25 IT-Sicherheit in der Energiewirtschaft	
Semester	6
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Partner-Hochschulen / Online-Bachelorstudiengang Regenerative Energien
Modulverantwortliche(r)	Prof. Dr. Dorina Gumm
Lerngebiet	Leit- und Steuerungstechnik
Teilnahmevoraussetzungen	Erfolgreicher Abschluss der Module Programmierung II und Intelligente Energienetze wird empfohlen
Lernergebnisse	Die Studierenden können • wesentliche Sicherheitskriterien in dezentralen Energieerzeugungs- und Verteilungssystemen erläutern und damit potenzielle Sicherheitsrisiken in dieser kritischen Infrastruktur identifizieren. • Sicherheitsrisiken bezüglich ihrer Auswirkungen einordnen. • die wesentlichen Angriffsziele unterscheiden und Schutzmechanismen benennen. • Konsequenzen bestimmter Systemdesigns auf IT-Sicherheit abschätzen. • Maßnahmen zur Reduzierung von Sicherheitsrisiken am Beispiel des eigenen Gefährdungspotentials durchführen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphase
Arbeitsaufwand	Selbststudium: ca. 145 h Präsenzteilnahme: ca. 3 h Prüfung: 120 Minuten (Präsenzteilnahme ist freiwillig)
Präsenzart	In Online-Konferenz möglich
Prüfungsform	Klausur (120 min.)
Literatur	Eckert, Claudia (2014): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 9. ed. Berlin/Boston: De Gruyter. Hadnagy, Christopher (2012): Die Kunst des Human Hacking. Heidelberg: mitp/bhv (mitp Professional).

	Kraft, Peter; Weyert, Andreas (2015): Network Hacking. 4. Auflage. Haar bei München: Franzis.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Grundlagen IT-Sicherheit auf Informations- und Systemebene; Sicherheitsanforderungen der Energiewirtschaft (u.a. Integrität, Authentizität, Verfügbarkeit); Relevanz für vernetzte Energiesysteme; Security vs. Safety; Risiko, Schwachstelle, Gefahr **Angriffsvektoren** Malwarearten; Angriffe auf verteilte Systeme; Angriffe auf Web-Ebene; Social Engineering **Schutzkonzepte** Authentifikation/Identity Management; Netzsicherheit; Kryptographie und Anonymisierung; Konzepte für sicheres Systemdesign (z.B. Sicherheitsstandards, Sicherheitsmodelle, BSI-Grundschutz, Angriffsbaum/Analyse); Digitale Selbstverteidigung (z.B. Verschlüsselte Kommunikation, Datensparsamkeit, sicheres Surfen) **Gesellschaftliche und sicherheitspolitische Fragestellungen**