FACHHOCHSCHULE ERFURT UNIVERSITY OF APPLIED SCIENCES
Angewandte Informatik

Modulbeschreibung

Fakultät Gebäudetechnik und Informatik — gültig ab WS 2010/11

Modul-Nr.: BA-AI-1150	**Modulname:** IT-Sicherheit (ITS)	**Niveaustufe:** Bachelor	**Empfohlenes Semester:** BA5
Studiengang: Angewandte Informatik	**Status:** Pflicht alle	**Verantwortliche/r:** Prof. Dr.-Ing. Gunar Schorcht	**Dozenten:** Prof. Dr.-Ing. Gunar Schorcht
Voraussetzung für die Teilnahme an diesem Modul/erforderliche Kenntnisse: Netze bzw. entsprechende Kenntnisse laut Modulbeschreibung		**Dieses Modul ist Voraussetzung für:**	

Kompetenz- und Lernziele:

- Studierende erwerben ein grundlegendes Verständnis der Risiken und Bedrohungen im Zusammenhang mit dem Betrieb von IT-Systemen, insbesondere in vernetzten Umgebungen.
- Sie kennen die verschiedenen Dimensionen der IT-Sicherheit.
- Sie lernen grundlegende Verfahren zur Sicherung von IT-Infrastrukturen und Daten kennen und zu bewerten.
- Sie sind in der Lage, grundlegende Maßnahmen zur Sicherung von IT-Infrastrukturen und Daten zu wählen und anzuwenden.
- Sie können bei Eintritt von Vorkommnissen geeignet reagieren.

Lehrinhalte:

- Grundbegriffe
- Bedrohungen
- Kryptographische Grundlagen
- Schlüsselmanagement
- Authentifizierung
- Zugriffskontrolle
- Sicherheit in Netzen
- Maßnahmen
- IT-Grundschutz

Literatur/Vorlesungsunterlagen: siehe Beschreibung der Teilmodule

Art der Lehrveranstaltung: Vorlesung mit integrierten Übungsanteilen	**Workload:** siehe Beschreibung der Einzelveranstaltung	**Leistungsnachweise:** siehe Beschreibung der Einzelveranstaltung
		Zusammensetzung der Modulnote: Note der Einzelveranstaltung
		Voraussetzungen für die Vergabe von Credits: Modulnote muss mindestens 4,0 sein
Bewertungstyp: dezimal	**Dauer des Moduls:** 1 Semester	**Zulassungsvoraussetzungen für die Modulprüfung/ Teilprüfung:** siehe Beschreibung der Einzelveranstaltung
Credits (ECTS): gesamt: 2 CP	**Häufigkeit des Angebots/ Verwendbarkeit des Moduls:** • Teilmodul ITS im SS	**Veranstaltungssprache:** deutsch

Modulbeschreibung
Fakultät Gebäudetechnik und Informatik gültig ab WS 2010/11

2 CP in Teilmodul ITS	• kann auch in anderen Studiengängen eingesetzt werden, in denen Kenntnisse über IT-Sicherheit benötigt werden	
Veranstaltungsort: Hörsaal	**Präsenzzeiten:** 2 SWS	**Bemerkungen:** Blockveranstaltung

Modulbeschreibung

Fakultät Gebäudetechnik und Informatik gültig ab WS 2010/11

Beschreibung der Einzelveranstaltungen des Moduls

Veranstaltungstitel:	IT-Sicherheit (ITS)
Dozent/in:	Prof. Dr.-Ing. Gunar Schorcht
Zuordnung zu Modul:	BA-AI-1150
Studiensemester:	5
Veranstaltungsform:	Vorlesung mit integrierten Übungsanteilen
Max. Teilnehmerzahl:	keine Begrenzung
Anmeldung:	keine
Kreditpunkte:	2
Präsenzzeiten:	2 SWS (2 Stunden wöchentlich bei 15 Vorlesungswochen, 2 SWS Vorlesung mit integrierten Übungsanteilen)
Sprache:	Deutsch
Leistungsnachweise/ Bedingung für die Vergabe von Credits:	studienbegleitende Prüfungsleistung (SPL) Klausur am Ende der Blockveranstaltung Klausur muss mit mindestens 4,0 bewertet sein
Zulassungsvoraussetzungen für die Teilprüfung:	Übungsaufgaben mit mindestens 4.0 bewertet
Wiederholungsprüfung:	Wiederholung der nicht bestandenen Prüfungsleistung
Workload:	30 Stunden Kontaktveranstaltung 20 Stunden Nachbereitung, Literatur und Übungen 10 Stunden Prüfungsvorbereitung
Inhalte:	1. Grundbegriffe 1. Bedrohungen − Viren, Würmer, Trojanische Pferde, Mobile Code − Buffer-Overflows − TCP/IP-Probleme (Sniffen, Spoofen, DoS) 2. Kryptographische Grundlagen − Symmetrische und Asymmetrische Verfahren − Kryptographische Prüfwerte − Digitale Signaturen − Zufallszahlen 3. Schlüsselmanagement − Schlüsselaustausch Diffie-Hellman − Public Key Infrastructure − Zertifikate 4. Authentifizierung − durch Wissen (OTP, Challenge-Response, ...) − durch Besitz (Smart-Card, biometrische Verfahren) − in verteilte Systemen (Kerberos, RADIUS) 5. Zugriffskontrolle

	– Zugriffskontrollmatrix – Rollenbasierte Zugriffskontrolle (RBAC) 6. Sicherheit in Netzen – Tunneling PPTP, L2F, L2TP – IPsec-Sicherheitsarchitektur (Einführung) – Transportschicht SSL, TLS 7. Maßnahmen – Firewalls und Proxies (Einführung) – Monitoring (Intrusion Detection) – Email-Sicherung (Verschlüsselung, Signierung, SMTP-Server) – Notfallplan 8. IT-Grundschutz
Veranstaltungsunterlagen/ Literatur	• Eckert, Claudia: IT-Sicherheit: Konzepte - Verfahren - Protokolle, 3. überarb. und erw. Aufl. München [u.a.]: Oldenbourg, 2004 • Schäfer, Günter: Netzsicherheit: Algorithmische Grundlagen und Protokolle. Heidelberg: dpunkt-Verl., 2003 • Kaufman, Charlie; Perlman, Radia; Speciner, Mike: Network Security: Private Communication in a Public World, 2. ed. Upper Saddle River, NJ: Prentice Hall PTR, 2002 • Gerloni, Helmar: Praxisbuch Sicherheit für Linux-Server und -Netze. München [u.a.]: Hanser, 2004 • Schwenk, Jörg: Sicherheit und Kryptographie im Internet: von sicherer E-Mail bis zu IP-Verschlüsselung, 2., erw. und verb. Aufl. Wiesbaden: Vieweg, 2005ISBN: 3-8348-0042-2 • Scheiderer, Jürgen: Mitp-Trainingsbuch SuSE Linux Sicherheit, 2. Aufl., aktualisierte Neuaufl. Bonn: mitp, 2004 • RRZN Universität Hannover: Netzwerke - Sicherheit, 2. Auflage. http://www.rrzn.uni-hannover.de/buecher.html • Plötner, Johannes; Wendzel, Steffen: Praxisbuch Netzwerk-Sicherheit. Bonn: Galileo Press, 2005