

IT Security und Datensicherheit

Modul: IT Security und Datensicherheit	
Studiengang: Bibliotheksinformatik	Abschluss: Master
Modulverantwortliche/r: Dr. Frank Seeliger & Prof. Dr. iur. Carsten Kunkel	

Semester: 3	Dauer: 1	
SWS: 30	davon V/Ü/L/P: 15/15/0/0	CP nach ECTS: 5.0
Art der Lehrveranstaltung: Pflicht	Sprache: Deutsch	Stand vom: 2017-03-07
Pflicht Voraussetzungen: Grundlagen der Funktionsweise des Internet und rechtlichen Rahmenbedingungen im Umgang mit Daten		
Empfohlene Voraussetzungen: Bewußtsein für sichere Datenübertragung im Web, Erfahrung im Umgang mit personenbezogene Fremddaten		
Pauschale Anrechnung von:		
Besondere Regelungen: Motto nach Joachim Ringelnatz: Sicher ist, dass nichts sicher ist. Selbst das nicht.		

Aufschlüsselung des Workload	Stunden:
Präsenz:	30.0
Vor- und Nachbereitung:	40.0
Projektarbeit:	55.0
Prüfung:	2.0
Gesamt:	127

IT Security und Datensicherheit

Lernziele	Anteil
Fachkompetenzen	
<p>Kenntnisse/Wissen</p> <ul style="list-style-type: none"> • Die Studierenden kennen die Grundzüge des Urheber- und Datenschutzrechts. • Die Studierenden kennen die rechtlichen Grundlagen des Bibliothekswesens einschließlich des Vertrags- und Benutzungsrechts. • Die Studierenden lernen sicherheitsrelevantes Verhalten im realen wie virtuellen Leben kritisch zu reflektieren. • Die Studierenden kennen die häufigsten Angriffsszenarien im Internet auf die Sicherheitsstrukturen eine Einrichtung. • Die Studierenden lernen grundlegende Schutzmechanismen der IT-security kennen. • Die Studierenden kennen grundlegende Verfahren des verschlüsselten Informationsaustauschs im Internet inkl. der Verwendung von Sicherheitszertifikaten. • Die Studierenden wissen um die mathematischen Grundlagen der asymmetrischen Verschlüsselung. 	40%
<p>Fertigkeiten</p> <ul style="list-style-type: none"> • Die Studierenden können Infrastrukturen in einer Informationseinrichtung auf sicherheitskritische Aspekte in technischer und rechtlicher Hinsicht analysieren und geeignete Schutzmaßnahmen treffen. • Die Studierenden können Verschlüsselungsalgorithmen anwenden. • Die Studierenden können eine Public-Key-Infrastruktur aufbauen. • Die Studierenden erlernen Techniken zur Überprüfung der Übereinstimmung von physischer mit virtueller/digitaler Identität. 	40%

IT Security und Datensicherheit

Personale Kompetenzen	
Soziale Kompetenz <ul style="list-style-type: none"> • Die Studierenden lernen, in kleinen Teams komplexe Fragestellungen aus dem Bereich Sicherheit und Bibliotheksrecht ergebnisorientiert zu bearbeiten. • Die Studierenden üben den Wissenstransfer auf dem informellen und formalen Markt des Informationsaustauschs. • Die Studierenden praktizieren Interessensgruppen und vernetzen sich aufgabenspezifisch. • Die Studierende erlernen kritisch Fachvorträge zu Sicherheitsvorkehrungen an Einrichtungen zu hinterfragen. 	20%
Selbstständigkeit <ul style="list-style-type: none"> • Die Studierenden sind in der Lage, selbständig für eine spezifische Aufgabenstellung im Bereich IT-Infrastruktur die geltenden rechtlichen Rahmenbedingungen zu eruieren und anzuwenden, und ebenfalls die unter dem Gesichtspunkt der IT-Sicherheit notwendigen Maßnahmen umzusetzen. 	

Inhalt:
<ol style="list-style-type: none"> 1. Grundlagen des Rechts und Rechtsformen der Bibliotheken und Informationseinrichtungen 2. Vertrags- und Benutzungsrecht 3. Grundzüge des Urheberrechts 4. Grundzüge des Datenschutzrechts 5. IT-Compliance und Sicherheitsrichtlinien in Behörden/Institutionen 6. Bedrohungsanalyse zu Internet und Bibliotheksdienstleistungen 7. Schutzziele 8. IT-Grundschutz nach BSI und Sicherheitskonzept 9. Sichere Kommunikation im Internet und Cybersicherheit 10. Verschlüsselungsverfahren 11. Authentifizierungsverfahren

IT Security und Datensicherheit

Prüfungsform:

Projektarbeit (25%)
Schriftliche Arbeit (25%)
Präsentation (25%)
Mündliche Prüfung (25%)

Pflichtliteratur:

Eckert, C. (2014). *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. De Gruyter Oldenbourg.
Ertel, W. (2012). *Angewandte Kryptographie*. Carl Hanser Verlag GmbH & Co. KG.
Meinel, C. & Sack, H. (2014). *Sicherheit und Vertrauen im Internet*. Wiesbaden: Springer Vieweg.
Schmeh, K. (2016). *Kryptografie: Verfahren, Protokolle, Infrastrukturen (iX-Edition)*. dpunkt.verlag GmbH.
Schwenk, J. (2010). *Sicherheit und Kryptographie im Internet*. Wiesbaden: Vieweg + Teubner.

Empfohlene Literatur:

Grünendahl, R. & Steinbacher, A. & Will, P. (2012). *Das IT-Gesetz: Compliance in der IT-Sicherheit*. Wiesbaden: Vieweg + Teubner.
Falk, M. (2012). *IT-Compliance in der Corporate Governance*. Wiesbaden: Springer Gabler.
Sowa, A. (2015). *IT-Revision, IT-Audit und IT-Compliance*. Wiesbaden: Springer Fachmedien Wiesbaden.
Freiermuth, K. (2014). *Einführung in die Kryptologie*. Wiesbaden: Springer Fachmedien.
Paar, C. (2016). *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender (eXamen.press)*. Springer Vieweg.