W4DSKI_207 - Grundlagen IT-Sicherheit und Datenschutz

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de, Raum 149B

Version: WDSKI23B

Modul

- das Modul hat 55 VL / 5 ECTS
- Workload: 150 Stunden
- Selbststudium: 95 Stunden
- Prüfung: Klausur mit einem Umfang von 120 Minuten

Inhalte gem. MHB

- Grundbegriffe der Kryptographie
- Einweg- und Hashfunktionen
- Kryptographische Verfahren
- Kryptoanalyse: Brute-Force, Wörterbücher, Seitenkanäle, Person-in-the-Middle
- Anonymisierung, Pseudonymisierung und Randomisierung
- Ausblick auf Auswirkung von Quantencomputern, Ansätze Post-Quantum Kryptographie
- Digitale Signaturen und Zertifikate
- Schlüsselmanagement und -austausch, Authentifikation
- Grundbegriffe der IT-Sicherheit
- Grundlagen der DSGVO, Privacy by Design
- Security-Audit
- Standards und Normen
- IT-Security Management
- Security By Design
- Risikomanagement, insbesondere unter dem Gesichtspunkt Data Science und Künstliche Intelligenz und deren Anwendungen
- Grundlagen der digitalen Forensik
- Analyse mit forensischen Tools (Sleuthkit, Autopsy, DFF, Filecarver)
- Netzwerksicherheit und Penetration Testing
- Beispielhafte Anwendungsbereiche im Kontext von Data Science und Machine Learning: Bedrohungsmanagement mit Mitteln des maschinellen Lernens, Erkennung von Ausreißern und verteilten Angriffen, Data Science in Cyber Security und Cyber Security in Data Science

Bemerkung

Wir können in 55 Stunden nicht alle dort gelisteten Inhalte besprechen. Wir werden nur einige ausgewählte Themen ausführlicher behandeln; ich werde jedoch versuchen zu den meisten Themen zumindest kurz was zu sagen.

Vorlesungsunterlagen

Links auf die Folien und Übungen finden Sie in Moodle und im Folgenden. Bitte laden Sie die Folien (insbesondere die PDFs) erst kurz vor der Vorlesung herunter, da die Vorlesungsunterlagen häufiger überarbeitet werden!

Die Passworte für die Lösungsvorschläge stelle ich in der Vorlesung bzw. nach dem Lösen im Moodle zur Verfügung.

- Maßgeblich ist die HTML Version der Folien.

  (Animationen und Lösungsvorschläge finden sich ggf. nur in den HTML Folien.)
- Bei Bedarf, können Sie die PDF Version der Folien nutzen, um Anmerkungen etc. zu machen.

Vorläufige geplante Inhalte

Achtung!

Die Reihenfolge ist vorläufig.

- Cybersicherheit
- Klassiche Sicherheitsprinzipien
- Klassische Verschlüsselungsverfahren
- Einführung in die Zahlentheorie
- BlockChiffre
- Einführung in "Endliche Körper"
- AES
- Operationsmodi von Blockchiffren
- Stromchiffre
- Public-Key Kryptographie
- Hashfunktionen
- Authentifizierte Verschlüsselung
- Passwortsicherheit
- Einführung in die Netzwerksicherheit
- TOR - The Onion Router
- Pentesting