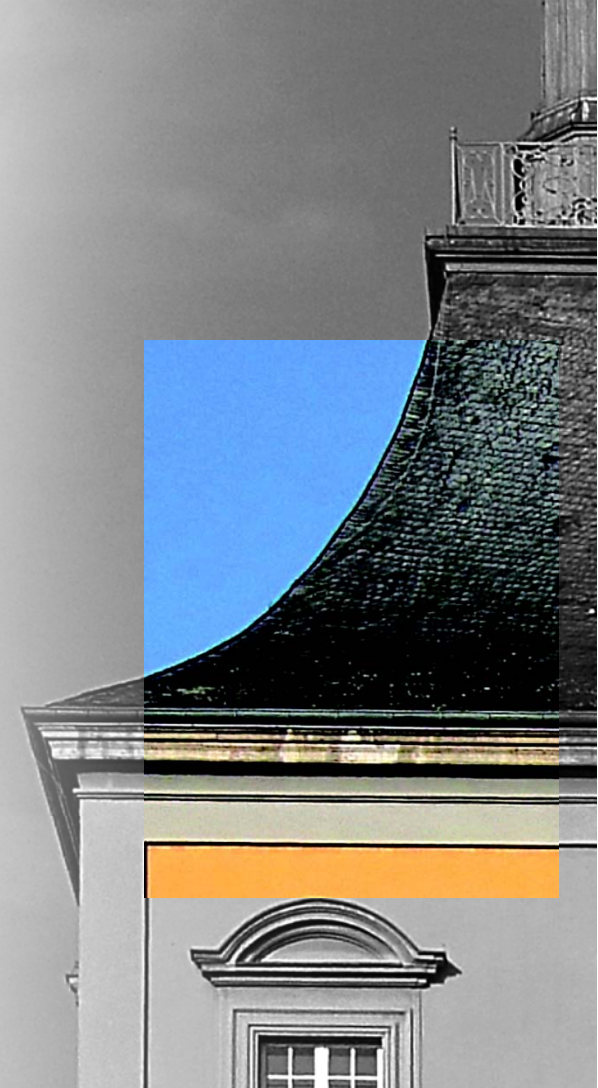


VORLESUNG  
**NETZWERKSICHERHEIT**

**SOMMERSEMESTER 2021**  
**MO. 14-16 UHR**



# BUGBOUNTY-CHALLENGE

Bisher wurden noch keine Punkte vergeben.

Platz	Studi	Punkte
1.	Hier könnte dein	Name stehen
2.	Hier könnte dein	Name stehen
3.	Hier könnte dein	Name stehen



# KAPITEL 2

# **GRUNDLAGEN**

# **IT-SICHERHEIT**

## Relevante Grundlagen der IT-Sicherheit (VL GRITSI) und mehr:

- Schutzobjekte / Daten
- Bedrohungen / Bedrohungsmodelle
- Schutzziele
- Angreifer / Angreifermodelle
- Maßnahmen

## IT-Systeme

- Personal Computer / Server
- (Aktive) Netzwerkelemente
- Mobiltelefone
- Fernseher
- Autos

## Informationen

- Beliebige Daten
- Interpretation der Daten

## Aktive/Passive Objekte

- Verarbeiten Informationen (Prozesse)
- Speichern Information (Dateien)

## Subjekte

- Benutzer
- Aktive Objekte (=Prozesse) in Ausführung durch Benutzer
- Gruppen

## Zugriffe

- Klassische Zugriffe (Inhalte):
  - Lesezugriff (R)
  - Schreibzugriff (W)
  - Ausführen (X)
- Erweiterte Zugriffe (Metadaten)
  - Dateiinformationen
  - Zugriffsrechte
  - Sticky-Bits (Benutzer / Gruppen / Berechtigungen)

## Allgemein:

- Unbefugter Zutritt (Räumlichkeiten / Infrastruktur / Dienste / Accounts / ...)
- Unautorisierter Zugriff (Daten / Informationen / ...)
  - Einsichtnahme (Lesen / Abhören / ...)
  - Veränderung (Fälschung / Löschung / ...)
- Unbefugte Aktionen (Prozesse)
  - Unautorisierte Tätigkeit (Code-Injection / Social-Engineering / ...)
  - Durch manipulierte Dritte (Privilege-Escalation / CEO-Fraud / ...)
- Verhinderung der Dienstleistung (Denial-of-Service)



## STRIDE (Microsoft)

- **S**poofing - Täuschung über die eigene Identität / Position / Kompetenz
- **T**ampering - Manipulation / Sabotage / Entzug der Integrität
- **R**epudiation - Abstreithen der Verantwortung
- **I**nformation Disclosure - Offenlegen von Vertraulichkeitsdaten
- **D**enial-of-Service - Ressourcenentzug
- **E**levation of Privilege - Rechteerweiterung



# SCHUTZZIELE

## CIA++

- Vertraulichkeit - Inhalte / Existenz
- Integrität - Inhalte / Ersteller / Absender / Zeitpunkte Erstellung und Änderung
- Verfügbarkeit - Informationen / Dienste
- Zurechenbarkeit - Ersteller / Zeitpunkt / Ort
- Untergeordnete Schutzziele
  - Unverkettbarkeit, Nicht-Verfolgbarkeit
  - Transparenz, Revisionsfähigkeit
  - Abstreitbarkeit, Nicht-Abstreitbarkeit



## STRIDE (Microsoft)

- **S**poofing - Zurechenbarkeit
- **T**ampering - Integrität
- **R**epudiation - Nicht-Abstreitbarkeit
- **I**nformation Disclosure - Vertraulichkeit
- **D**enial-of-Service - Verfügbarkeit
- **E**levation of Privilege - Autorisierung

## Unterschiedliche Daten

### ■ Möglichkeiten zur Klassifikation?

	Bewegte Daten	Stationäre Daten	Lokale Daten
<b>Kundendaten</b>	Online-Formulardaten, E-Mails	Datenbanken (Stammdaten, Abrechnungsdaten, Bestelldaten)	Fallbezogene Datensätze, E-Mails
<b>Unternehmensdaten</b>	Briefe (Steuerdaten, Gehaltsbescheinigungen), E-Mails (Angebote, Bestellungen)	Datenbanken (Abrechnungsdaten, Mitarbeiterdaten), Richtlinien, Dokumentation	Projektbezogene Datensätze, Fallbezogene Dokumente, Präsentationen
<b>Geistiges Eigentum</b>	Binärcode, Produktionsdaten, Produktdaten (Preise, Angebote ), E-Mails	Sourcecode, Produktionsdaten (Zeichnungen, Dokumentation), Produktdaten (Preiskalkulation, ...)	Entwicklungsdaten

## Relevante Daten im Bereich Netzwerksicherheit?

- Passive Angreifer
  - Mitlesen bewegter Daten (Eavesdropping)
  - Verbindungs-/Verkehrsdatenanalyse (Metadaten)
  
- Aktive Angreifer
  - Datenmanipulation (Man-in-the-Middle)
    - Transmit, Replay, Modify, Delete
  - Denial-of-Service

## Cybercrime

- Akteure
  - Skript-Kiddies / Einzeltäter / Hacktivisten
  - Organisierte Kriminalität / Terrororganisationen
- Methodik
  - Denial-of-Service
  - Code-Injection & Daten Exfiltration (Identitätsdatendiebstahl)
  - Standard-Malware (Botnetze / Ransomware)
  - SPAM / Phishing / CEO-Fraud
- Wirtschaftlich / Politisch motiviert



## Cyberwar

- Akteure
  - Mitbewerber
  - Staatliche Akteure
- Methodik
  - Individuelle Malware (z.B. Stuxnet)
  - Spear-Phishing / Social-Engineering
  - Advanced Persistent Threats (APT)
- Wirtschaftlich / Staatlich motiviert



## ▪ Schutzziele

- Zurechenbarkeit
  - Signaturen
- Integrität
  - Prüfsummen und Signaturen
- Verfügbarkeit
  - Redundanz
- Vertraulichkeit
  - Verschlüsselung

Bewegte Daten

Bei stationären und lokalen Daten:  
Zugriffskontrolle



Fazit: Übergeordnete Schutzziele durch kryptografische Verfahren sicherstellen

- Hashsummen
- Signaturen
- Verschlüsselung
  - Symmetrisch
  - Asymmetrisch
  - Hybrid
- Public-Key-Kryptografie für bewegte Daten verwenden!

## Public-Key-Kryptografie

- Absicherung der Kommunikation

- SSL/TLS
- GnuPG
- S/MIME

Inhalt der nächsten Vorlesung

- Absicherung stationärer / lokaler Daten

- Z.B. verschlüsselte Backups (wie <https://www.duplicati.com>)

- Standards: Public Key Cryptography Standards (PKCS)

- Bedrohungen
  - Zugriff / Manipulation / Löschung von Information
  - Denial-of-Service von Diensten / Infrastruktur
- Angreifer
  - Cyberwar vs. Cybercrime (inkl. Angreifermodelle)
- Schutzziele
  - Systematisierung von Eigenschaften der Subjekte / Daten / Objekte
- Maßnahmen
  - Zum Erreichen genannter Eigenschaften der Schutzziele

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 3. Mai 2020

Nächste Übung:

- Dienstag, 27. April 2020 – 16 Uhr
- Abgabe des Übungszettels 1 bis morgen – 16 Uhr