

Modulcode (1.)	Modulbezeichnung (2.)	Zuordnung (3.)
BAI7010	IT-Sicherheit (ITS)	
	Studiengang (4.)	Bachelor Angewandte Informatik/ Bachelor Angewandte Informatik DUAL
	Fakultät (5.)	Gebäudetechnik und Informatik

Modulverantwortlich (6.)	Prof. Dr.-Ing. Gunar Schorcht
Modulart (7.)	Pflicht
Angebotshäufigkeit (8.)	WS
Regelbelegung / Empf. Semester (9.)	BA7
Credits (ECTS) (10.)	5 CP
Leistungsnachweis (11.)	PL (N)
Unterrichtssprache (12.)	Deutsch
Voraussetzungen für dieses Modul (13.)	BAI3040: Netze 1 BAI6030: Netze 2
Modul ist Voraussetzung für (14.)	-
Moduldauer (15.)	1 Semester
Notwendige Anmeldung (16.)	-
Verwendbarkeit des Moduls (17.)	-

Lehrveranstaltung (18.)	Dozent/in (19.)	Art (20.)	Teilnehmer (maximal) (21.)	Anzahl Gruppen (22.)	SWS (23.)	Workload	
						Präsenz (24.)	Selbststudium (25.)
1 IT-Sicherheit	Schorcht	V	50	1	3	45	30
2 IT-Sicherheit	Schorcht	PÜ	25	2	1	15	35
Summe					4	60	65
Workload für das Modul					(26.)	125	

Qualifikationsziele	<p>Die Studierenden ...</p> <ul style="list-style-type: none"> • verstehen die Risiken und Bedrohungen im Zusammenhang mit dem Betrieb von IT-Infrastrukturen, insbesondere in vernetzten Umgebungen. • kennen grundlegende Verfahren zur Sicherung von IT-Infrastrukturen und können diese bewerten. • kennen Methoden zur Überprüfung der Sicherheit von IT-Infrastrukturen sowie der Wirksamkeit von Maßnahmen zur Sicherung von IT-Infrastrukturen. • können grundlegende Maßnahmen zur Sicherung von IT-Infrastrukturen wählen und anwenden. • können mit geeigneten Methoden die Sicherheit von IT-Infrastrukturen sowie die Wirksamkeit von Maßnahmen zur Sicherung von IT-Infrastrukturen anwenden. • können bei Eintritt von Vorkommnissen geeignet reagieren.
Inhalte	<ul style="list-style-type: none"> • Grundbegriffe: IT-Sicherheit, Schutzziele, Sicherheitsarchitektur • Bedrohungen: Viren, Würmer, Trojanische Pferde, Mobile Code, Buffer-Overflows, TCP/IP-Probleme (Sniffen, Spoofen, DoS) • Kryptographische Grundlagen: Symmetrische und Asymmetrische Verfahren, Kryptographische Prüfwerte, Digitale Signaturen, Zufallszahlen • Schlüsselmanagement: Schlüsselaustausch Diffie-Hellman, Public Key Infrastructure, Zertifikate • Authentifizierung: durch Wissen (OTP, Challenge-Response, ...), durch Besitz (Smart-Card, biometrische Verfahren), in verteilte Systemen (Kerberos, RADIUS) • Zugriffskontrolle: Zugriffskontrollmatrix, Rollenbasierte Zugriffskontrolle (RBAC) • Sicherheit in Netzen: <ul style="list-style-type: none"> • IPsec-Sicherheitsarchitektur • Trasportschicht TLS/SSL • WLAN Security • VPNs: IPsec, OpenVPN, Wireguard • Firewalls und Proxies • Monitoring und Intrusion Detection Systems • Email-Sicherung: Client (Verschlüsselung, Signierung), SMTP-Server (Virenfilter, SPAM-Filter, RBLs, SPF, DKIM, DMARC) • Sicherung von Web-Servern • Penetration Testing • Notfallplan • Informationssicherheitsmanagementsysteme (Sicherheitsprozess, Schutzbedarf, Bedrohungs- und Risikoanalyse, ISO27001 sowie BSI-Grundschutz)
Vorleistungen und Modulprüfung	<p>Vorleistungen:</p> <ul style="list-style-type: none"> • Erfolgreiche Teilnahme an den praktischen Übungen <p>Modulprüfung:</p> <ul style="list-style-type: none"> • 100 % Klausur über 90 min im Prüfungszeitraum

- Eckert, Claudia: *IT-Sicherheit: Konzepte - Verfahren – Protokolle*, 10. Auflage. Berlin, Boston: De Gruyter Oldenbourg, 2018.
ISBN 978-3-11-055158-7
- Schäfer, Günter: *Netzicherheit - Grundlagen & Protokolle - Mobile & drahtlose Kommunikation - Schutz von Kommunikationsinfrastrukturen*, 2. aktual. und erw. Auflage. Heidelberg: dpunkt-Verlag., 2014
ISBN 978-3-86490-115-7
- Kaufman, Charlie; Perlman, Radia; Speciner, Mike; Perner, Ray: *Network Security: Private Communication in a Public World*, 3rd ed. Addison-Wesley Professional, 2020
ISBN 978-0-13-664360-9
- Gerloni, Helmar: *Praxisbuch Sicherheit für Linux-Server und -Netze*. München [u.a.]: Hanser, 2004
ISBN 978-3-446-22626-5
- Schwenk, Jörg: *Sicherheit und Kryptographie im Internet: von sicherer E-Mail bis zu IP-Verschlüsselung*, 5., erw. und aktual. Auflage Wiesbaden: Springer Vieweg, 2005
ISBN 978-3-658-29259-1
- Dehn, Siegmund: *Netzwerke Sicherheit*, 11. Ausgabe. RRZN-Handbuch Nachdruck des Herdt-Verlages, 2019
ISBN 978-3-86249-848-2
<https://www.luis.uni-hannover.de/de/services/kurse-beratung-und-support/handbuecher/it-handbuecher-und-ebooks/details/manuals/nwsi>
- Plötner, Johannes; Wendzel, Steffen: *Praxisbuch Netzwerk-Sicherheit*, 2. aktual. und erw. Auflage. Bonn: Galileo Press, 2007
ISBN 978-3-89842-828-6
- Kofler, Michael et. al.: *Hacking & Security Das umfassende Handbuch*, 2. Auflage. Bonn: Rheinwerk Computing, 2020
ISBN 978-3-8362-7191-2
- Schäfers, Tim Philipp, Walde, Rico: *WLAN Hacking*. München: Franzis Verlag, 2018
ISBN 978-3-645-60523-6
- Kraft, Peter: *Network Hacking*, 5. Auflage. München: Franzis Verlag, 2017
ISBN 978-3-645-60531-1