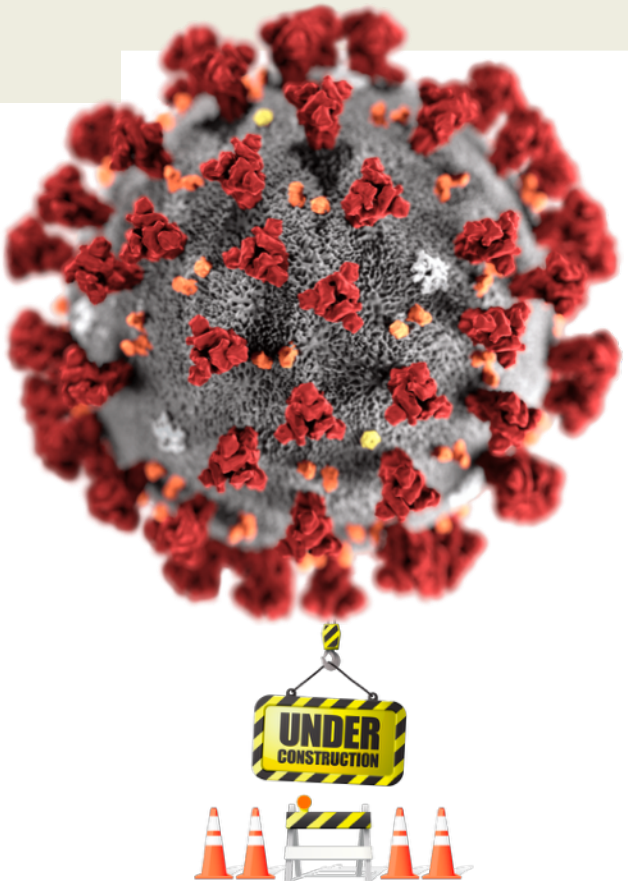
isec: Informationssicherheit

WS 2024/2025



Prof. Dr.-Ing. Carsten Bormann
PD Dr. habil. Karsten Sohr
Dr.-Ing. Stefanie Gerdes
Jan-Frederik Rieckers
Finn Marvin Ewers
Andreas Benischke

mailto:isec@tzi.org https://mattermost.informatik.uni-bremen.de/isec2024

Di 14–~17 im MZH 6200 und im Stud.IP-Meeting

Inhalt: **Security**

- Sicherheitsziele; Zugriffskontrolle
- Schwachstellen; Firewalls
- Kryptographische Grundfunktionen **und ihre Einsatzbereiche**
- **Sicherheitsprotokolle**
  - Authentisierung, Schlüsselverwaltung, …
  - **Kerberos, IKEv2, TLS, EAP-__, SAML, …**
- S.-Management, **s. Engineering**
- S.-Bewertung; Ausblick

Inhaltliche Voraussetzungen

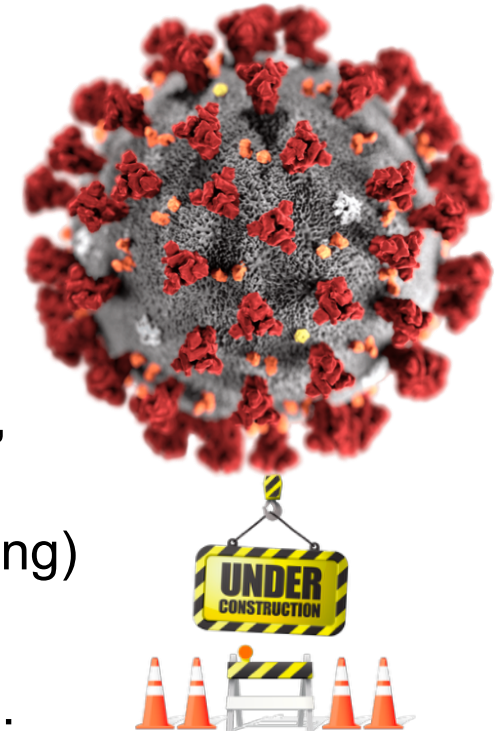
isec

RN

Grundstudium, u.a.:
TeI2

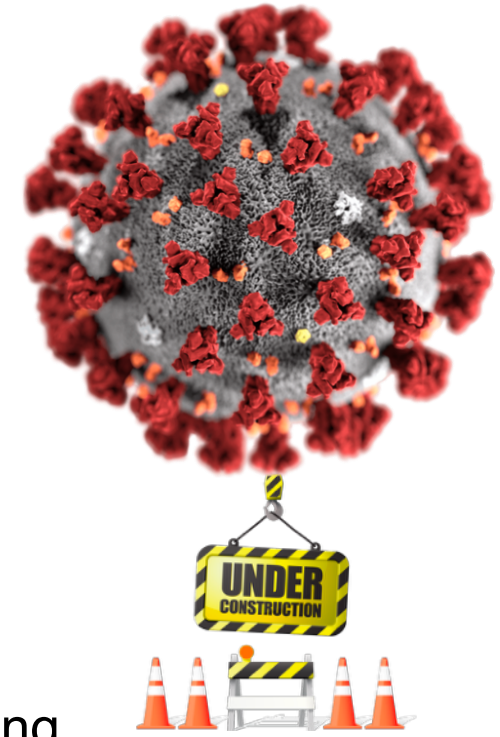
- 5. Semester: isec
  Grundlagen der Informationssicherheit
- 4. Semester: Rechnernetze
  Grundlagen Netze und Medien (Wahlpflicht)
- 3. Semester: TeI2 (DM/WI: TGI)
  Grundlagen Betriebssysteme und nebenläufige Systeme (Pflicht)

Form



- Team
  - Carsten Bormann, Karsten Sohr: „Vorlesung“ (Video), Fragestunde Di 14–~15: MZH 6200/Stud.IP-Meeting
  - Tutoren: „Übungen“ (Di ~15–~16: MZH/Stud.IP-Meeting)
- Integrierte Veranstaltung:
  - Plenum: ~~Vorlesungen,~~ Demonstrationen, Übungen, …
  - Übungsaufgaben (in Kleingruppen)
- Prüfungsrelevante Studienleistung: 6 CP (ECTS)
  - Übungsblätter (alle bearbeitet, $\sum$ 50 % der Punkte)
  - Fachgespräch am Ende des Semesters
- ggf. Modulprüfung auch als mündliche Prüfung
  - Teilnahme am Übungsbetrieb geboten; Übungen vertiefen Vorlesung

„Vorlesung“ **asynchron**



- Vorlesung als Video: Folien + Sprache
  - Carsten Bormann, Karsten Sohr
- Verfügbar zum Herunterladen auf Stud.IP
  - Jeweils zum Wochenende vor der Fragestunde (Di)
- Zum besseren Suchen: Folien auch als PDF
  - Folien ohne Sprache ersetzen aber **nicht** die Vorlesung

- Fragestunde: Di 14–~15 **synchron** (MZH 6200/Stud.IP-Meeting); bitte vorbereiten
- Fragen vorher schon (und nachher) in Mattermost möglich
  - Kein SLA für die Antwort :-)
- An Fragestunde schließt sich Tutorium an (Di ~15–~16)

Übungen

- 3er-Gruppen ($3 \leq N \leq 3$)
- Ausgabe
  - in Stud.IP + Vorstellung in der Übung
  - meist wöchentlich, am Mo
- Bearbeitung in der Gruppe
  - Ansätze diskutieren, ausführen, ggf. implementieren
  - ggf. Austausch mit anderen Gruppen, aber individuelle Abgaben
- Abgabe
  - in Stud.IP; Dokumente im markdown-Format + PDF-Rendering; mehrere Dateien in einem ZIP-Archiv
  - normalerweise in der Woche nach Ausgabe (Mo → Do+1 23:59)
- Fachgespräch
  - Feststellung der individuellen Leistung
  - ggf. Differenzierung der Teilnehmer

Flow der Wochen

- Uploads in Stud.IP:
  - Freitag: Neue Vorlesung N (Folienvortrag als Video, nackter Foliensatz als PDF)
  - Montag: Neues Übungsblatt N
- **Vor Di 14 Uhr**: Teilnehmende
  - **arbeiten die Vorlesung durch** (z.B. mit VLC) und
  - schauen das Übungsblatt durch (klar, was zu tun ist?)
- Synchron am Dienstag 14 Uhr:
  - Fragestunde zur Vorlesung N. Bitte **Fragen** dazu vorbereiten.
  - Klarstellung aktuelles Übungsblatt N. Bitte **Fragen** dazu vorbereiten.
  - Besprechung zurückgegebenes Übungsblatt N-2. Feedback.
- **Nach Di 14 Uhr: Bearbeitung Übungsblatt in der Gruppe (gern im MZH)**
  - Ansätze diskutieren, ausführen, ggf. implementieren
  - ggf. Austausch mit anderen Gruppen, aber individuelle Abgaben
- Abgabe Übungsblatt **spätestens** am Donnerstag Woche N+1 23:59 UTC
  - OK, das ist zu viel Zeit ins Land; besser schon am Freitag Woche N abgeben.

Neu und verbessert: isec3+3

- 3 CP in der Vorlesungszeit
  - Kann mit **Fachgespräch** abgeschlossen werden („erfolgreicher Abbruch“)
- 3 CP Blockwoche im Februar
  - (Eine Brückenübung)
  - Eine Woche kompakt (KW7: 2025-02-10..–14?)
    - Vornehmlich Laboranteil (tägliche, etwas größere Übungen)
    - Ein paar Vorlesungen/Einführungen dazu
    - **Fachgespräch** zum Abschluß (gleich schon am Fr., 14.02.2025 möglich)
- Über bearbeitetes 3+3 ist auch **mündliche Prüfung** möglich

„Präsenz“ WS 2024/2025

- Dienstags 14–18 Uhr MZH 6200
- Immer Combo Präsenz/BBB
- Heute, evtl. weitere Termine:
  Projektion BBB durch Lehrveranstalter
- Andere Termine: Jemand von Euch schnappt sich den Projektor und projiziert BBB
- Wichtig: Gemeinsames Bearbeiten von Übungsaufgaben nach Fragestunde/Tutorium
  - Präsenz: Grüppchen im Raum
  - BBB: Breakout-Rooms

„Du“

- Wen duzt man als Studi in einer Universität:
  - Studis
  - Wissenschaftliches Personal
  - Junge/junggebliebene :-) Professoren
  - Und auf jeden Fall mich!
- Wen siezt man:
  - Professoren (jedenfalls erst einmal auf Verdacht)
    - Vor allem, wenn mit Krawatte ☺
  - Verwaltungsmitarbeiter
- Was soll das alles?
  - Keine Ahnung...

Carsten Bormann

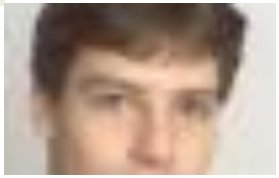
- Promoviert an der TU Berlin 1990
  - Offene Dokumentverarbeitung (ODA/SGML)
    ≈ „XML-Technologien“
- Universität Bremen
  - Honorarprofessor für „Internet-Technologie“
  - TZI-Vorstand (LT „Empowering Digital Media“)
  - Vorlesungen in Rechnernetze und Medieninformatik
- UdK Berlin
  - Studiengang „Electronic Business“
    Technical Literacy
- Teknillinen Korkeakoulu (Aalto U)
  - Tietoverkkolaboratorio (netlab)
  - Protokollasuunnittelu

IoT
CoAP
CBOR
➔ 60 RFCs

Technologie-Zentrum Informatik

HELSINKI UNIVERSITY OF TECHNOLOGY

Karsten Sohr

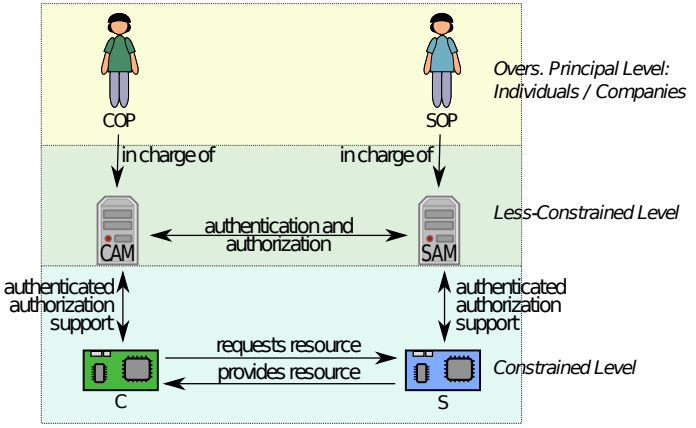


- Promoviert an der Uni Marburg 2001
  - Java-Sicherheit
- Universität Bremen
  - Koordinator am TZI für Informationssicherheit
  - Forschungsthemen
    - Rollenbasierte Zugriffskontrolle
    - Formale Methoden und Informationssicherheit
    - Sicherheit mobiler Anwendungen
  - Beteiligung an diversen Forschungsprojekten (BMBF, BMWI, DFG) zu den Themen rollenbasierte Zugriffskontrolle, RFID-Sicherheit, Sicherheit mobiler Applikationen, Intrusion Detection und KI

Technologie-Zentrum Informatik

Stefanie Gerdes

- Promoviert an der Uni Bremen 2021
  - Authentisierte Autorisierung für das Internet of Things
- Universität Bremen
  - Vor der Promotion: WiMi / Lehre Informationssicherheit
  - Seit 2021: Postdoc
  - Forschungsschwerpunkt Security
- Forschung
  - Authentisierung, Autorisierung
  - Co-Autorin libdcaf
  - Standardisierung in der IETF ACE WG



Jan-Frederik Rieckers

- Informatik-Student im Master
- Mitarbeiter am Deutschen Forschungsnetz (DFN)
- Interessengebiete:
  - Serveradministration
  - Rechnernetze (Layer 1-3)
- Aktueller Forschungsschwerpunkt:
  - TLS im eduroam-Login
  - EAP-FIDO/EAP-NetAuthn

Finn M. Ewers

- Informatik Vollfach. (seit WiSe 2019/2020)
- Für Informationssicherheit begeistert seit 2017
- Seit WiSe 2021/2022 Teil des Roboter-Fussball Teams B-Human

Andreas Benischke

- 7. Semester
  Informatik Vollfach
- professionell begeistert
  für Informationssicherheit
  seit 2022
- regelmäßiger
  CTF-Teilnehmer
  und TryHackMe-Nutzer

Wie studiert man **isec**?

- Vorlesung: Zuhören, mitdenken, Fragen stellen
  - für die Fans des Mitschreibens: Folien sind im Web
- Übungsaufgaben: bearbeiten
  - Wirklich... In der Gruppe...
- Stud.IP/Web: Eigenständig Stoff bearbeiten
  - Nicht überfliegen wie andere Webseiten
  - Übungsaufgaben/Fragebögen nutzen
- Vor Fachgesprächen: zeitig Stoff durchgehen
  - Fragebögen als Gedächtnisstütze

Fragen ?

Noch kurz zum Thema Fragen ...

- Bitte Fragen stellen, wenn etwas unklar ist.
  Ich kann leider nicht hellsehen.
- Fragen helfen mir, den nachfolgenden Stoff besser aufzubereiten – also wieder Euch selbst.
- Nein, Fragen sind nicht zu dumm. Hier nicht.
- Es stimmt wirklich: Wer nicht fragt, bleibt dumm.
- Für viele Themen gilt hier: „Last chance to see ...“

Fragen ?

Gruppenbildung

- Bitte Dreiergruppen bilden...
- ... und in Stud.IP eintragen

Informationssicherheit:
Einführung

Wozu Sicherheit?

- Erwartung an IT-Systeme: **Verlässlichkeit**
  - Immer mehr, immer wichtigere Aufgaben werden IT-Systemen übertragen
- Problem: Bugs, Abstürze, Fehlfunktionen, Naturkatastrophen
- Problem: **Böse Absicht** (aber auch böse Zufälle)

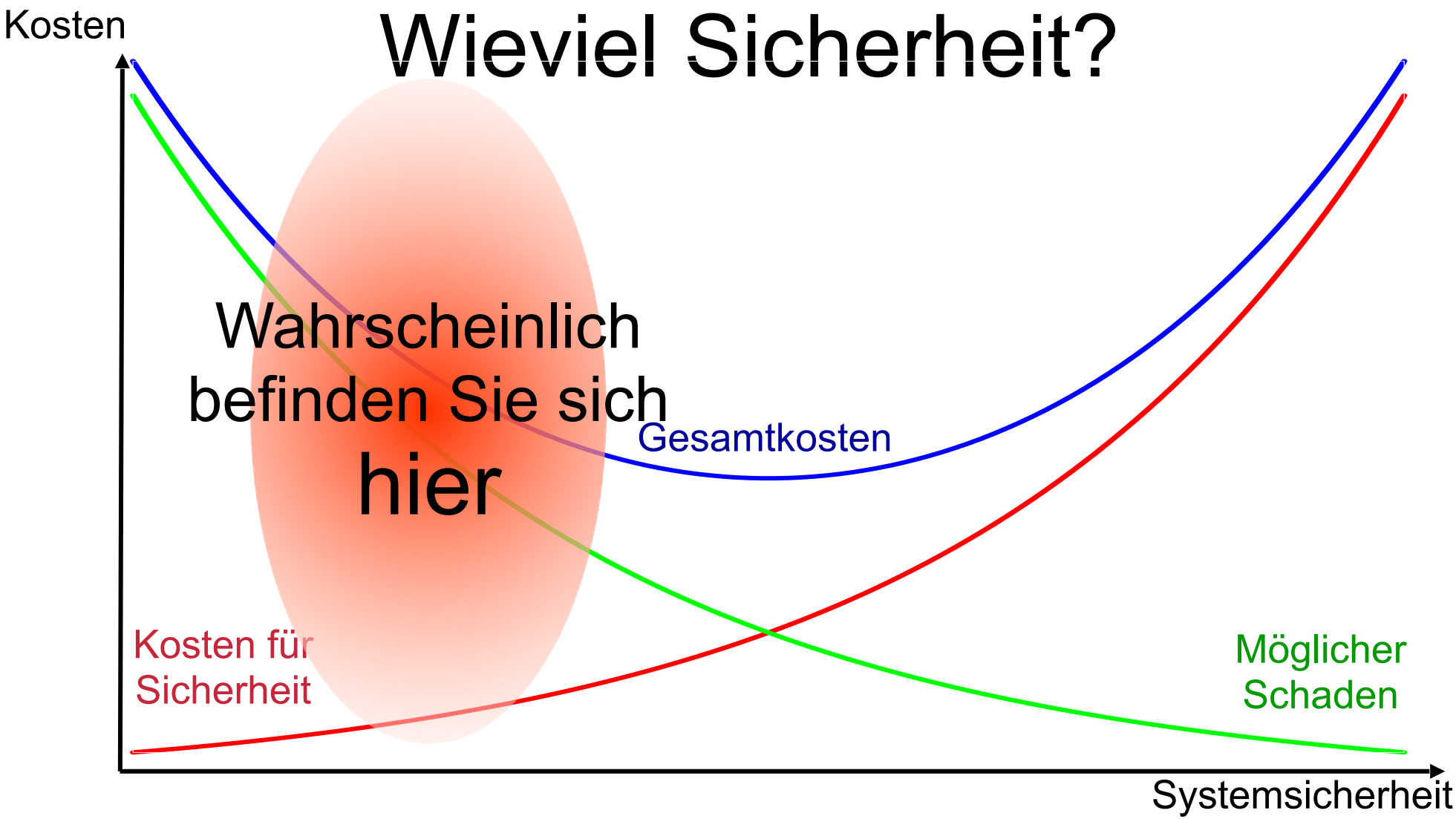
Stark vereinfacht:

- Sicherheit *(Safety)*:
  System hat von sich aus keine Fehlfunktionen
- Sicherheit *(**Security**):* Sicherheit gegen böse Absicht

Safety vs. Security

- Nicht immer klare Trennung
- Sicherheit gegen Angriffe (Security) liefert oft auch Sicherheit gegen unbeabsichtigte Fehlbedienung
- Betriebssicherheit (Safety) vs. Funktionssicherheit
- Gelegentlich Widerspruch (Beispiel Fluchttür)

Wieviel Sicherheit?



Sicherheitsprobleme

- Für ein **System** bestehen **Sicherheitsziele** ***(security objectives)***
- Sicherheitssysteme haben **Schwachstellen (*weaknesses)***
- **Verwundbarkeiten *(vulnerabilities)*** erlauben das Umgehen (oder den Missbrauch) von Sicherheitsmechanismen
- Eine **Bedrohung *(threat)*** ist die Möglichkeit eines **Angriffs *(attack)***
- Angriffe erzeugen u.U. **Schaden *(damage)***
- **Risiko *(Risk)*** = p(attack) × cost(damage)

Risiko einschätzen

- Problem **allgemein**:
  Availability Bias (Verfügbarkeitsheuristik)
  - Schwierig, seltene Risiken einzuschätzen:
    “Bis jetzt ist nichts passiert” vs. heftig beworbene Risiken
  - Flugangst, Kernenergie vs. Klima, Impfangst…
- Problem **Informationssicherheit**:
  Risiken hängen von Angreifern ab
  - Wo ist gerade deren Fokus?
  - Welche anderen Vorgehensweisen gehen nicht mehr?
  - Wie haben sich technische Voraussetzungen geändert?

Sicherheitssysteme

- Erfolgreiche Angriffe
  - Verhindern *(prevention)*
  - Erkennen *(detection)*
  - Eingrenzen (Schadensbegrenzung) *(containment)*
- Sicherheitsregeln ***(security policy)***
  - Richtlinien; Schulung der Mitarbeiter
  - Notfallplanung, -training
  - Management-Unterstützung, Schutz der Sicherheitsverantwortlichen

Wer sind die Angreifer?

- **Insider** (faul, anders fokussiert, frustriert, kriminell)
  - Evtl. als Folge von **Social Engineering**
- **„Hacker“** (richtiger: Cracker), „script kiddies“
  - Pures Interesse, Spaß/Spannung/Sucht, Geltungssucht!

- **Professionelle** Angreifer (Spionage, Geheimdienste)
- Organisiertes **Verbrechen**
  - Z.B. Erpressung
  - Z.B. Ausschalten eines Konkurrenten, Wirtschaftsspionage
  - Z.B. Beschaffung einer Plattform für weitere Angriffe

Forensic Readiness

- Prevent
- Detect
- Contain
- **Prosecute**
  - (or at least fend off the inevitable law suits)

Sicherheitsziele

- **Vertraulichkeit**/Geheimhaltung/Datenschutz
  - Anonymität
- **Integrität**/Authentizität
- Zurechenbarkeit/Verbindlichkeit
- **Verfügbarkeit**

Vertraulichkeit/Geheimhaltung/ Datenschutz

- Vertraulichkeit ***(confidentiality)***: Verpflichtung zur Geheimhaltung der Informationen anderer
- Geheimhaltung ***(secrecy)***: Einschränkung des Zugriffs
- Datenschutz ***(privacy)***: Recht auf Schutz eigener (persönlicher) Informationen

- Achtung: Oft ist die Tatsache einer Kommunikationshandlung bereits geheimzuhaltende Information (vs. ***traffic analysis***)

Anonymität

- Anonymität (**anonymity**): Durchführung von Handlungen ohne Preisgabe der Identität
  - Evtl. auch Preisgabe eines **Pseudonyms**
  - Anonymität = Vertraulichkeit der Identität

Integrität/Authentizität

- Integrität (***integrity***) der Daten: Schutz vor **unautorisierter** und **unbemerkter** Veränderung von Daten.

  (vgl. Integritätsbegriff aus den Datenbanken)

  Beispiel: Kontendaten in einer Bank

- Authentizität (***authenticity***): Information ist **integer** und **frisch**; eindeutig einer **Identität** zuzuordnen

Zurechenbarkeit/Verbindlichkeit

- Zurechenbarkeit (***accountability***): Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.
- Verbindlichkeit (***3rd-party verifiability, 'non-repudiation'***): kein unzulässiges Abstreiten durchgeführter Handlungen

  Notwendig beispielsweise für:
  - Abschließen von elektronischen Kaufverträgen
  - Digital unterschriebene Gerichtsanträge

Authentizität, Zurechenbarkeit, Verbindlichkeit

	A	B	C (Dritter)
Authentisierung	Will →	**Weiß**	—
Zurechenbarkeit	(...)	**Weiß**	—
Verbindlichkeit	(...)	Will →	**Weiß**

Verfügbarkeit

- Verfügbarkeit *(**availability**)*: Schutz vor unbefugter Beeinträchtigung der Funktionalität von Komponenten, Diensten etc.
  - vs. Denial-of-Service- (DoS-) Angriffe
- Ergibt zusammen mit Korrektheit: Verlässlichkeit ***(dependability):*** Funktionssicherheit; zuverlässige Erbringung der Funktion ***(reliability)***

Eselsbrücke: **CIA**

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Gruppenbildung

- Bitte Dreiergruppen bilden...
- ... und in Stud.IP eintragen