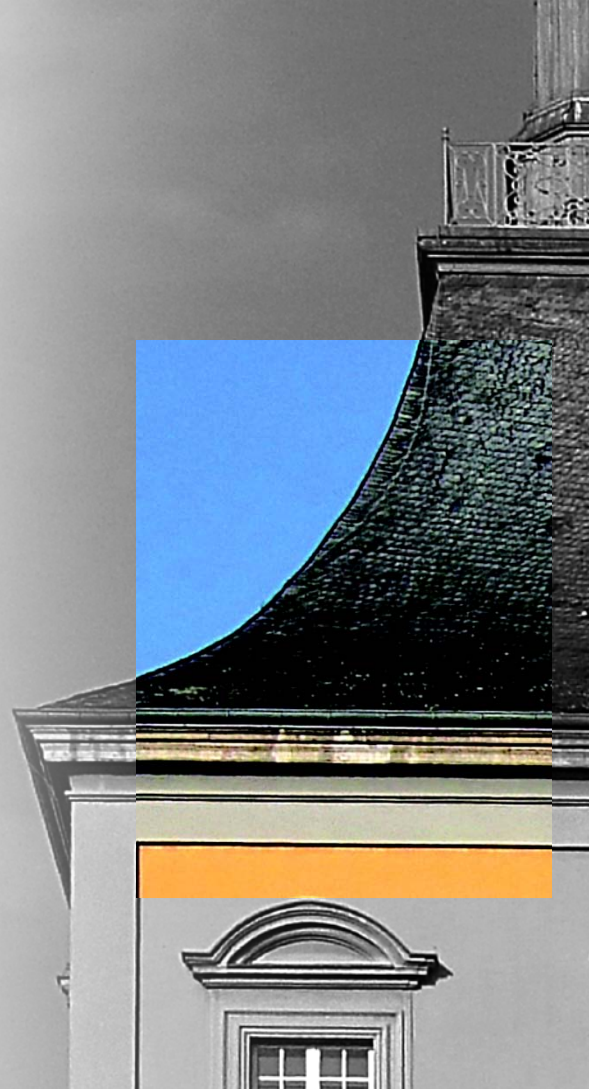
UNIVERSITÄT BONN

VORLESUNG

NETZWERKSICHERHEIT

SOMMERSEMESTER 2023

MO. 14-16 UHR



UNIVERSITÄT BONN

KAPITEL 2

GRUNDLAGEN IT-SICHERHEIT

UNIVERSITÄT BONN

IT-SICHERHEIT

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

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

UNIVERSITÄT BONN

SCHUTZOBJEKTE / DATEN

IT-Systeme

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

Informationen

- Beliebige Daten
- Interpretation der Daten

UNIVERSITÄT BONN

SCHUTZOBJEKTE / DATEN (FORTS.)

Aktive/Passive Objekte

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

Subjekte

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

UNIVERSITÄT BONN

SCHUTZOBJEKTE / DATEN (FORTS.)

Zugriffe

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

UNIVERSITÄT BONN

BEDROHUNGEN

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 Diensterbringung (Denial-of-Service)

UNIVERSITÄT BONN

BEDROHUNGSMODELLE

STRIDE (Microsoft)

- **S** poofing - Täuschung über die eigene Identität / Position / Kompetenz
- **T** ampering - Manipulation / Sabotage / Etikettenschwindel
- **R** epudiation - Abstreitbarkeit / Zurechenbarkeit
- **I** nformation Disclosure - Kopie von Geschäftsgeheimnissen / Identitätsdaten
- **D** enial-of-Service - Ressourcenverbrauch / Infrastruktur / Wartung
- **E** levation of Privilege - Rechteausweitung zum Zugang zu Ressourcen

BEDROHUNGSMODELLE

STRIDE (Microsoft)

- **S** poofing
- **T** ampering
- **R** epudiation
- **I** nformation Disclosure
- **D** enial-of-Service
- **E** levation of Privilege

UNIVERSITÄT BONN

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, Verdecktheit, Pseudonymität, Transparenz, Revisionsfähigkeit, Beherrschbarkeit, Kontingenz, Glaubhafte Abstreitbarkeit, Nicht-Abstreitbarkeit …

SCHUTZZIELE

CIA++

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Zurechenbarkeit

- Untergeordnete Schutzziele
  - Unverkettbarkeit, Nicht-Verfolgbarkeit, Verdecktheit, Pseudonymität, Transparenz, Revisionsfähigkeit, Beherrschbarkeit, Kontingenz, Glaubhafte Abstreitbarkeit, Nicht-Abstreitbarkeit …

!ACHTUNG!

Schutzziele können sich gegenseitig widersprechen!

Offensichtlich: Vertraulichkeit vs. Verfügbarkeit

UNIVERSITÄT BONN

SCHUTZZIELE - STRIDE

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) Zurechenbarkeit

UNIVERSITÄT BONN

INFORMATIONEN = DATEN

Unterschiedliche Daten

- Möglichkeiten zur Klassifikation?

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

Relevante Daten im Bereich Netzwerksicherheit?

UNIVERSITÄT BONN

ANGREIFER / ANGREIFERMODELLE

- Passive Angreifer
  - Mitlesen bewegter Daten (Eavesdropping)
  - Verbindungs-/Verkehrsdatenanalyse (Metadaten)

- Aktive Angreifer
  - Datenmanipulation (Man-in-the-Middle)
    - Transmit, Replay, Modify, Delete
  - Denial-of-Service

ANGREIFER (FORTS.)

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

ANGREIFER (FORTS.)

Cyberwar

- Akteure
  - Mitbewerber
  - Staatliche Akteure

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

MAßNAHMEN

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

Bewegte Daten

Bei stationären und lokalen Daten:
Zugriffskontrolle

UNIVERSITÄT BONN

MAßNAHMEN (FORTS.)

Fazit: Übergeordnete Schutzziele durch kryptografische Verfahren sicherstellen

- Hashsummen
- Signaturen
- Verschlüsselung
  - Symmetrisch
  - Asymmetrisch
  - Hybrid

- Public-Key-Kryptografie für bewegte Daten verwenden!

UNIVERSITÄT BONN

MAßNAHMEN (FORTS.)

Public-Key-Kryptografie

- Absicherung der Kommunikation
  - SSL/TLS
  - GnuPG
  - S/MIME
- Absicherung stationärer / lokaler Daten
  - Z.B. verschlüsselte Backups (wie https://www.duplicati.com)
- Standards: Public Key Cryptography Standards (PKCS)

Inhalt der nächsten Vorlesung

UNIVERSITÄT BONN

ZUSAMMENFASSUNG

- 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

UNIVERSITÄT BONN

ENDE

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 24. April 2023

Nächste Übung:

- Dienstag, 18. April 2023 – 16 Uhr
- Abgabe des Übungszettels 1 bis morgen – 16 Uhr