änderungen — *authenticity*
- Datenintegrität (nicht unbefugt manipuliert - auch durch technische Fehler nicht!) — *integrity*
- Vertraulichkeit (kein unbefugter Zugriff) — *confidentiality*
- Datenschutz (informationelle Selbstbestimmung) — *privacy*
- Verfügbarkeit (es funktioniert ohne ungeplante Unterbrechung; Zugriff auf notwendige Daten stets möglich) — *availability*

**während die ersten drei Punkte eng mit dem Datenschutz verknüpft sind, ist das letzte Thema auf den ersten Blick nur technisch und wenig spannend - dennoch nach wie vor extrem bedeutsam**

# D.2. Schwachstelle vs. Verwundbarkeit

„Wird eine […] Schwachstelle ausgenutzt, so kann es zu Beeinträchtigungen der Datenintegrität, Informationsvertraulichkeit oder auch Verfügbarkeit [d. h. insgesamt der zuvor genannten Schutzziele] kommen“

*Eckert, IT-Sicherheit*

- Schwachstelle = Schwäche eines Systems oder ein Punkt, an dem das System verwundbar werden kann; => allgemein! — *weakness*
- Verwundbarkeit = Schwachstelle, über die ein unautorisierter Zugriff auf das System möglich ist; => speziell im Hinblick auf Angriffe! — *vulnerability*
- Exploit = Möglichkeit der Ausnutzung einer Schwachstelle für einen Angriff — *exploit*

**Schwachstellen können über Gefährdungsfaktoren identifiziert werden**

# D.3. Exploit

Exploit, d. h. die Möglichkeit der Ausnutzung einer **Schwachstelle** für einen Angriff, ist - im Hinblick auf die Möglichkeit vorsätzlicher Angriffe - ein bedeutsames Phänomen der IT!

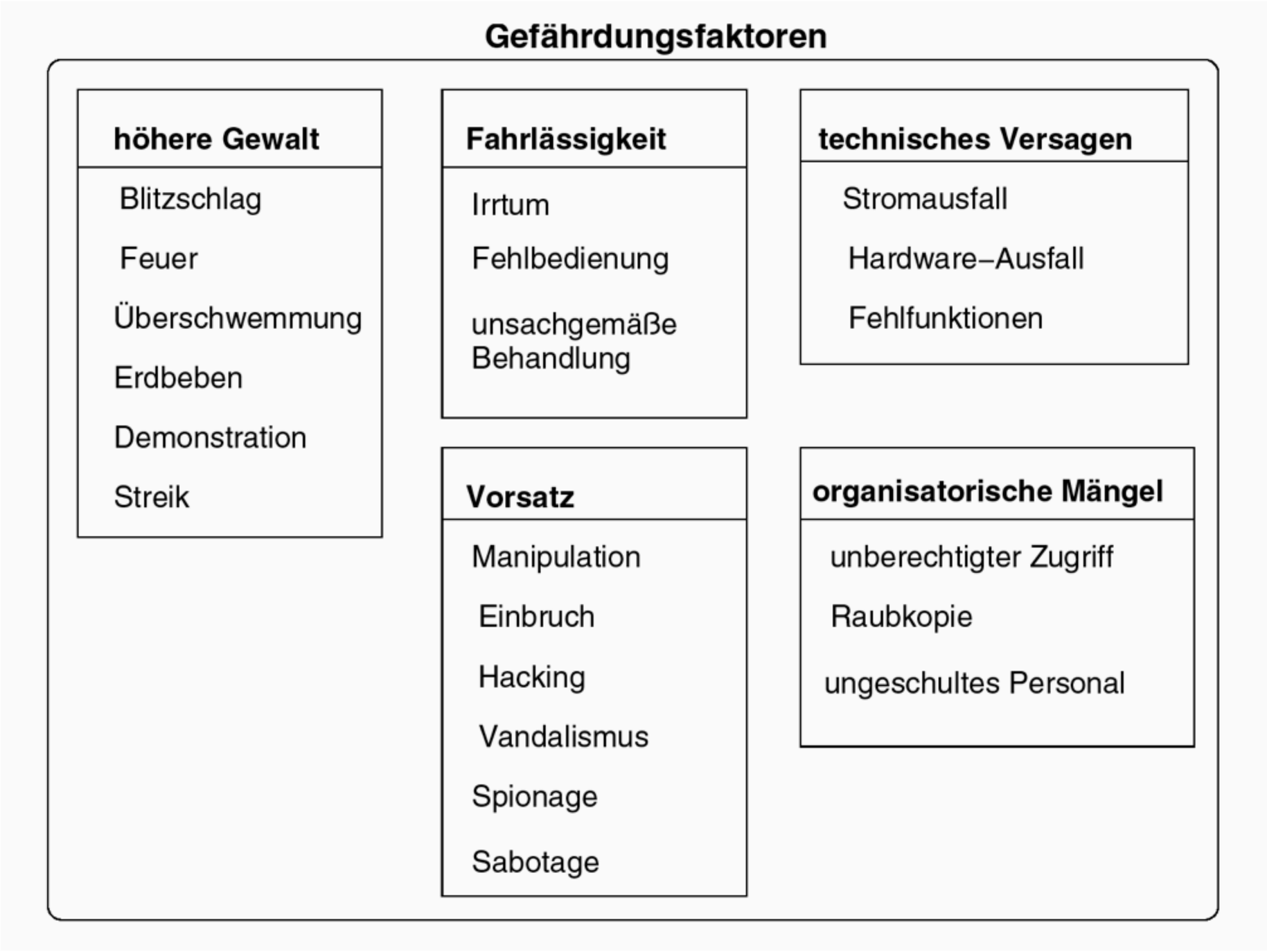
- besondere Kategorie: ***zero day exploit***
- Bedeutung für:
  - Hersteller = Qualitätsmanagement (Wettbewerbe)
  - aber auch: Kriminelle und (?) Geheimdienste
- Typen:
  - lokal vs. remote
  - Art der Schwachstelle:
    - *buffer overflow*
    - Eingabevalidierung
    - *race conditions*
    - *privilege escalation*

# D.4. Gefährdungsfaktoren

Die Suche nach Schwachstellen ist anhand der Liste von **Gefährdungsfaktoren** möglich:

- höhere Gewalt
- Fahrlässigkeit, menschliche Fehler
- Angriffe vorsätzlicher Art
- technisches Versagen
- organisatorische Mängel

# D.4. Gefährdungsfaktoren




Eckert, IT-Sicherheit, Abb. 1.2

# D.5. Bedrohung vs. Risiko

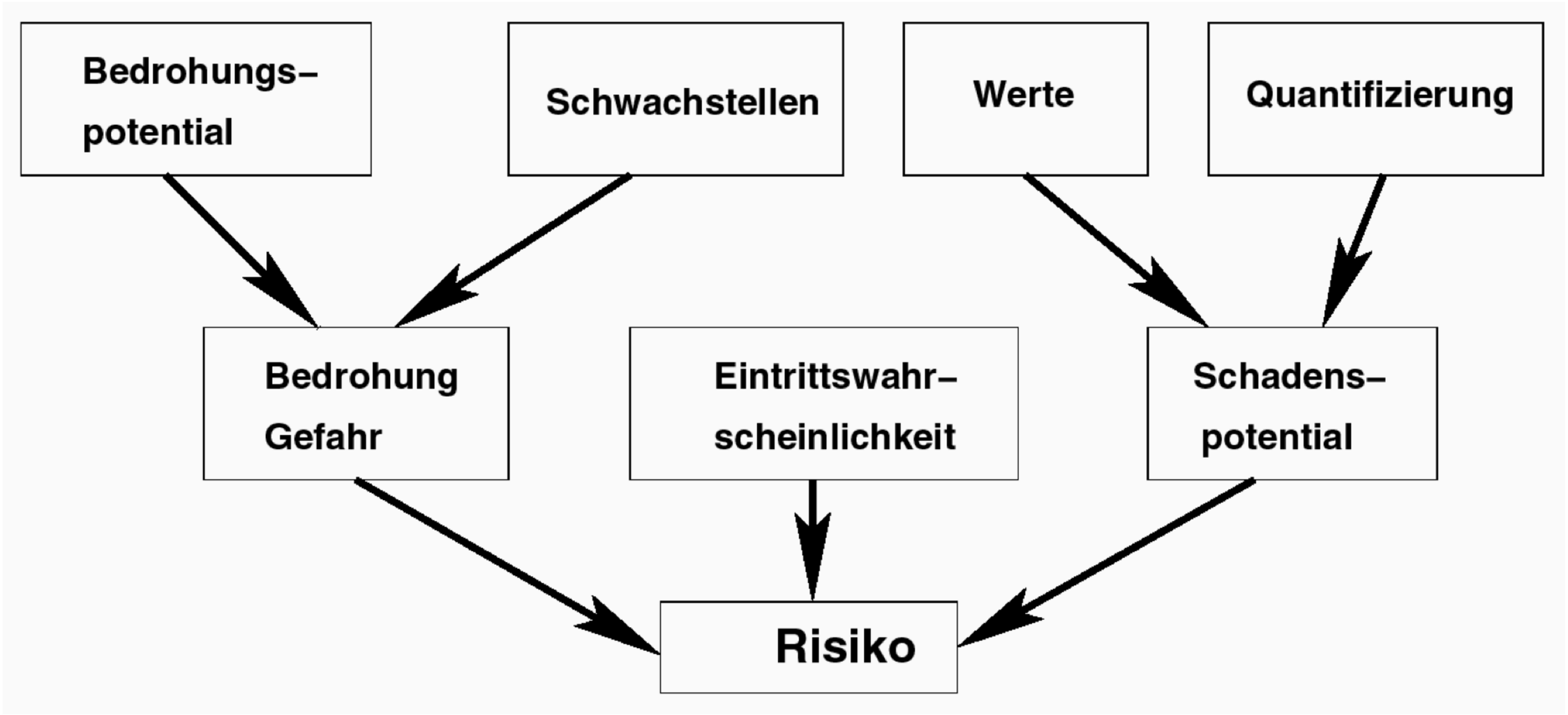
Verschiedene Schwachstellen können insbesondere Angriffe ermöglichen. Welche Bedeutung die jeweiligen Schwachstellen im konkreten Kontext haben, ist mittels Bedrohung und Risiko zu ermitteln.

- Bedrohung = Schwachstelle / Verwundbarkeit wird ausgenutzt, um die Schutzziele zu verletzen — *threat*
- Risiko = Wahrscheinlichkeit (relative Häufigkeit) des Eintritts eines Schadensereignisses und Höhe des potentiellen Schadens — *risk*
- Gewichtung zwischen dem Wert der Güter, dem Schadenspotential und der Wahrscheinlichkeit des Schadenseintritts erforderlich! — *assets*

**darauf basiert ein wichtiges Instrument der Daten- und IT-Sicherheit**
**=> die Bedrohungs- und Risikoanalyse**

# D.5. Bedrohung vs. Risiko => Systematik

## Zusammenhang zwischen den Begriffen




Eckert, IT-Sicherheit, Abb. 1.3

# D.6. Angriff

Verschiedene Schwachstellen können insbesondere Angriffe ermöglichen. Da Schwachstellen selten allein in unserer Hand liegen (Softwareanbieter, Dienstleister etc. ist für Anwender immer weniger transparent, der Anwender versteht immer weniger von der IT-Infrastruktur), ist mit Angriffen **immer** zu rechnen:

- Angriff = nicht autorisierter Zugriff / Zugriffsversuch auf das System *attack*
  - passiv = unauthorisierte Informationsgewinnung (Verlust der Vertraulichkeit)

    Beispiele: *eavesdropping, sniffing*

  - aktiv = unauthorisierte Modifikation von Daten / Systemen (Verlust der Datenintegrität / Verfügbarkeit)

    Beispiele: *DoS, spoofing*

# D.6. Angriff - Beispiele

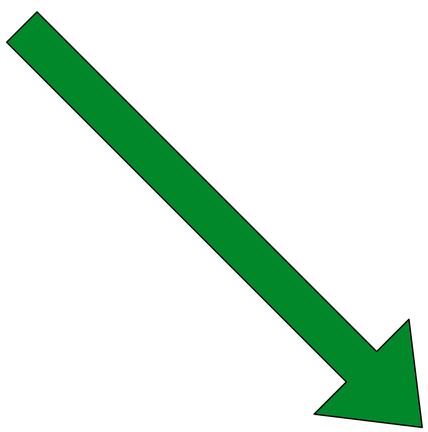
- *eavesdropping* = Abhören von Datenleitungen / unauthorisiertes Lesen aus Dateien
- *sniffing* = Ausspähen von Passwörtern
- *spoofing* = Datenänderung (insb. zur Identitätsverschleierung)
  - durch falsche Angabe der E-Mail-Absenderadresse, des DNS-Namens
- *phishing* = Abfangen von Passwörtern (z. B. nach *spoofing*)
- *denial of service* = Störung der Verfügbarkeit von Diensten
- Einschleusen von Schadsoftware (Virus / Wurm / Trojaner) zu verschiedenen Zwecken

Vgl. auch Arten von Schadsoftware nach ihrem Zweck!

# D.6. Angriff - Ursachen

Großteil nach wie vor intern - Bedeutung externer Angriffe steigt aber deutlich an!

| Angriffe von Innen | Angriffe von Außen |
|---|---|
| ▸ Mitarbeiter aus Frust<br>▸ Korruption<br>▸ Whistleblowing | ▸ Hacker<br>▸ Spionage<br>▸ Skript Kiddies |



# D.6. Angriff - Typen von Schadsoftware

Folgende Arten von Schadsoftware sind weit verbreitet - eine zu 100 % eindeutige systematische Einordnung wird hier nicht angestrebt - zunächst einmal erfolgt eine grobe Einteilung nach Funktionsweise der Schadsoftware:

- Virus
- Wurm
- Trojaner

Sollte Schadsoftware nach ihrem konkreten (schädigenden) Zweck identifiziert werden, dann empfiehlt sich folgende Einteilung:

- Rootkit
- Backdoor
- Ransomware
- Spyware
- Scareware
- Adware

# D.6. Angriff - Typen externer Angriffe

- Hacker = technisch versiert, sucht nach Exploits, nicht zwingend kriminell aber mitunter illegal — *exploit*
- Skript Kiddies = nutzen bekannte Lücken für Angriffe, nicht zwingend kriminell, verursachen aber Schäden — *script kiddie*
- Spionage = Geheimdienste oder Wirtschaftsspione überwachen massiv Datenverkehr — ***z. B. NSA***
- Kriminelle = Angriffe zum Zwecke der Bereicherung, z. B. durch *Ransomware* — *ransomware*
  - mit Bot-Netzen
  - mit Spyware
  - mit einer *brute-force*-Attacke
  - usw.