IT-SICHERHEIT UND DATENSCHUTZ

KAPITEL 1 - IT-SICHERHEIT

buchmann@hft-leipzig.de

LERNZIEL DIESES KAPITELS

- Verständnis der allgemeinen Ziele der IT-Sicherheit
  - Entwickle IT-Systeme mit so wenig Schwachstellen wie möglich
  - Identifiziere/behebe Schwachstellen in existierenden Systemen
  - Berücksichtige dabei verschiedene Perspektiven
    - Ist es besser, den Geschäftsprozess zu ändern, anstelle das unsichere Programm zu überarbeiten?
    - Führt eine Sicherheitsmaßnahme tatsächlich zu einem Gewinn an Sicherheit, oder ist sie so komplex das die Nutzer sie sabotieren?
    - ...
- Kein Ziel
  - Bestimmte Sicherheitswerkzeuge anwenden
  - Hacker-Programme entwickeln und nutzen

WAS IST DAS PROBLEM DABEI? (1/2)

- **Es reicht nicht, ein System vor allen bekannte Schwachstellen zu schützen!**
  - Zahllose Schwachstellen vs. begrenztes Personal in der Sicherheitsabteilung
  - Angreifer entwickeln ständig neue Formen von Angriffen
  - Es braucht Zeit, Maßnahmen gegen neue Angriffe zu entwickeln

- Problem: Wie kann man sich gegen einen neuen, unbekannten Angriff schützen?

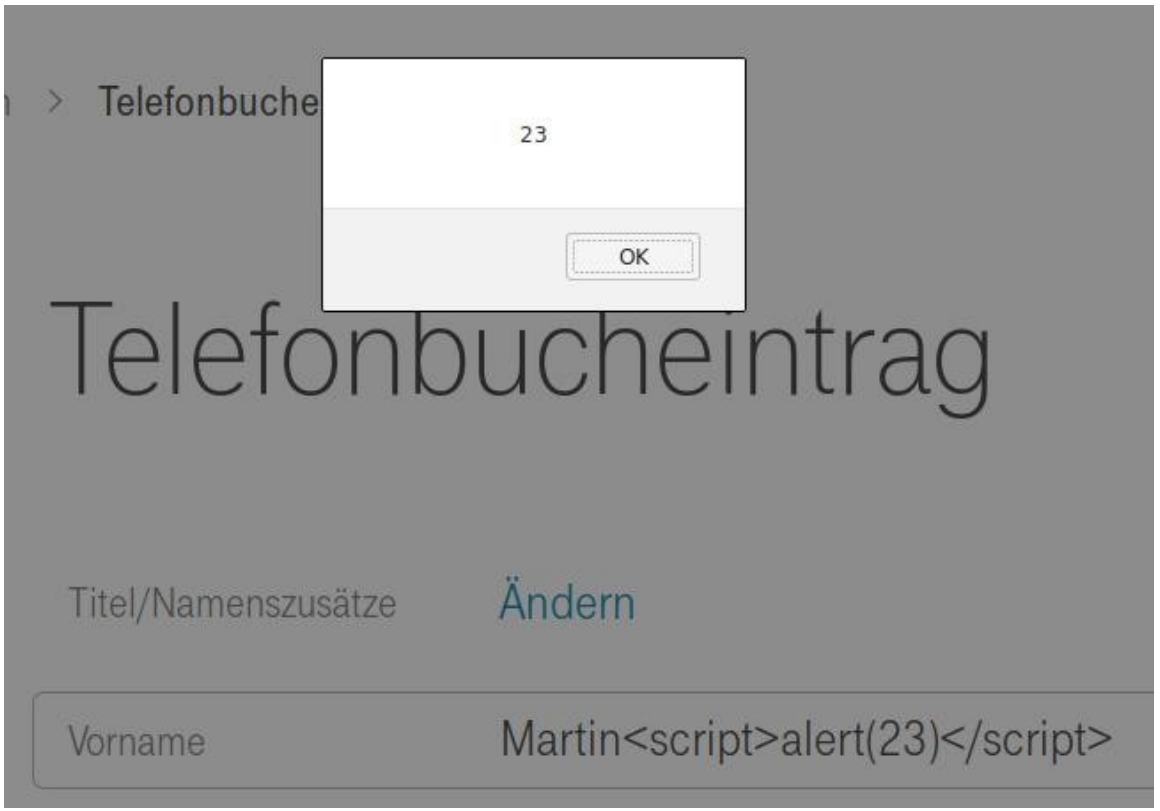
- Allgemeine Idee:
  - Minimiere die genutzten Bibliotheken/Schnittstellen/Codezeilen/...
  - Mache alles richtig (Software Engineering, System Design, Tests, Bug Fixes einspielen, etc.)
  - Berücksichtige Risiko eines Angriffs und Wert eines System, um kritische Ressourcen auch am besten zu schützen

WAS IST DAS PROBLEM DABEI? (2/2)

- **Es reicht nicht, ein System vor allen bekannte Schwachstellen zu schützen!**
  - Komplexe Systeme → hohe Wahrscheinlichkeit, etwas Wichtiges zu übersehen

- Problem: Wie lässt es sich erreichen, das ein Angriff keinen ernsthaften Schaden anrichtet?

- Allgemeine Idee:
  - IT-Sicherheit als Management-Aufgabe
  - Realisiere eine umfassende Sicherheitsstrategie von der Angriffserkennung bis zum Umgang mit erfolgreichen Angriffen über alle Prozesse, Systeme, Fachabteilungen hinweg



Screenshot from March 16th, 2019

ABSOLUTE VS. PRAKTISCHE SICHERHEIT

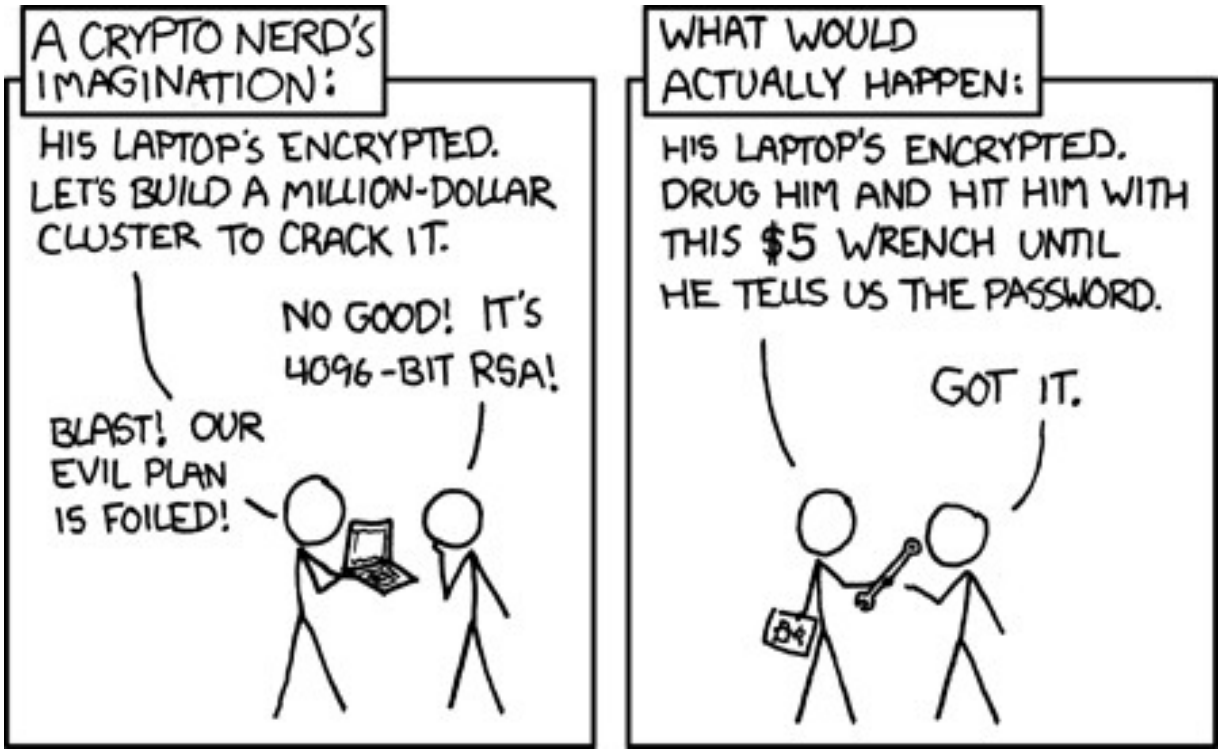
- Absolute Sicherheit
  - Das System kann nicht beeinträchtigt werden
  - Schwierig, teuer und/oder unpraktisch zu erreichen
    - siehe One-Time Pad, Kapitel „Verschlüsselung“

- Praktische Sicherheit
  - Wenn eine der folgenden Eigenschaften gilt, ist das System sicher (genug)
    - Aufwand zum Eindringen in ein System > Gewinn durch den Einbruch
    - Zeit zum Eindringen in ein System > Zeit, in der der Einbruch einen Wert hat
    - Menge/Wert der dafür nötigen Daten > Menge/Wert der gewonnenen Daten

WAS IST DEN NUN IT-SICHERHEIT EIGENTLICH?

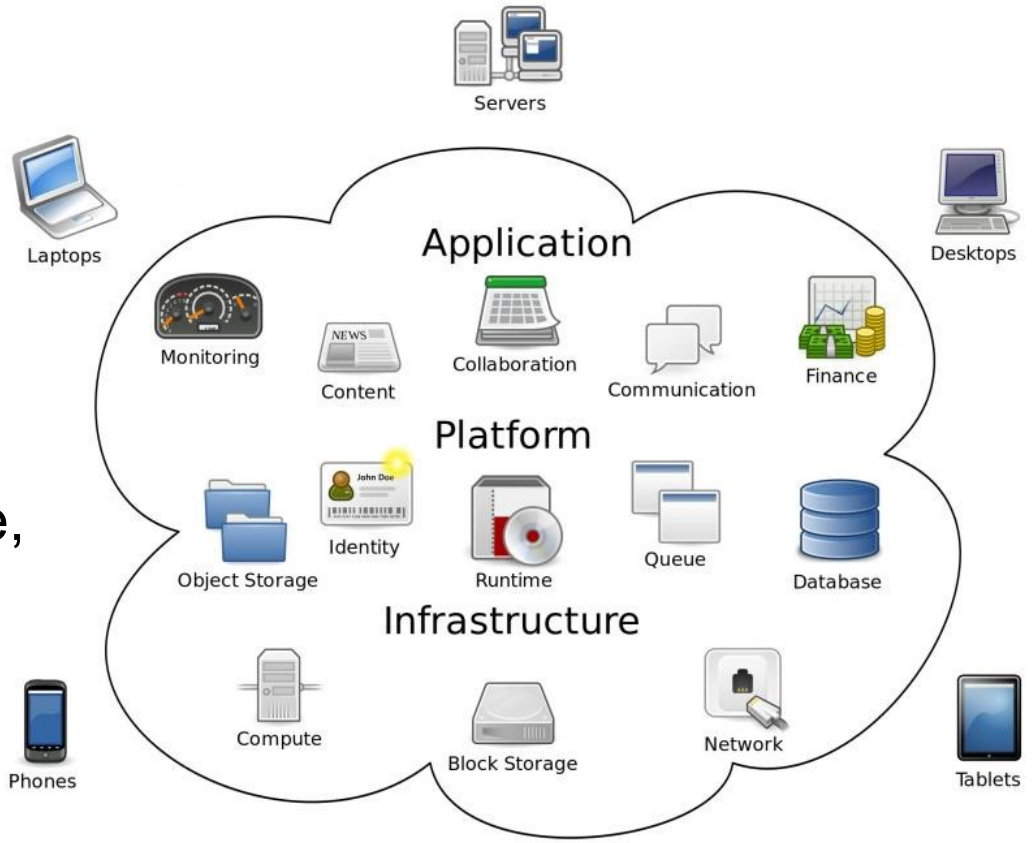
DEFINITION

- *IT-Sicherheit ist der Schutz der Assets eines IT-Systems*
  - *Hardware, Software, Daten, Mitarbeiter, Prozesse*
  - *Kombinationen davon*



IT-SYSTEME

- Hardware
  - Computer, Geräte, Netzwerktechnik, ...
- Software
  - Betriebsysteme, Anwendungen, Werkzeuge, Spezialsoftware, ...
- Daten
  - Inhalt, Kommunikation, Metadaten, ...
- Prozesse
  - Organisation, Abläufe, Geschäftseinheiten, Personen, ...



WERT

- Wertbasierte Entscheidungen sind etwas altbekanntes...
  - Sie lassen Handtuch und Schuhe einfach so am Strand liegen, aber nicht Handy und Brieftasche
  - Je teurer Ihr Fahrrad, desto mehr Geld geben Sie für das Fahrradschloss aus
  - Ein altes Familienfoto hat sehr viel Wert für Sie, aber keinen Wert für jemand anderen

- Dasselbe gilt für IT-Systeme
  - Je mehr Wert ein IT-System für Sie hat, desto besser sollte es geschützt sein

WERT IHRER ASSETS

- Marktübliche Hardware
  - Leicht zu ersetzen, aber Ersatz kostet Zeit
- Individuelle Anwendungen und Spezialhardware
  - Schwer zu ersetzen, Ersatz kostet viel Zeit
- Daten
  - Üblicherweise einzigartig, oft nicht ersetzbar
  - Daten aus dem Front-end sind oft wertvoller als Backups
- Prozesse
  - Können einzigartig sein, Ersatz kostet Zeit

- *Der Wert der Assets hängt von Besitzer und Zeit ab, ist oft unpräzise*

SCHWACHSTELLE VS. BEDROHUNG

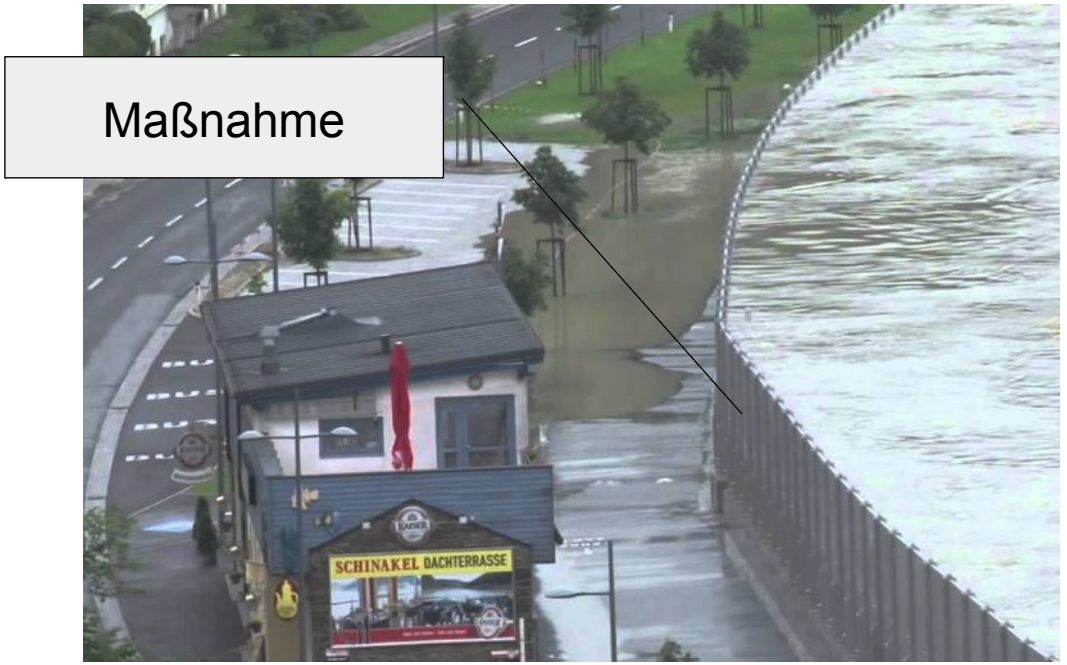
- **Schwachstelle**: Kann ausgenutzt werden, um einen Schaden zu verursachen
- **Bedrohung**: Umstände, die einen Schaden verursachen können

(GEGEN)MASSNAHMEN

Eine **Maßnahme** ist

- eine Aktion
- ein Gerät
- ein Prozess oder
- eine Technik

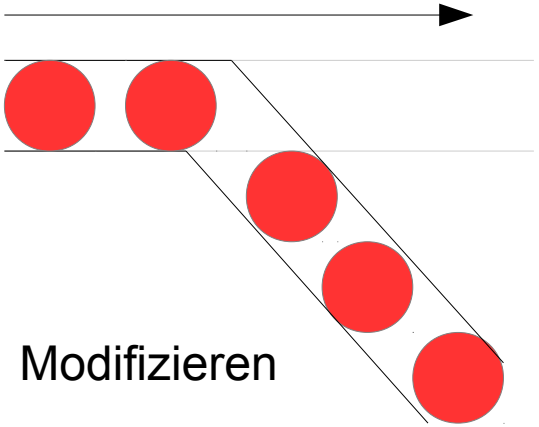
die eine **Schwachstelle**
entfernt oder
deren Auswirkungen
reduziert



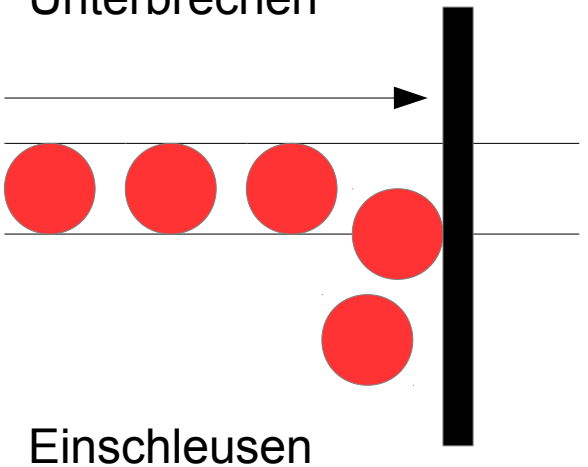
- **Maßnahmen** verhindern, das **Bedrohungen** die vorhandenen **Schwachstellen** ausnutzen, um einen **Schaden** zu verursachen

MÖGLICHKEITEN, UM SCHADEN ZU VERURSACHEN

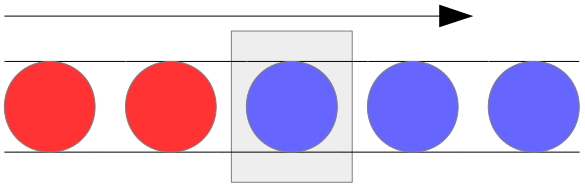
- Abfangen



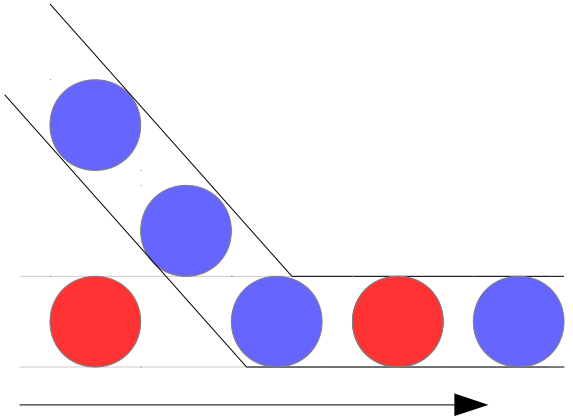
- Unterbrechen



- Modifizieren



- Einschleusen



ZIELE DER IT-SICHERHEIT

- „Security triad“
  - **Vertraulichkeit**: Asset ist nur Autorisierten zugänglich
  - **Integrität:** Asset kann nur von Autorisierten modifiziert werden
  - **Verfügbarkeit**: Asset kann von Autorisierten genutzt werden

- ISO 7498-2 fügt hinzu
  - **Authentisierung**: Identität eines Senders wird überwacht
  - **Nichtabstreitbarkeit**: Sender kann nicht abstreiten, das eine Nachricht von ihm kam
- US Department of Defense fügt hinzu
  - **Auditierbarkeit**: Alle Aktionen mit dem Asset sind nachvollziehbar

VERTRAULICHKEIT

- *Nur autorisierte Personen dürfen auf geschützte Daten zugreifen*
  - Im wesentlichen **Zugriffskontrolle**

- Das ist weniger trivial als es aussieht!
  Unautorisierte Person kann herausfinden:
  - die Daten selbst
  - den Wertebereich der Daten
  - Metadaten (Sprache, Länge, Erstellzeit, ...)
  - das auf Daten zugegriffen wurde
  - das Daten überhaupt existieren
  - das jemand anderes darauf zugreifen möchte
  - ...

ZUGRIFFSKONTROLLE

- Subjekt, Art des Zugriffs, Objekt und Regel

Subjekt
(Wer möchte zugreifen)

Art des Zugriffs
(Wie soll das passieren)

Objekt
(Was wird zugegriffen)

Regel:
f(Wer + Was + Wie) → {Ja|Nein}

INTEGRITÄT

- Kann je nach Kontext etwas anderes bedeuten!

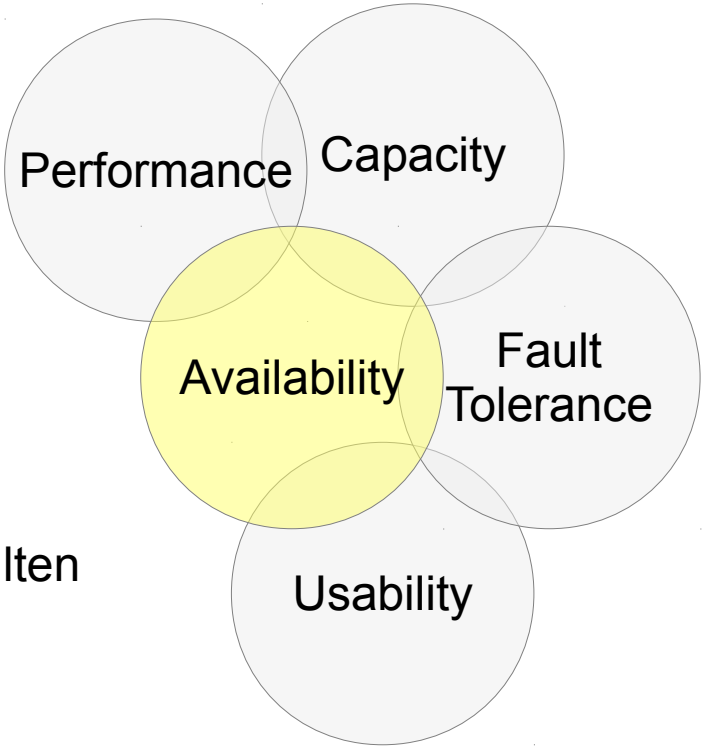
- Eine oder mehr dieser Eigenschaften
  - objektiv korrekt
  - nur auf erlaubte Weise verändert
  - nur von autorisierten Personen verändert
  - konsistent mit anderen Daten
  - in sich konsistent
  - für die Anwendung bedeutsam und nützlich
  - ...

BEISPIEL

- In Datenbanksystemen üblicherweise drei Anforderungen
  - Jedes Attribut bleibt innerhalb seines definierten Wertebereichs
  - Jedes Datentupel kann durch einen Primärschlüssel (oder row id) eindeutig identifiziert werden
  - Jedes Datentupel kann über eine Fremdschlüsselbeziehung referenziert werden

(die anderen auf der letzten Folie genannten Eigenschaften liegen außerhalb des Datenbanksytems)

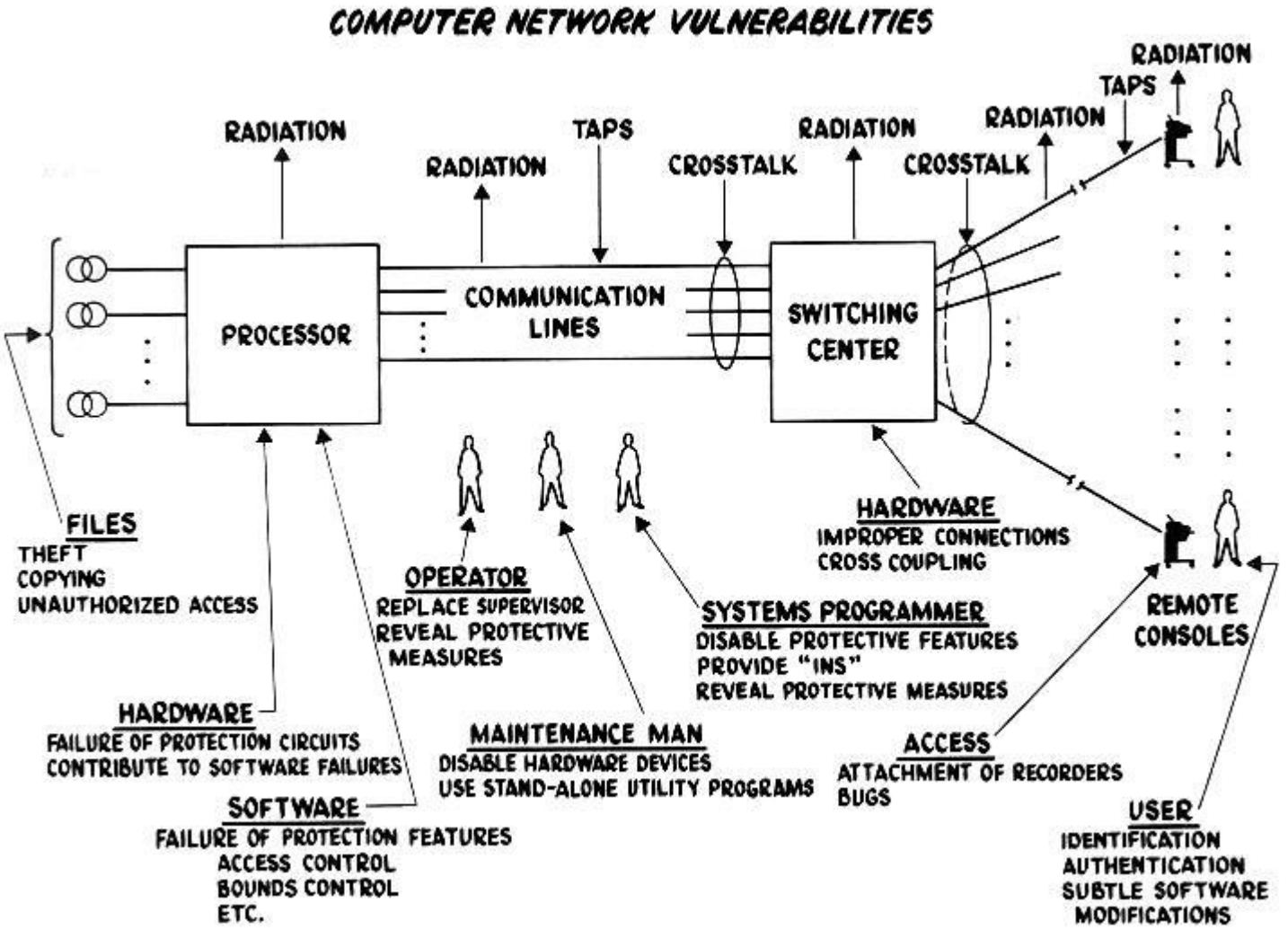
VERFÜGBARKEIT



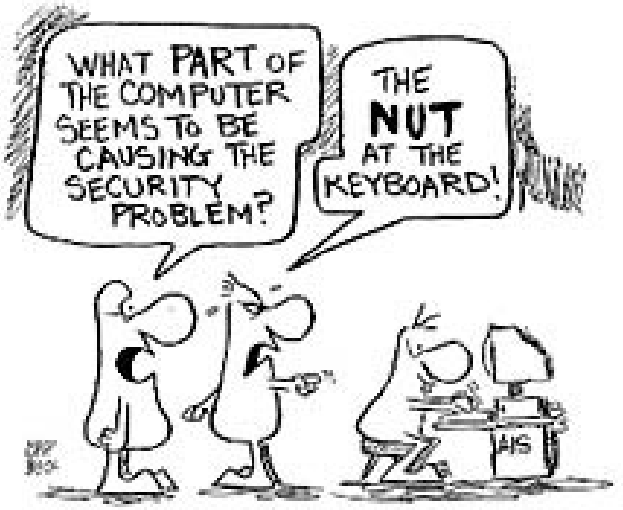
- *Hier gemeint: Daten und Prozesse*
- Ein Prozess ist verfügbar wenn
  - er sich in einer nützlichen Form darstellt
  - er die nötige Kapazität hat, um die an ihn gestellten Anforderungen zu erfüllen
  - er sichtbar und zuverlässig Rückmeldung zum Bearbeitungsfortschritt anzeigt
  - er in einer für die Aufgabe akzeptablen Zeit fertig wird

VERFÜGBARKEIT, INTEGRITÄT, VERTRAULICHKEIT

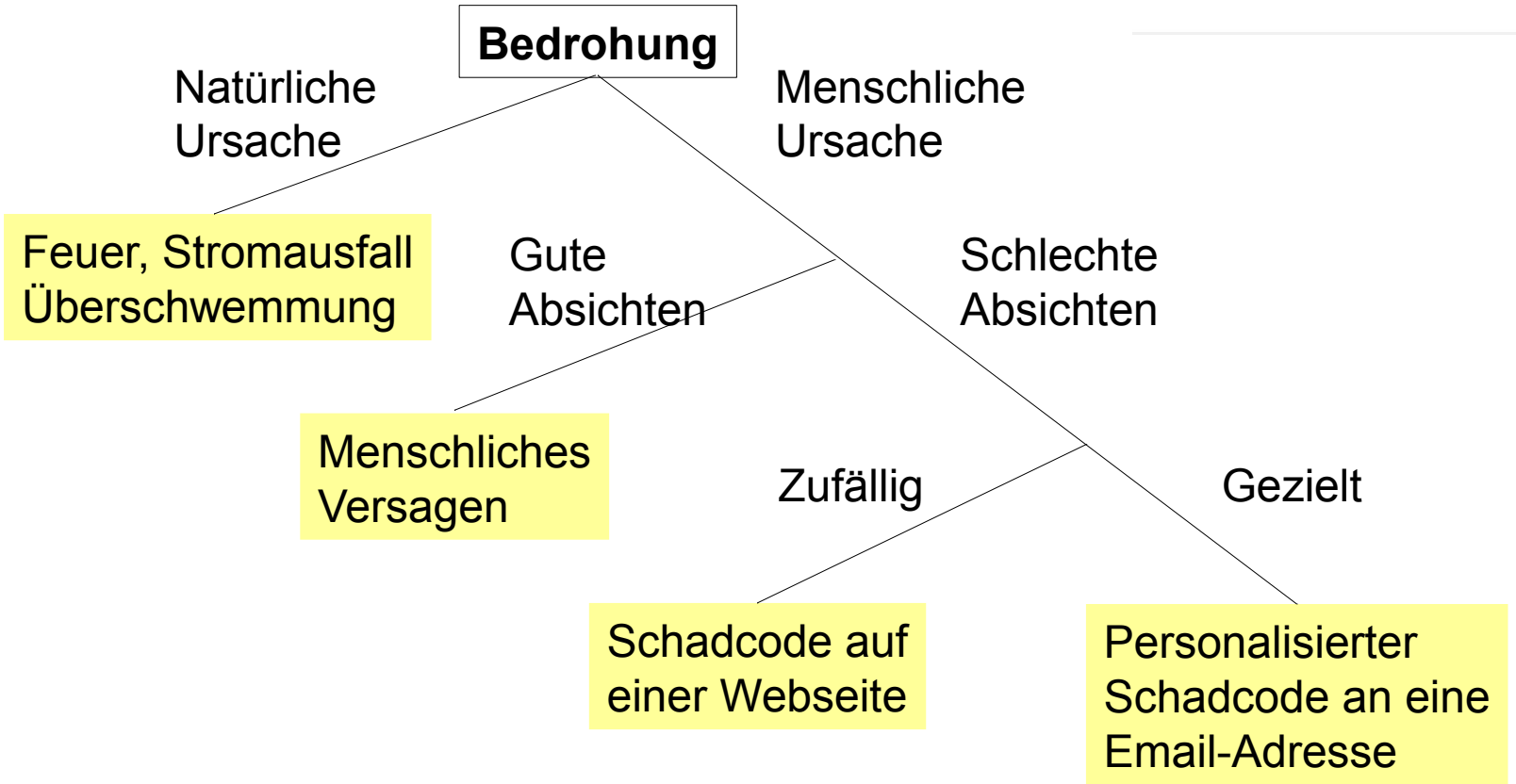
- Illustration aus den 70ern:



UMGANG MIT BEDROHUNGEN



- Die *Abwesenheit* von Bedrohungen lässt sich praktisch nicht beweisen, nur die *Anwesenheit* von Bedrohungen die bereits gefunden wurden



EINIGE BEDROHUNGEN SIND SCHWIERIGER ALS ANDERE

- Natürliche Ursachen, menschl. Versagen
  - Bedrohungen entwickeln sich nicht
  - können „nach Handbuch“ bearbeitet werden
    - Schutz gegen Erdbeben, Fluten, Stomausfälle, Feuer ist gut verstanden
    - Häufige Backups, redundante Anlagen auf „hot standby“ etc.

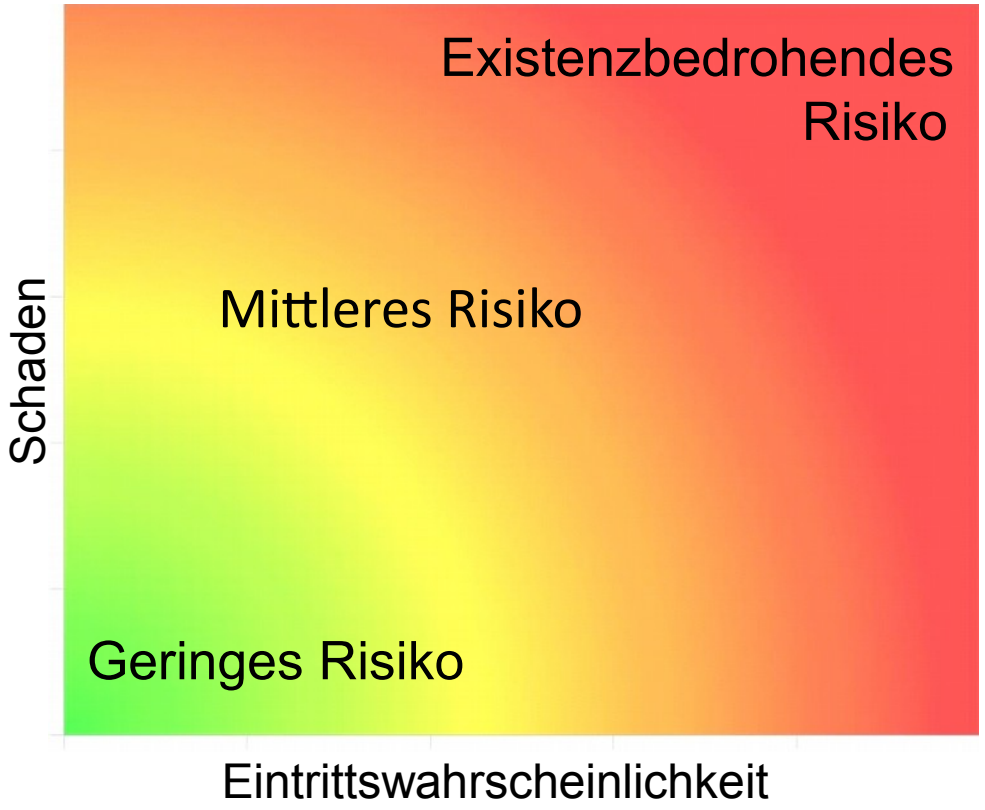
- Zufällige oder gezielte Angriffe
  - Hacker entwickeln sich weiter
    - Sicherheitsupdates schließen nur Lücken, *nachdem* sie bekannt wurden
      → es existiert ein Zeitfenster für Angriffe
  - Botnetze, organisiertes Verbrechen bis hin zu quasistaatlichen Gruppen können über sehr große Ressourcen verfügen
    - Wissen um Schwachstellen,
      Hardware zum brute-force Knacken von Schlüsseln

RISIKOMANAGEMENT

- **Schaden**: Negative Konsequenz aus einer Bedrohung
  - Kann quantifiziert werden als
    - Monetärer Wert: Kosten für Ersatz, Kosten für Service-Ausfall, ...
    - Nichtmonetärer Wert:
      Allgemeine Skala (sehr hoch, … mittel, … sehr niedrig)
      - Beispiel: Der Wert Ihrer Kreditkarte ist für Sie geringer als der Wert einer Bachelor-Arbeit, die morgen abgegeben werden muss

- **Risikomanagement**: Entscheiden, welche Bedrohungen am meisten Aufmerksamkeit und Ressourcen benötigen
  - Ganz einfach: Mehr Aufwand für den Schutz wertvollerer Assets
  - Doch nicht so einfach: Anzahl und Art der Bedrohungen sind praktisch unbegrenzt, Wert der Assets verändert sich mit der Zeit
  - **Restrisiko**: Risiko, das Sie ohne Maßnahmen akzeptieren

RISIKEN UND WAHRSCHEINLICHKEITEN



RISIKO VON EXTREMEREIGNISSEN

- Extreme Bedrohung
  - Verursacht unbegrenzt Schaden, aber Sie haben nur begrenzt Ressourcen (Roboter tötet Monteure, Erdbeben zerstört die komplette IT incl. Backups, ...)
- Extrem selten
  - Wahrscheinlichkeit und Kosten können nicht so leicht geschätzt werden (Wahrscheinlichkeit, das ein Tsunami eine 10m hohe Flutmauer überspült)

→ Verzerrte Risikowahrnehmung und -bewertung

ABSCHÄTZEN DER EINTRITTSWAHRSCHEINLICHKEIT

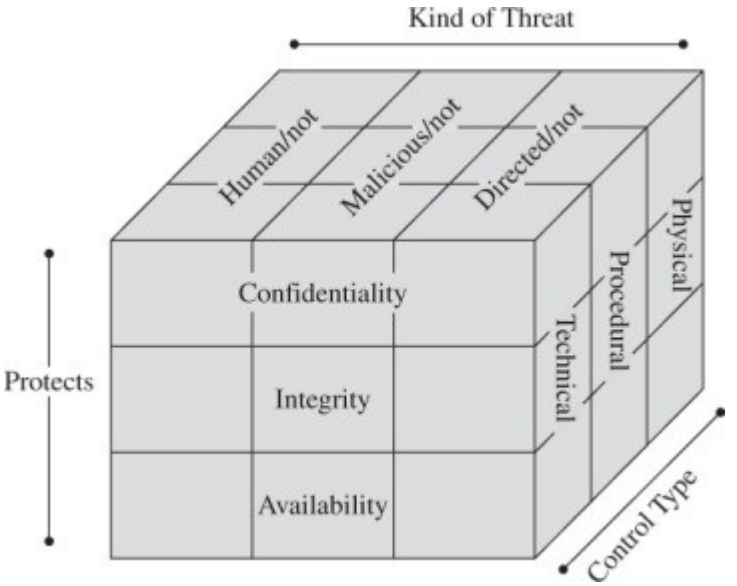
- **Methodode**
  - Fähigkeiten, Wissen, Ressourcen für einen erfolgreichen Angriff
- **Möglichkeit**
  - Genügend Zeit und Zugangsmöglichkeiten für einen erfolgreichen Angriff
- **Motiv**
  - Ein Grund für den Angriff
- *Methode, Möglichkeit und Motiv müssen gemeinsam gegeben sein, damit ein Angriff erfolgreich ist!*
  - Motiv kann auch sein „Weil es Spaß macht“!

UMGANG MIT ANGRIFFEN

Sie können

- **verhindern:** blockieren des Angriffs
- **erschweren:** die Erfolgswahrscheinlichkeit reduzieren
- **umlenken:** die Motivation für einen Angriff auf ein Asset reduzieren
- **abmildern:** die Auswirkungen eines erfolgreichen Angriffs reduzieren
- **erkennen:** herausfinden ob ein Angriff stattfindet
- **erholen:** den Schaden eines erfolgreichen Angriffs beheben

ARTEN VON MASSNAHMEN



- Physisch
  - Stoppen von Angriffen an physischen Grenzen, z.B. durch einen Pförtner oder einen abgeschlossenen Serverraum
- Prozessual oder administrativ
  - Erschweren oder umenken von Angriffen durch Regulierung, Gesetze, Richtlinien etc., beispielsweise durch eine Vorschrift, das Passwörter nicht aufgeschrieben werden oder Daten nur auf Firmenhardware gespeichert werden
- Technisch
  - Passwörter, kryptografische Protokolle, Firewalls
    (den meisten Laien fällt diese Kategorie von Maßnahmen als erstes ein)

ABSCHLUSS

ZUSAMMENFASSUNG

- Sicherheitsprobleme entstehen täglich
  - Einige Probleme sind schwieriger als andere
- Eine Bedrohung für das Ausnutzen einer Schwachstelle führt zu einem Schaden an einem Asset
  - Viele Möglichkeiten, dies zu vermeiden
- Perfekte Sicherheit ist nicht zu erreichen
  - Begrenzte Ressourcen, Abwesenheit von Schwachstellen nicht beweisbar
- Angreifer benötigt eine Methode, eine Möglichkeit und ein Motiv
  - Erlaubt eine systematische Abschätzung der Wahrscheinlichkeit für einen erfolgreichen Angriff → Risikomanagement

MÖGLICHE PRÜFUNGSFRAGEN

- Erläutern Sie die Begriffe Schwachstelle, Bedrohung, Risiko und Maßnahme.
- Geben Sie drei Arten von Schäden an, die ein Unternehmen durch Bruch der Vertraulichkeit für Unternehmensdaten erleiden kann.
- Gegen welche Arten von Bedrohungen helfen Backups, und gegen welche nicht?
- Auf welche Weise beeinflusst die Zeit den Wert eines Assets? Geben Sie drei eigene Beispiele an.
- Eine Firma stellt Programme für Tele-Medizin her. Wer könnte über Motive und Methoden verfügen, um dieses Programm anzugreifen?

LITERATUR

- Pfleeger, Charles P. et al.: Security in Computing, *Prentice Hall,* 2015

- Eckert, Claudia. IT-Sicherheit: Konzepte-Verfahren-Protokolle. *Walter de Gruyter*, 2018

  (Die Auflage ist für Grundlagenkapitel egal, falls Sie eine alte Version besitzen oder als PDF im Netz finden)