Modulbezeichnung	Informationssicherheit (Kopie vom Fri May 22 16:55:34 +0200 2020) (Kopie vom Fri May 22 17:00:49 +0200 2020)
Modulverantwortliche(r)	Prof. Dr. C. Bormann
Modulart	Pflicht/Wahl □ Wahlpflicht ⊠
Spezialisierungsbereich	Systemsoftware / Eingebettete Systeme
Dauer des Moduls	1 Semester
Kreditpunkte	6 CP
Arbeitsaufwand	Berechnung des Workloads Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h
Turnus des Moduls	i. d. R. angeboten alle 2 Semester
Voraussetzung für die Teilnahme	Keine Folgende Inhaltliche Voraussetzungen: Technische Informatik 2
Lehr- und Lernformen	Seminar □ Vorlesung ⊠ Tutorium ⊠ Praktikum □ Projekt □
Lernziele	 Grundkonzepte der Informationssicherheit kennen; Die gängigsten Sicherheitsprobleme in heutigen IT-Infrastrukturen und deren Ursachen kennen; Notwendigkeit für den Einsatz von Sicherheitstechnik erkennen; Grenzen der im Einsatz befindlichen Technologien einschätzen können; Verschiedene Bereiche von Sicherheitstechnik einordnen können; Modelle und Methoden zur systematischen Konstruktion sicherer Systeme kennen.
Lerninhalte	 Grundbegriffe der IT-Sicherheit, Bedrohungen und Sicherheitsprobleme: Vertraulichkeit, Integrität, Verfügbarkeit etc.; Viren, Würmer, Trojanische Pferde etc. Kryptografie (Symmetrisch, Asymmetrisch, Hash, PRF): DES, 3DES, AES; RSA, DSA; MD5, SHA1; TLS-PRF, PBKDF2 Mechanismen zur Authentisierung und Integritätsprüfung digitaler Signaturen, Zertifikate, PKI Zugriffskontrolle, Autorisierung, Rollen Sicherheitsprotokolle, z.B. Schlüsselaustausch Diffie-Hellman, TLS (SSL), Kerberos Probleme mit Protokollen, Angriffe (fehlende Bindung, Replay,) Netzsicherheit (Firewalls/IDS, VPN, Anwendungssicherheit) Sicherheit in Layer 2 (GSM, WLAN,) Software-Zertifizierung: Common Criteria Mobiler Code Smart Cards, Trusted Computing Platform Security Engineering Organisationelle Sicherheit; Security: The Business Case
Prüfungsformen	i.d.R. Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

Literatur	(deutschsprachig:) Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle; Oldenbourg 2009: 981 Seiten
	 (englischsprachig:) Ross Anderson: Security engineering: a guide to building dependable distributed systems; Wiley 2008; 1040 Seiten