Vorlesungsbeschreibung Datenschutz und Sicherheit

Lernergebnisse

Das Modul befähigt die Studierenden, die Relevanz von personenbezogenen Daten im unternehmerischen Umfeld bewerten zu können. Sie sind in der Lage zu prüfen, ob ein IT-System in der geplanten Form eingesetzt werden darf oder nicht. Datenschutz ist sowohl für die Gestaltung als auch die Bewertung von Systemen relevant und soll von den Studierenden v.a. in der Praxis (Praktikum) angewandt werden.

Inhalte

Grundlagen des Datenschutzes und der Datensicherheit, EU Charta und DSGVO als Basis des deutschen und -internationalen DV-Rechts, Technologiekonzerne, staatliche Hoheit und Souveränität, Sicherheitsbehörden, Wirtschaftsspionage und Cyberkonflikte, Social Engineering und Data Mining

Technisch-organisatorische Grundlagen des Datenschutzes:

- Risikoanalysen
- ISO 27001, BSI-Grundschutzhandbuch (Struktur und Anwendung)
- Kryptographie und Verschlüsselungstechnologie
- Rechte der Betroffenen

Arbeitnehmerdatenschutz

Datenschutz und Telekommunikationsgesetz

Anwendungen des Datenschutzes und der Datensicherheit: Auswahl aus aktuellen Themen und relevanten (neuen) Technologien, wie bspw. Adresshandel, Scoring, Human Resources Gesundheitskarte und Datenschutz

IT-Sicherheit: Schädlinge (Trojaner, Root-Kits usw.) und deren Abwehr

Netzwerksicherheit (Firewalls, Spam-Filter usw.)

Zugangskontrollsysteme

PKI, Authentifizierung und Identitätsmanagement

Videüberwachung; Sicherheitsbehörden und Überwachung

Studien-/Prüfungsleistung

Es muss ein Projektreferat über ein bestimmtes datenschutzrelevantes Thema geschrieben (ca. 5 Seiten) und vorgestellt werden (Referat ca. 15 min). Die jeweiligen Themen der Referate der anderen Studierenden können als Aufgabe in der mündlichen Prüfung oder Klausur relevant sein. Die Note der Projektarbeit fließt in die Gesamtbewertung ein.

Credits

5 (150 h = 60 h Präsenz- und 90 h Eigenstudium)

Besonderes

Exemplarische Transferaufgaben:

- Technologie-und Datenschutz-Folgeabschätzung durchführen
- Schutzbedarfe feststellen und Maßnahmenkatalog erstellen
- Public Key Infrastruktur analysieren
- Awareness-und Schulungskonzepte entwickeln
- Anleitungen für sichere Software-Systemarchitektur erarbeiten

Alle öffnen Alle schließen