Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

**Am Fachbereich 2 - Duales Studium Wirtschaft • Technik ist zum August 2024 folgender Lehrauftrag zu besetzen:**

# Modul WI3053 - Informationssicherheitsmanagement

Für den dualen Bachelor-Studiengang „Wirtschaftsinformatik“ ist im 5. Semester für einen Kurs mit etwa 35 Teilnehmenden im Rahmen des o. g. Moduls, die Lehrveranstaltung im Umfang von je 5 Semester-Wochen-Stunden, insgesamt 55 akademische Stunden, zu besetzen.

**Qualifikationsziele des Moduls:**

Die Studierenden verstehen das Management von IT-Sicherheit, d.h. die systematische Sicherstellung der Sicherheit von Systemen im Unternehmen sowie die wichtigsten Frameworks. Sie kennen den typischen Aufbau der IT-Sicherheits-Abteilungen in Unternehmen und verstehen, wie diese im Rahmen der Prozesse zusammenarbeiten.

Sie kennen die wichtigsten Prozesse, Technologien und Tools zur Detektion, Reaktion, und Prävention von IT-Sicherheits-Risiken mit dem Fokus auf Web- und Cloud-Applikationen. Sie verstehen, wie geeignete Maßnahmen frühzeitig in den Softwareentwicklungslebenszyklus integriert werden können, um DevSecOps zu erreichen. Die Studierenden können anhand von Fallbeispielen und Softwarearchitekturen die Bedrohungslage analysieren, Schwachstellen identifizieren und Maßnahmen zur Verbesserung des Sicherheitsniveaus der Systeme entwickeln.

**Inhalte des Moduls:**

- Grundlegende Frameworks für IT-Sicherheit (u.a. ISO 27001 ff., NIST SP 800-53, OWASP ASVS)
- Aufbau einer typischen IT Sicherheitsabteilung in Unternehmen (u.a. SOC, IAM, Product Security, Compliance) und deren Prozesse
- Product und Application Security Konzepte (u.a. Threat Modelling, Aspekte der Softwarearchitektur hinsichtlich Security)
- Organisation und Tooling eines Security Operations Center (SOC)
- Use Cases zum Design und der Bewertung von Architekturen für Web- und Cloud-Architekturen hinsichtlich Security
- Tooling und Techniken zur Detektion, Reaktion und Prävention von wichtigen Angriffen auf Web- und Cloud-Applikationen (z.B. WAFs, CDNs für DDoS prevention, nessus für scanning, cloudbasierte Technologien wie AWS Organizations, Cloud Trail, Security Hub, Shield, Detective, Certificate Manager, Cognito – statt AWS auch andere Cloudservices möglich)
- DevSecOps (u.a. statische und dynamische Code-Analysen für Security, Implementierung von Techniken in CI-CD pipelines zur Automatisierung bzw. shift left im software development lifecycle)
- Optional: Machine Learning für IT Security (u.a. Anwendungen Deep Learning zur Detektion von OWASP Automated Threats, AWS

**Prüfungsleistung:** Klausur (Die Bearbeitungszeit für eine Klausur beträgt max. 120 Minuten.)

Das Semester dauert vom **12.08.2024** bis zum **03.11.2024**. Die Terminplanung erfolgt tagesgenau, d.h. ein Eingehen auf individuelle Terminwünsche ist prinzipiell möglich. Die Vergütung beträgt 42,22 Euro je akademischer Stunde á 45 Minuten, zzgl. Aufwandsentschädigung für die Korrektur der Prüfungsleistungen.

Sie erhalten Unterstützung durch den Modulverantwortlichen (z.B. Materialien, Konzepte, Ansätze zur Durchführung von Übungen), können aber auch in der konkreten Ausgestaltung Ihrer Lehrveranstaltung variieren.

Es erwarten Sie interessierte Studierende mit Unternehmensbezug.

Bitte senden Sie Ihre Bewerbung per Email an die Assistentin des Fachleiters Tatjana Wache
Email: tatjana.wache@hwr-berlin.de.