7 Grundlagen der IT-Sicherheit

Principles of IT Security

Semester	2	
Dauer (Semester)	einsemestrig	
Credit Points	5	
Pflicht/ Wahlpflicht	Pflicht	
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.	
Modulverantwortliche(r)	Prof. Dr. Claus Vielhauer, Technische Hochschule Brandenburg; Jeweils betreuender Professor/ betreuende Professorin	
Lerngebiet	IT-Sicherheit	
Teilnahmevoraussetzungen	Digitaler Selbstschutz, Informatik Grundlagen	
Lernziele nach Bloom	Formale, algorithmische, mathematische Kompetenzen	
	Wissen	Formale Beschreibung grundlegender Sicherheitsmodelle werden beherrscht.
	Verstehen	Grundlegender Prinzipien von Protokollen für Kryptographie, Authentifizierung und Netzwerkanalyse werden verstanden.
	Analyse-, Design- und Realisierungs-Kompetenzen	
	Wissen	Grundlegendes Wissen über wesentliche Sicherheitsprobleme in IT- und Medienanwendungen wird aufgebaut.
	Verstehen	Verständnis der grundlegenden rechtlicher Rahmenbedingungen im Bereich IT Sicherheit
	Analysieren	IT Systeme können systematisch in Bezug auf grundlegende Sicherheitsaspekte multilateral analysiert werden.
	Evaluieren, Bewerten	Grundlegende Methoden zur analytischen Vorgehensweisen bei der Schwachstellenanalyse können zur Bewertung der Bedrohung eingesetzt werden, sowohl für Fragestellungen der IT, als auch in anderen Bereichen wie beispielsweise der betrieblichen Organisationen.
	Technologische Kompetenzen	

	Wissen	Grundlegende Konzepte zur Verwaltung und Überprüfung von Identitäten in IT Systemen werden vermittelt und ausgewählte technische Ansätze vertieft.
	Verstehen	m Bereich der praktischen Sicherheit sind aktuelle Einsatzgebiete von Sicherheitswerkezugen vertraut.
	Anwenden	Anhand von konkreten Problemstellungen Lösung mit Sicherheitswerkzeugen herbeiführen, durch Anwendung ausgewählter praktischer Sicherheitswerkzeuge wie z.B. PGP oder Firewall.
	Fachübergreifende Kompetenzen	
	Wissen	Kenntnis der Prinzipien von Datenschutzrecht und Social Engineering.
	Verstehen	Wesentliche juristische Rahmenwerke können benannt, sowie deren Wirkungsweise auf die IT beschrieben werden.
	Methodenkompetenzen	
	Wissen	Grundsätzliche organisatorische Konzepte für die Entwicklung von Sicherheitsrichtlinien sind bekannt.
	Verstehen	Grundlagen von Sicherheitsmodellen und wesentliche Sicherheitsstandards können beschrieben und im Hinblick auf Anwendungsgebiete als auch der adressierten Sicherheitsaspekte eingeordnet werden.
	Anwenden	Sicherheitsrichtlinien können widergegeben und angewandt werden
	Synthetisieren	Befähigung, um künftig aktuelle Verfahren zu Erarbeitung und Umsetzung von Sicherheitskonzepten zu bestimmen und umzusetzen.
	Evaluieren, Bewerten	Grundlegende organisatorische Methoden zur Schutzbedarfsanaylse (z.B. BSI Grundschutz, Angriffsbäume) können zur Bewertung von Bedrohung und Schutzbedarf von IT Systemen eingesetzt werden.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme	

Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Web-Konferenz, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 120 h Webkonferenzteilnahme: ca. 26 h Präsenzteilnahme: ca. 4 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von erweiterten Übungsaufgaben
Prüfungsform	Klausur (120 min.)
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte

Lehrziel des Moduls IT-Sicherheit ist es, den Teilnehmer für die Problematik der Sicherheit in den Bereichen Datenerzeugung, -speicherung, -transfer und -verarbeitung mit seinen umfangreichen Facetten zu sensibilisieren und Kenntnisse über die Abwehr möglicher Angriffe zu vermitteln. Dabei hervorzuheben ist, dass dieses Studienmodul Sicherheitsbedrohungen und potentielle Schwachstellen motivieren und den Handlungsbedarf aufzeigen soll. Es soll die Fähigkeit erlernt werden, die Sicherheit von IT-Systemen zu überprüfen, einzuschätzen und gegebenenfalls Lösungen für auftretende Probleme zu entwickeln und umzusetzen. Dazu werden dem Studierenden Grundlagen der IT-Sicherheit nahe gebracht, aktuelle Sicherheitsstandards erläutert, technische und nicht-technische beziehungsweise organisatorische Maßnahmen zur Aufrechterhaltung der Sicherheit diskutiert und die Einhaltung beziehungsweise Anwendung rechtlicher Rahmenbedingungen dargelegt.

Lehreinheiten

1. Einführung und organisatorische Sicherheit
- Security versus Safety
- Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen
- Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken
- Sicherheitspolicies und Modelle
- Sicherheitsstandards
- Social Engineering

2. Datenschutz und Nicht-technische Datensicherheit
- EU Datenschutzverordnung, Bundes- und Landesdatenschutzgesetze
- Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Staatsvertrag für Rundfunk und Telemedien (RStV)
- Urheberrecht, Strafgesetzbuch
- IT Sicherheitsgesetz

3. Identity Management
- Grundlagen der Benutzerauthentifizierung
- Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc.
- Besitzbasierte Authentifizierung: Smartcards & RFID
- Einführung und organisatorische Sicherheit
- Multifaktorielle Authentifizierung
- Single-Sign-On Systeme
- Positionsbasierte Authentifizierung

4. Angewandte IT Sicherheit
- Einführung in die IT Forensik
- Einführung in die Mediensicherheit

5. Praktische IT Sicherheit
- Vorgehen bei Sicherheitskonzepten: BSI-Grundschutz
- Ausblick kryptographischer Schutz
- Ausblick Netzsicherheit