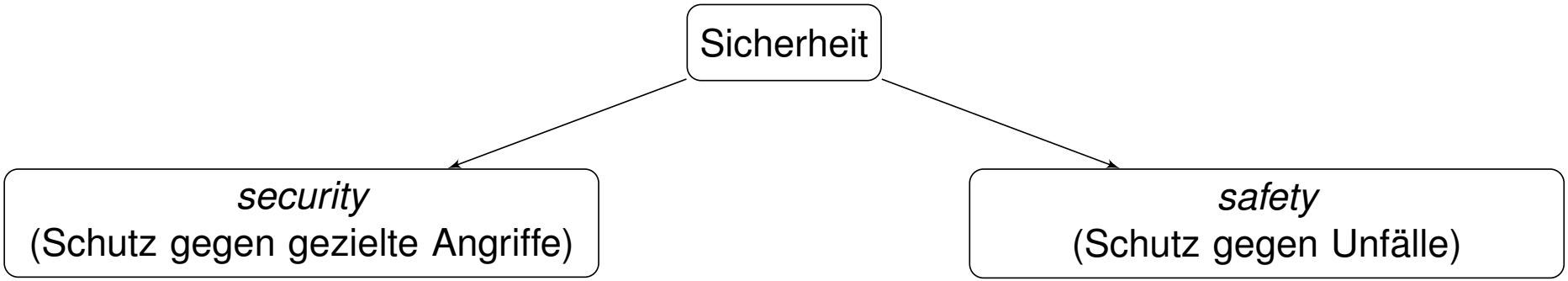
Kapitel 6: Grundlagen der IT-Sicherheit

6: Grundlagen der IT-Sicherheit



Frage: Kennen Sie Beispiele aus der realen Welt?

Diese Vorlesung beschäftigt sich ausschließlich mit **security**.

In eigener Sache

Es heißt **IT-Security** bzw. Informationssicherheit. Der Begriff **Cybersecurity** ist Neusprech und wird gerne in Politik, Journalismus und Militär verwendet.

`http://www.therestlessmachine.de/?p=901`

Sicherheit ist bedeutungsarm

Wogegen schützt z.B. eine Firewall die auf einem Computer läuft?

- Gegen Angreifer, die Daten ausspionieren wollen?
- Gegen Angreifer, die Daten verändern wollen?
- Gegen Angreifer, die das System vorübergehend stören wollen?
- Gegen Angreifer, die das System dauerhaft stören wollen, z.B., in dem sie den Computer mit einer Bombe in die Luft sprengen?
- Gegen Angreifer, die wissen wollen, ob und wann bestimmte Personen das System nutzen?

Sicherheit braucht Kontext

- Ist das System mit dem Internet verbunden? Oder mit anderen unsicheren Netzwerken?
- Sind die Angreifer
  - Externe,
  - normale Benutzer,
  - Benutzer mit speziellen Privilegien,
  - unerfahrene Gelegenheitstäter,
  - fähige "Hacker" ohne größeres Budget,
  - kriminelle Organisationen oder Geheimdienste?

Merke

Die Begriffe sicher und Sicherheit sind ohne Kontext bedeutungslos.

Frage: Kennen Sie weitere bedeutungsarme Wörter.

Grundregel des Security Engineering

1. Spezifiziere die angestrebten Schutzziele:
   Was soll **gegen wen** geschützt werden?

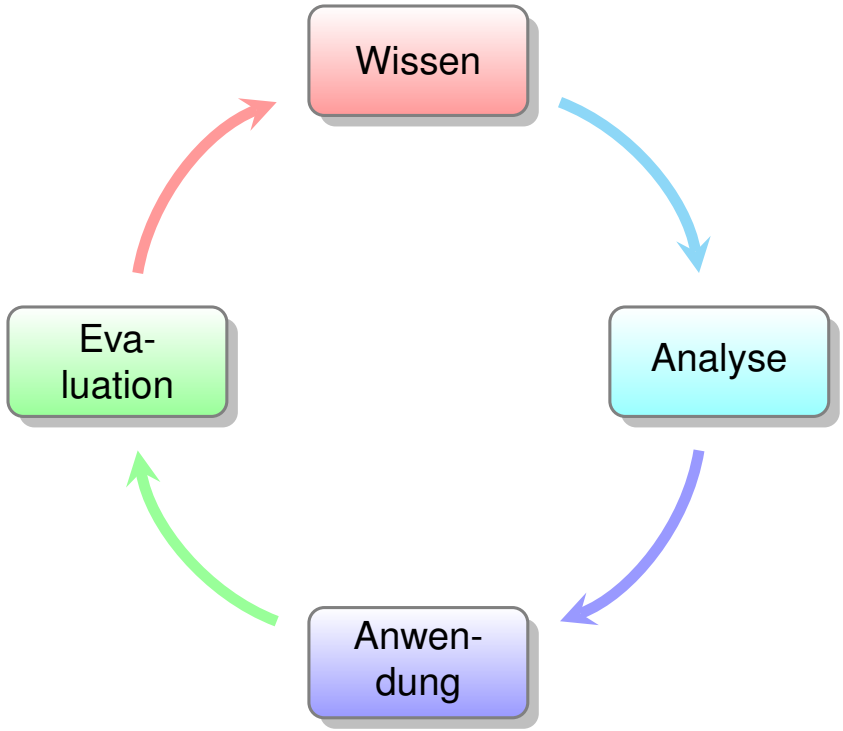
2. Ermittle die Bedrohungen für ein System:
   Wie könnten Angreifer ein Schutzziel unterlaufen?

3. Beachte das Gesamtsystem, nicht nur das IT-System:
   Personen, gesellschaftl. und wirtschaftl. Faktoren, ...

Achtung

- Diese Regeln mögen selbstverständlich erscheinen.
- Sie werden in der Praxis aber häufiger miss- als beachtet!

IT-Sicherheit ist ein Prozess



IT-Sicherheit ist ein Prozess . . .

. . . der ständig an den Stand der Technik angepasst und verbessert werden muss, um sich vor neuen Angriffen zu schützen.

Anmerkungen zum IT-Sicherheitsprozess

- Lernen Sie so viel wie möglich über die mögliche Bedrohungen.
- Entwerfen Sie einen sinnvollen Maßnahmenkatalog.
- Kaufen Sie sie nicht einfach Software und Appliances.
- Maßschneidern Sie sich Ihre Lösungen nach **Ihrer** Analyse.
- Evaluieren Sie regelmäßig Ihren Maßnahmenkatalog.
- Verbessern Sie regelmäßig Ihre Maßnahmen.
- Achten Sie auf Usability für legitime Nutzer.
- Bereiten Sie Prozesse für den Ernstfall vor.
- Testen, testen, testen.

6.1: Schutzziele

Hauptproblem der IT-Sicherheit

IT-Sicherheit kann nicht gemessen werden.

Lösungsansatz

Indirekte Definition von IT-Sicherheit durch Schutzziele.

- Vertraulichkeit (engl. confidentiality, data privacy)
  Schutz gegen unbefugte Informationsgewinnung
- Integrität (engl. (data) integrity)
  Schutz gegen unbefugte Veränderung der Daten
- Verfügbarkeit (engl. availability)
  Schutz gegen unbefugte Beeinträchtigung der Funktionalität

Vertraulichkeit

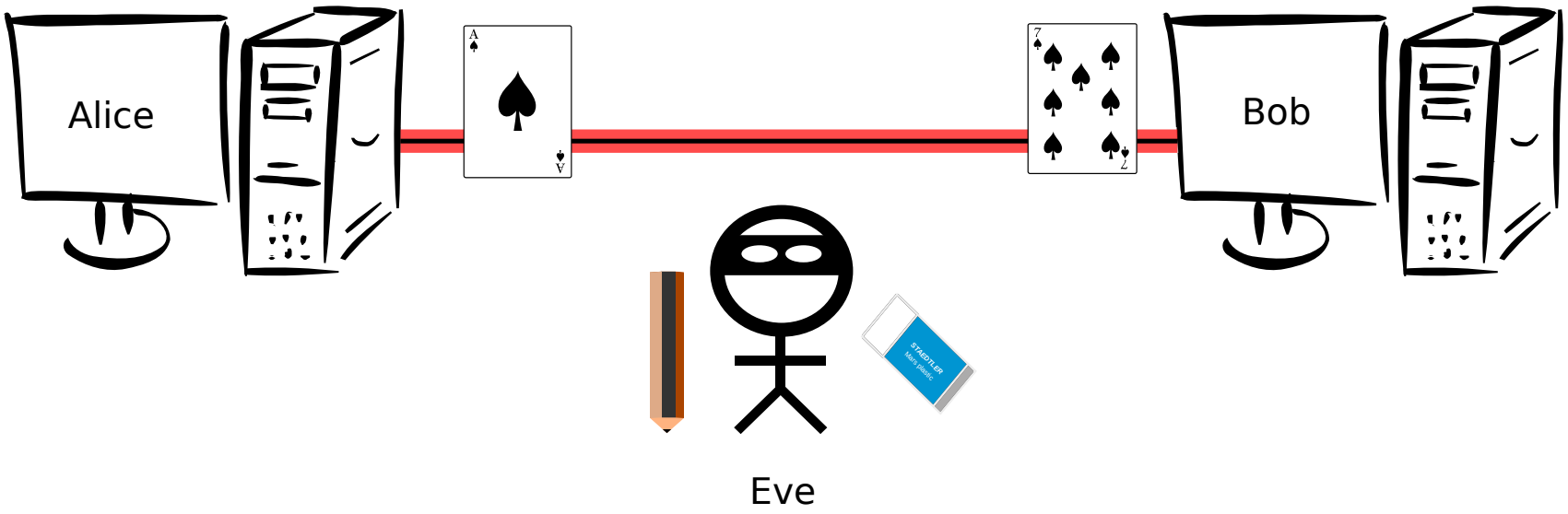
- Geschützte Daten können nur von Berechtigten genutzt werden.
- Vertraulichkeit gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten (Angreifer) eingesehen werden können
- In vernetzten Systemen ist zu betrachten
  - Der Transport von Daten (über Rechnernetze)
  - Speicherung von Daten (inkl. Backup)
  - Verarbeitung von Daten
- Typische Sicherheitsmaßnahme: Verschlüsselung
- Kontext Dienste: Vertrauliche IT-Dienste können nur von autorisierten Anwendern genutzt werden

Vertraulichkeit: Visualisierung

Integrität

- Geschützte Daten können nur von Berechtigten verändert werden.
- Integrität verletzt, wenn Daten von einem Angreifer unbemerkt verändert werden können.
- Wiederum bei Transport, Speicherung und Verarbeitung sicherzustellen!
- Typische Sicherheitsmaßnahme: Kryptographische Prüfsummen
- Kontext Dienste: Integre IT-Dienste haben keine (versteckte) Schadfunktionalität.

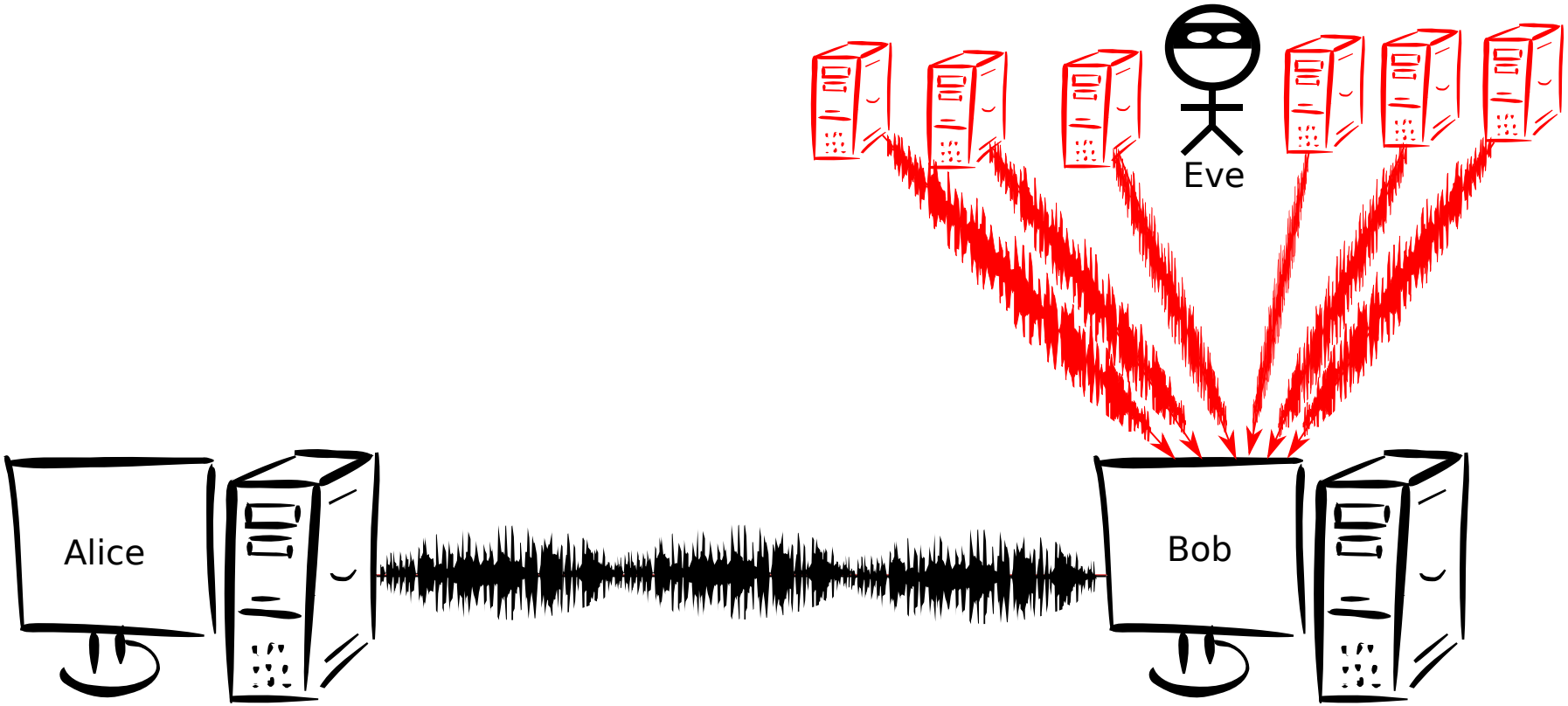
Integrität: Visualisierung



Verfügbarkeit

- Daten sind für berechtigte Nutzer verfügbar.
- Verfügbarkeit verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender einschränkt.
- Typische Sicherheitsmaßnahme: Redundanz (z.B. Daten-Backups), Overprovisioning (z.B. mehr als genug Server).
- Bezieht sich nicht nur auf Daten, sondern z.B. auch auf Dienste und ganze IT-Infrastrukturen.

Verfügbarkeit: Visualisierung



Werte

(Unternehmens-)werte (engl. assets) sind Objekte, die geschützt werden sollen.

- Daten
- Dokumente
- Physische Werte
- Software
- Dienstleistungen
- Mitarbeiter
- Immaterielle Werte

Angreifermodelle

Wer ist und was kann unser Angreifer?

- Position des Angreifers
  - Innentäter
  - Besucher, Einbrecher, ...
  - Intern / extern
- Fähigkeiten des Angreifers (= Wissen + finanzielle Möglichkeiten)
  - Experimentierfreudiger Amateur (Schüler, Student)
  - Kriminelle
  - Geheimdienste
- Motivation bzw. Zielsetzung des Angreifers
  - Spieltrieb, Geltungsbedürfnis, Vandalismus
  - Geld
  - Politischer oder religiöser Fanatismus, vermeintlicher Patriotismus
- Spezifische Charakteristika durchgeführter Angriffe,
  - Passives Abhören des Netzverkehrs
  - Aktive Eingriffe in die Kommunikation

Angreifer

Gruppenarbeit: Füllen Sie die Tabelle aus.

	Amateur	**Kriminelle**	**Dienste**	**(Ex-)Mitarbeiter**
Risiko				
Motivation				
Skill				
Budget				

Frage: Wer ist der gefährlichste Angreifer und warum?

6.2: Bedrohungs- und Risikoanalyse

Bedrohungsanalyse

Erstellung einer Liste aller möglichen Angriffe auf ein zu schützendes System.

Risikoanalyse

Bewertung einzelnen Bedrohungen, ggf. in Abhängigkeit von verschiedenen Angreifertypen

- Wahrscheinlichkeit des Eintretens
- Schwere des Schadens

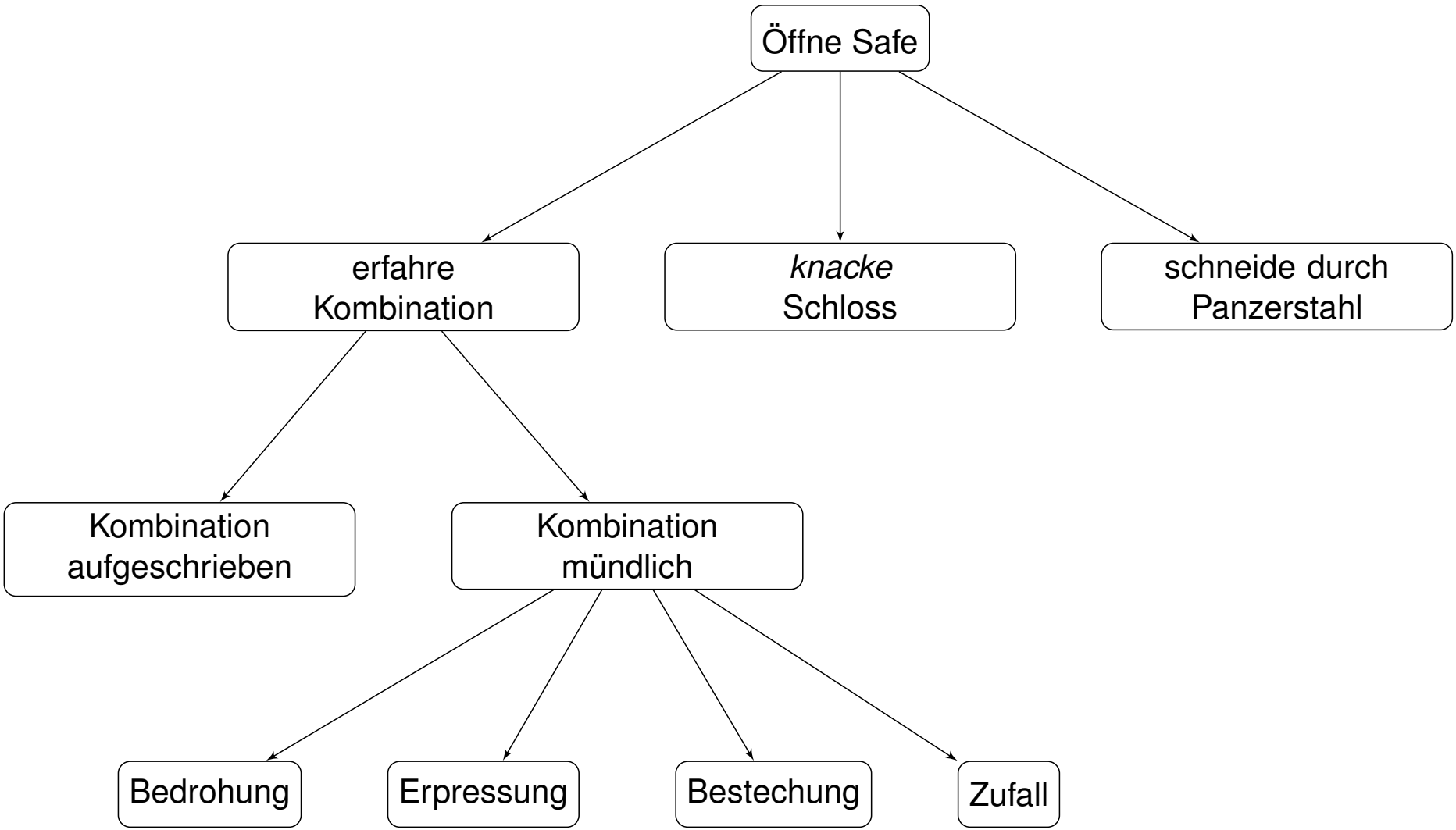
Bedrohungsanalyse

- Bedrohungsanalyse ist einfach: Man zähle einfach alle möglichen Bedrohungen auf.
- Gute Bedrohungsanalyse ist schwierig, wenn nicht gar unmöglich – ein *Security Engineer* sollte noch erfinderischer sein, als alle Gegner zusammen.
- Bedrohungsbäume (engl. Attack Trees) sind eine Methode, den schwierigen Prozess der Bedrohungsanalyse etwas zu systematisieren.

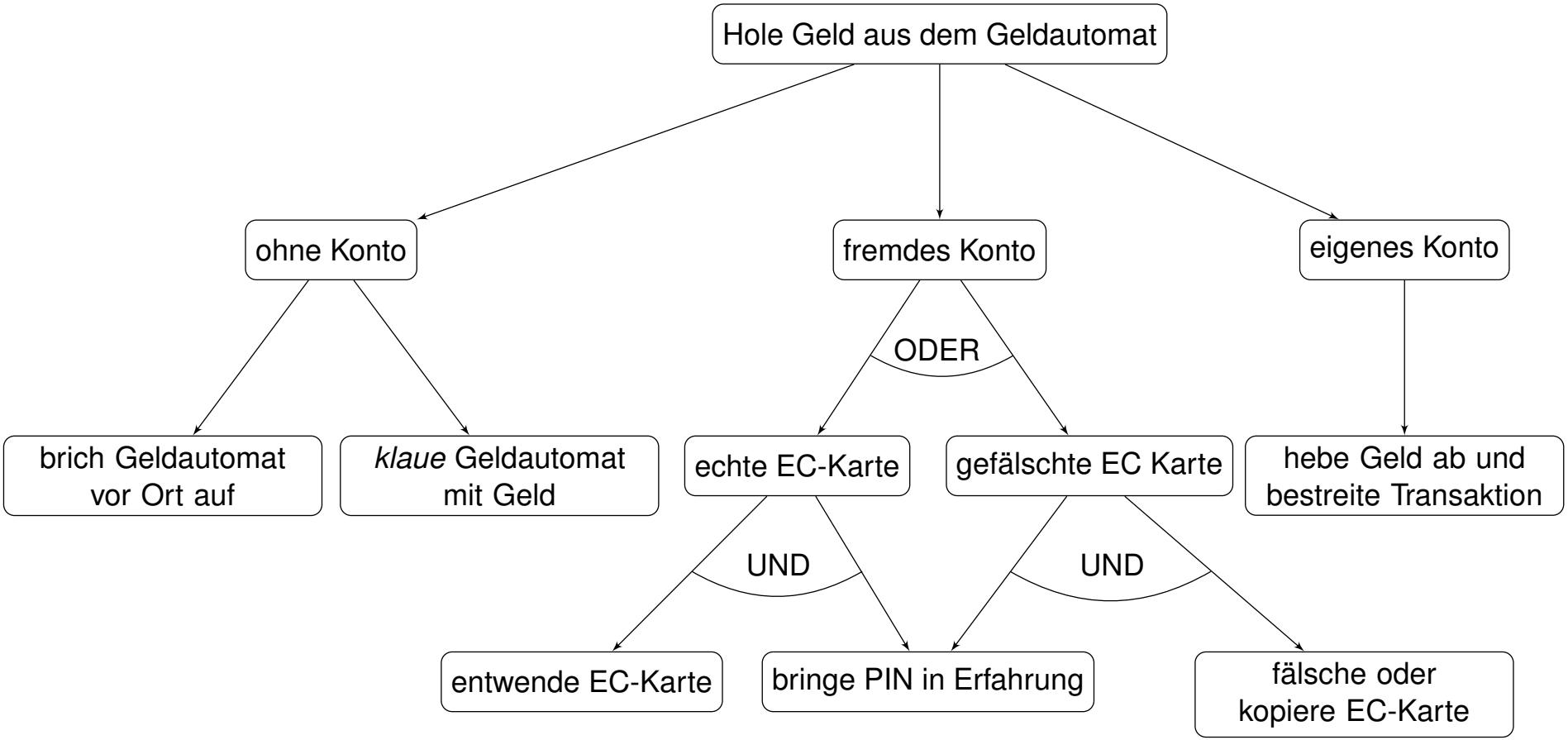
Bedrohungsbäume

- Jeder **Knoten** im Bedrohungsbaum repräsentiert ein mögliches **Ziel** für einen Angreifer.
- Die Nachfolger ("**Kinder**") eines Knotens K sind **Teilziele**, um das von K repräsentierte Ziel zu erreichen.
- Die Kinder eines Knotens K, können UND-verknüpft sein, dann muss man alle durch die Kinder repräsentierten Teilziele erreichen, oder sie können ODER-verknüpft sein, dann genügt es, eines der entsprechenden Ziele zu erreichen. (Üblicherweise werden UND-Verknüpfungen besonders markiert.)
- Die **Wurzel** eines Bedrohungsbaumes: **Angriffsziel** (=Verletzung eines Schutzzieles)

Beispiel: Bedrohungsbaum für Panzerschrank



Beispiel: Bedrohungsbaum für Geldautomat



Frage: Wie kann man eine EC-Karte fälschen oder kopieren *und* dabei eine passende PIN in Erfahrung bringen?

Beispiel: Klausur-Auskunftssystem

Projekt: Server, für Klausurergebnisse.

Eingabe: Matrikelnummer und Passwort
Ausgabe: Ergebnisse.

Schutzziel Vertraulichkeit: Unbefugte dürfen die Ergebnisse nicht erfahren. *(Es gibt offensichtlich noch andere relevante Schutzziele, aber wir konzentrieren uns auf dieses.)*

Man stelle einen Bedrohungsbaum auf ($\rightarrow$ Gruppenarbeit).

Risikoanalyse mit Bedrohungsbäumen

Die Risikoanalyse dient der Abschätzung, wie wahrscheinlich eine Bedrohung eintritt, und ggf. wie groß der angerichtete Schaden ist.

Die Wahrscheinlichkeit einer Bedrohung hängt oft von Angreifertypen ab, von den Fähigkeiten und Kenntnissen der Angreifer, von ihrer Risikobereitschaft, ihrer Motivation, ihrer Finanzierungsquelle, ...

Die Risikoanalyse dient dazu, unser Wissen um mögliche Bedrohungen mit unserem Wissen über potentielle Angreifer zu *verheiraten*.

Beispiel 1 Panzerschrank-Bedrohungsbaum

Welche Angriffe sind unmöglich, schwierig oder leicht, für

1. friedfertige Gelegenheitstäter

2. professionelle Einbrecher
   - 2.1 ohne Spezialausrüstung
   - 2.2 mit Spezialausrüstung

3. die Mafia

Beispiel 2: Geldautomat und zugehöriger Bedrohungsbaum.

Gruppenarbeit

- Welche Gruppen von Angreifern sollte man betrachten?
- Für jede dieser Gruppen überlege man sich, welche Angriffe möglicherweise "leicht" sind.
- Für welche Gruppe lohnt sich der Angriff?
- Überlegen Sie sich sinnvolle Maßnahmen um einen Angriff zu erschweren.

Umgang mit Risiko

- Das Risiko kann eliminiert werden.
- Das Risiko wird akzeptiert.
- Das Risiko kann durch eine Versicherung abgesichert werden.
- Das Risiko kann durch geeignete Maßnahmen reduziert werden.

Anmerkungen

- Die Bedrohungs- und Risikoanalyse sind ein wichtiger Teil der IT-Sicherheit, der leicht *vergessen* wird.
- Bedrohungs- und Risikoanalyse sind schwierige kreative Prozesse, die sich kaum formalisieren oder automatisieren lassen.
- Bedrohungsbäume sind ein Werkzeug für die Bedrohungs- und Risikoanalyse. Es gibt auch andere, z.B. Bedrohungsmatrizen.

Annual Loss Expectancy (ALE)

In der Literatur findet man oft den Vorschlag, die Kosten und den Erwartungswert der Häufigkeit des Eintretens einer Bedrohung konkret anzugeben. *(“Die Bedrohung tritt im Durchschnitt x-mal im Jahr ein, und jedes Eintreten kostet y EUR.”)*

Dies erlaubt die Berechnung der *“Annual Loss Expectancy”* (ALE):

xy EUR pro Jahr.

In vielen Fällen ist der tatsächliche Erwartungswert *x* unbekannt und wird einfach geschätzt, was die Benutzung der ALE als Entscheidungsgrundlage zur Kaffeesatzleserei degradiert.

6.3: ISO/IEC 2700x

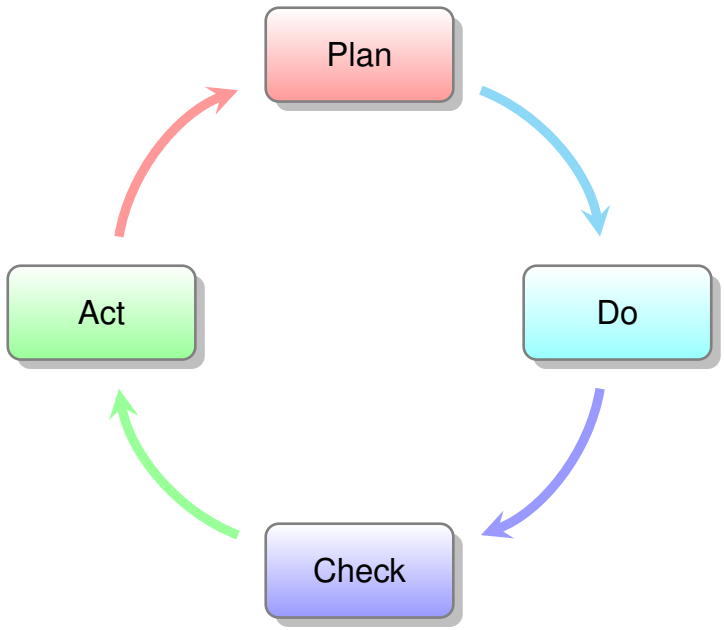
- Bei ISO/IEC 2700x handelt es sich um mehrere kostenpflichtige Standards zum Thema Informationssicherheit für Firmen
- Alternativ: die frei zugänglichen IT-Grundschutz-Kataloge vom BSI (Bundesamt für Sicherheit in der Informationstechnik).
- Idee: Anwendung der Grundprinzipien des Qualitätsmanagements auf das Management der IT-Sicherheit.
  - Kein *Übersehen* wichtiger Aspekte.
  - Organisationsübergreifende Vergleichbarkeit.
  - Nachweis von Engagement gegenüber Kunden und Partnern (Zertifizierung).

ISO/IEC 27001

Norm ISO/IEC 27001 legt Mindestanforderungen an sog. Information Security Management Systems (ISMS) fest.

- Zertifizierungen möglich für
  - Organisationen (seit 2005)
  - Personen (seit 2010)
- Inhaltliche Basis
  - Kontinuierliche Verbesserung durch Anwendung des Demingkreis (Plan-Do-Check-Act, PDCA)
  - Risikogetriebenes Vorgehen
- Seit 2008 auch DIN ISO/IEC 27001.

Demingkreis



Demingkreis (PDCA)

Demingkreis beschreibt einen vierphasigen Prozess zum Lösen von Problemen, der seine Ursprünge in der Qualitätssicherung hat.

Kerninhalte / Struktur von DIN ISO/IEC 27001

- Begriffsdefinitionen
- PDCA-basierter Prozess zum Konzipieren, Implementieren, Überwachen und Verbessern eines ISMS
- Mindestanforderungen u.a. an Risikomanagement, Dokumentation und Aufgabenverteilung
- Normativer Anhang A enthält:
  - Definition von Maßnahmenzielen (control objectives)
  - Definition von Maßnahmen (controls)
- Umfang: DIN ISO/IEC 27001:2015 - 31 Seiten

Maßnahmenziele und Maßnahmen: Überblick

A.5 Informationssicherheitsleitlinien

A.6 Organisation der Informationssicherheit

A.7 Personalsicherheit

A.8 Verwaltung der Werte

A.9 Zugangssteuerung

A.10 Kryptographie

A.11 Physische Sicherheit

A.12 Betriebssicherheit

A.13 Kommunikationssicherheit

A.14 Anschaffung, Entwicklung von Systemen

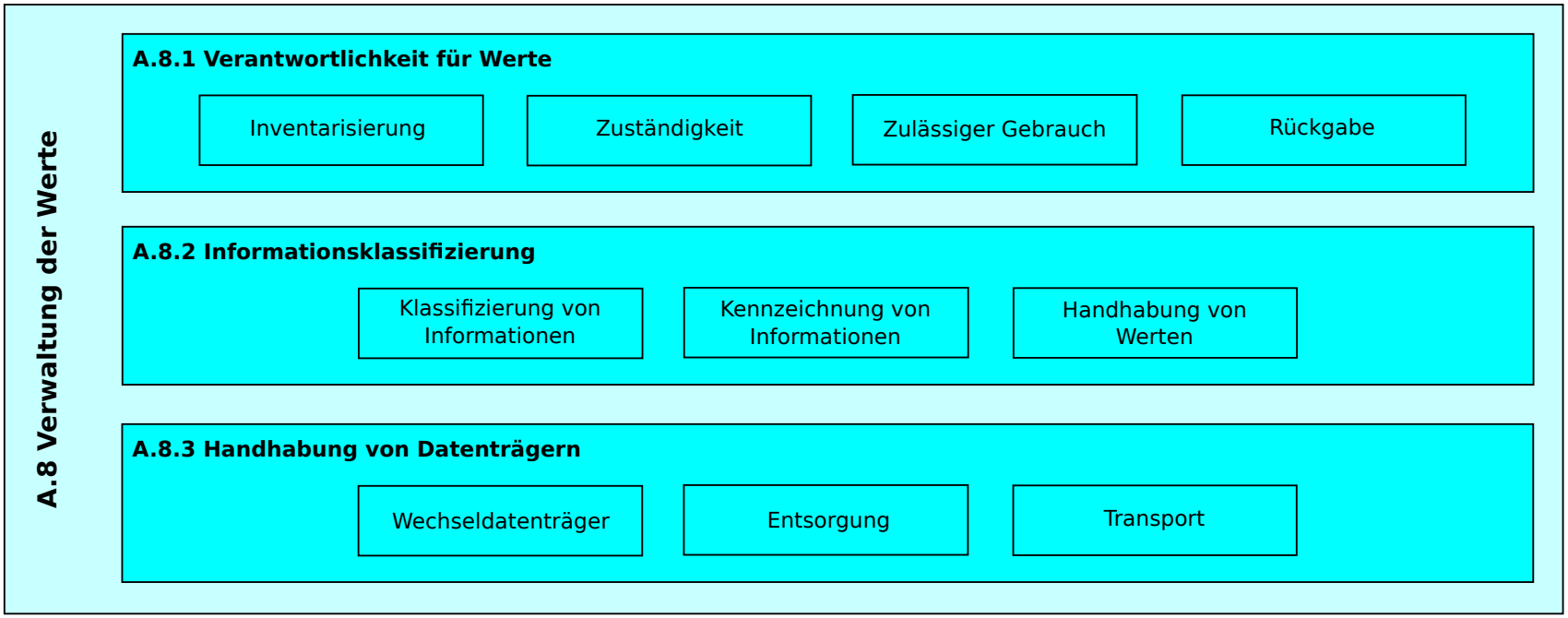
A.15 Lieferantenbeziehungen

A.16 Handhabung von Sicherheitsvorfällen

A.17 Business Continuity Management

A.18 Compliance

Beispiel: Maßnahmen in ISO/IEC 27001 A.8



Beispiel A.8.3.2 - Entsorgung von Datenträgern:

Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt. [DIN ISO/IEC 27001:2015-03, S. 19]

6.4: Der Ernstfall

- Phase 1: Vorbereitung für den Ernstfall
- Phase 2: Handeln im Ernstfall
- Phase 3: Forensik

Vorbereitung für den Ernstfall

- Legen Sie die Verantwortlichkeiten fest.
- Etablieren Sie ein Berichtswesen.
- Erstellen Sie Notfallpläne für kritische Systeme.
  - Konkrete Maßnahmen
  - Leitfaden
  - Simple Anweisungen (Stichpunkte)
  - Checklisten
- Kritische Systeme mit Rettungspaketen *versehen*.
  - `tar.bz2`- oder `zip`-Archive
  - Statisch gelinkte System- und Sicherheits-Werkzeuge
- Externe Gutachter zur Qualitätssicherung.
- Regelmäßige Übungen. (Virtueller Feueralarm)

Anmerkungen für den Ernstfall

- Automatisierte Abwehrmechanismen wie Firewalls und Spamfilter kümmern sich um *langweilige* und allgegenwärtige Angriffe.

- Ernstzunehmende Angriffe zu bemerken ist schwierig.
  - Anzahl Schadsoftware Stand Q1 2018: $>$ 771 Millionen.
  - Anzahl Schadsoftware von 2017: $>$ 121 Millionen.
  - Erkennungsrate von AV-Programmen (AV-Hersteller): 99%
  - Erkennungsrate von AV-Programmen (Research): 70%
  - Erkennungsrate von brandneuer Schadsoftware (Research): 5%

- Versierte Angreifer sind praktisch nicht verfolgbar.
  - Festnahmen sind die Ausnahme.
  - Verurteilungen sind sehr selten.

Handeln im Ernstfall

1. Bestätigen Sie den Angriff.
2. Arbeiten Sie die Notfallpläne ab.
3. Isolieren Sie kompromittierte Systeme.
4. Räumen Sie Ihre Infrastruktur wieder auf.
5. Stellen Sie den *Normalbetrieb* wieder her.
6. Überwachen Sie die wiederhergestellten Systeme.

Auf frischer Tat ertappt

Was Sollten Sie tun.

- Demotivation des Angreifers
  - Feedback eliminieren.
  - Feedback einschränken.
  - Feedback hinauszögern.
- Isolation der kompromittierten Systeme.
- Schnell und entschlossen handeln ($\rightarrow$ Notfallpläne).

Was sollten Sie auf keinen Fall tun.

- Motivieren Sie den Angreifer unter keinen Umständen.
  - Geben Sie dem Angreifer nicht ihren Namen.
  - Beleidigen Sie nicht die Intelligenz des Angreifers.
  - Verärgern/Drohen Sie dem Angreifer nicht.
- Keine Gegenangriffe.

Forensik

- Holen Sie sich professionelle Hilfe.
- Finden Sie die Sicherheitslücke.
- Versuchen Sie den Angriff komplett nachzuvollziehen.
- Schließen Sie die Sicherheitslücke.
- Passen Sie Ihren IT-Sicherheitsprozess an.
- Für IT Gerichtsverfahren gilt oftmals:
  Die Partei mit der umfangreichsten Dokumentation gewinnt.

Zusammenfassung

Sie sollten . . .

- . . . die Grundregeln des Security Engineering kennen.
- . . . verstanden haben, dass es sich bei IT-Sicherheit um einen Prozess handelt.
- . . . die drei Schutzziele der IT-Sicherheit kennen.
- . . . das Konzept Der Bedrohungsbäume verinnerlicht haben.
- . . . wissen was eine Risikoanalyse ist.
- . . . wissen was es mit ISO/IEC 2700x auf sich hat.
- . . . wissen was im Ernstfall zu tun ist.