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

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

Modul WI2033-IT-Sicherheit

Für den dualen Bachelor-Studiengang „Wirtschaftsinformatik“ ist im 3. Semester für einen oder zwei Kurse mit je etwa 35 Teilnehmenden im Rahmen des o. g. Moduls, die Lehrveranstaltung im Umfang von je 5 Semester-Wochen-Stunden, insgesamt 55 (110) akademische Stunden, zu besetzen.

Qualifikationsziele des Moduls:

Die Studierenden

- kennen die grundlegenden Konzepte für IT-Sicherheit
- haben ein Verständnis für die mathematischen (zahlentheoretischen) Zusammenhänge der Kryptographie und können diese auf Anforderungen zur Sicherstellung der Vertraulichkeit und Integrität von Daten anwenden
- verstehen das Vorgehen von Angreifern und kennen entsprechende Techniken und Technologien, um das Vorgehen von Angreifern nachzuvollziehen und können grundlegende Techniken selbst anwenden (Fokus: Web- und Cloud Security)
- kennen die wichtigsten Schwachstellen in Web-Applikationen, erkennen diese und können ableiten, wie man dagegen vorgeht
- kennen die Grundkonzepte und wichtigsten Services in Cloudumgebungen und können daraus Richtlinien für die Architektur von Software-Architekturen in Cloudumgebungen ableiten
- optional: kennen die wichtigsten Schwachstellen in eingebetteten Systemen, erkennen diese und können ableiten, wie man dagegen vorgeht

Inhalte des Moduls:

- Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität
- Grundlegende Konzepte: Threat, Vulnerability, Risk etc.
- Einführung in die Kryptografie inkl. zahlentheoretischer Grundlagen
- Konzepte der Authentifizierung und Sicherung der Integrität von Daten (u.a. kryptographische Hashes, Signatur-Schemata, OAuth 2.0 (als delegierte Autorisierung) und OpenID Connect für Authentifizierung, PKIs, PGP)
- Konzepte der Autorisierung (u.a. DAC, MAC, RBAC, ABAC, Bell-LaPadula)
- Anwendung von Konzepten der Authentifizierung und Kryptographie in wichtigen Netzwerkprotokollen (u.a. SSH, IPSec, VPN)
- Vorgehen Angreifer (Reconaissance, Exploration, Enumeration, Initial Access, Execution, Persistence, Privilege Escalation etc.), MITRE Attack Framework
- Web Application Threats, ihre Erkennung und Prävention (u.a. SQL-Injection, XSS, CSRF, SSRF)

- Überblick und Use Cases mit wichtigen Netzwerk- und Security Tools (u.a. Einführung KALI-Linux, nmap, netcat, metasploit framework), Anwendung in den verschiedenen Phasen des Angriffs
- Cloud Security (u.a. Aspekte der Softwarearchitektur für moderne Web-Applikationen in Cloud Umgebungen hinsichtlich Sicherheit, ggf. Fokus auf AWS, aber nicht zwingend)
- Optional: Embedded Systems Threats (u.a. Side Channel Attacks, Verbände zur Modellierung des Informationsflusses mit Security Annotationen)

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

Das Semester dauert vom **30.09.2024** bis zum **22.12.2024**. 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.