

## Studiengang Informatik

### Studienschwerpunkt „IT SECURITY“

Die Vernetzung von Informationssystemen und ihr Stellenwert im Unternehmen werden jedes Jahr größer. Immer mehr Prozesse und Daten sind digitalisiert. Funktionsausfälle in der IT bringen häufig die gesamte Firma zum Stillstand.

Kriminelle machen sich diese Tatsache zunutze, um Daten zu stehlen, Systemausfälle zu provozieren und mit Ransomware und ähnlichen Mitteln Lösegelder zu erpressen. Die finanziellen und Reputationsrisiken für betroffene Firmen sind erheblich und nehmen jedes Jahr zu.

Daher ist es notwendig, Systeme und Netzwerke adäquat zu schützen. Dafür benötigen Unternehmen Fachkräfte in der IT Security, die am Markt allerdings Mangelware sind.

Deshalb soll an der DHBW Stuttgart ein Studienschwerpunkt eingerichtet werden, der den Bedarfen der Partnerunternehmen der DHBW gerecht wird. Hierzu gehören Informatik-nahe Themen wie sichere Softwareentwicklung, Administration von IT-Systemen und -Netzwerken, und Datensicherheit. Hinzu kommen auch organisatorische, rechtliche und soziale Aspekte der IT-Sicherheit. Damit ein ganzheitlicher Schutz möglich wird, muss ein Unternehmen all diese Aspekte komplett betrachten, um gegen verschiedenartige Angriffe bestmöglich gerüstet zu sein.

Es werden ab 2023 voraussichtlich sechs parallele Kursgruppen im Studiengang Informatik angeboten. Einer davon wird nun auf den Schwerpunkt „IT Security“ umgestellt, die übrigen verbleiben im etablierten Curriculum der Informatik. Je nach Interesse können mittelfristig weitere Kurse umgestellt werden. Die Zuordnung zu den Kursgruppen für den Jahrgang 2023 erfolgt vor Studienbeginn vom ersten Semester an auf Meldung der Unternehmen.

### Bedarf und Ausrichtung

Der große Bedarf der Unternehmen bezüglich IT-Sicherheit ist der DHBW Stuttgart bereits einige Zeit bekannt. Einer immer größeren Bedrohungslage steht ein gravierender Mangel an Fachkräften gegenüber, der die Sicherheit von IT-Systemen, Daten und Netzwerken und damit von Firmen und Bürgerinnen und Bürgern gefährdet. Am Standort Stuttgart sollen die Partnerunternehmen in die Gestaltung des Studienschwerpunktes einbezogen werden, so dass dieser bedarfsgerecht ausgerichtet wird.

## Integration in aktuelle Studienpläne

Der Studiengang Informatik wurde in der letzten Akkreditierung ohne Studienrichtung angelegt. Die dadurch vorhandenen lokalen Profilmodule (Wahlmodule) werden für die Festlegung eines Studienschwerpunkts genutzt. Im Folgenden werden der aktuelle Plan und die geplanten Anpassungen im Studienschwerpunkt dargelegt.

Der Studienschwerpunkt IT Security wird nach dem folgenden Schema angepasst. Es ergibt sich keine Änderung der Module in den ersten beiden Studienjahren, so dass es möglich ist, die Studierenden der Informatik und des speziellen Schwerpunkts in diesen Jahren gemeinsam zu unterrichten. Das 3. Studienjahr unterscheidet sich dann deutlich von dem Studiengang ohne Schwerpunktbildung.

### Aktueller Studienplan Informatik

1. Studienjahr (keine Änderung)			
Modulnummer	Modulname	Typ	ECTS
T3INF1001	Mathematik I	Kernmodul	8
T3INF1002	Theoretische Informatik I	Kernmodul	5
T3INF1003	Theoretische Informatik II	Kernmodul	5
T3INF1004	Programmieren	Kernmodul	9
T3INF1005	Schlüsselqualifikationen I	Kernmodul	5
T3INF1006	Technische Informatik I	Kernmodul	5
T3_1000	Praxis I	Kernmodul	20
T3INF4101	Webengineering I	Lokales Profilmodul	3
T3INF4103	Anwendungsprojekt Informatik	Lokales Profilmodul	5
T3INF9011	Schlüsselqualifikationen II	Lokales Profilmodul	5

  

2. Studienjahr (keine Änderung)			
Modulnummer	Modulname	Typ	ECTS
T3INF2001	Mathematik II	Kernmodul	6
T3INF2002	Theoretische Informatik III	Kernmodul	6
T3INF2003	Software Engineering I	Kernmodul	9
T3INF2004	Datenbanken I	Kernmodul	6
T3INF2005	Technische Informatik II	Kernmodul	8
T3_2000	Praxis II	Kernmodul	20
T3INF4201	Kommunikations- und Netztechnik I	Kernmodul	5
T3INF4221	Einsatz von Webtechnologien	Lokales Profilmodul	5
T3INF4901	Wahlmodul Informatik (STG Jahr 2)	Lokales Profilmodul	5

**3. Studienjahr (alt)**

<b>Modulnummer</b>	<b>Modulname</b>	<b>Typ</b>	<b>ECTS</b>
T3INF3001	Software Engineering II	Kernmodul	5
T3_3000	Praxis III	Kernmodul	8
T3_3201	Große Studienarbeit	Kernmodul	10
T3INF3002	IT Sicherheit	Kernmodul	5
T3INF4304	Datenbanken II	Lokales Profilmodul	5
T3INF9100	Data Science	Lokales Profilmodul	5
T3INF9101	Künstliche Intelligenz und Maschinelles Lernen	Lokales Profilmodul	5
T3INF9103	Mensch-Maschine-Interaktion	Lokales Profilmodul	5
T3INF4902	Wahlmodul Informatik	Lokales Profilmodul	5
T3INF9104	Big Data Architectures	Lokales Profilmodul	5
T3_3300	Bachelorarbeit	Kernmodul	12

**Studienplan im Schwerpunkt IT Security****3. Studienjahr (neu - mit Schwerpunkt IT Security)**

<b>Modulnummer</b>	<b>Modulname</b>	<b>Typ</b>	<b>ECTS</b>
T3INF3001	Software Engineering II	Kernmodul	5
T3_3000	Praxis III	Kernmodul	8
T3_3201	Große Studienarbeit	Kernmodul	10
T3INF3002	IT Sicherheit	Kernmodul	5
T3INF4304	Datenbanken II	Lokales Profilmodul	5
T3INF4300	Network Security	Lokales Profilmodul	5
T3INF4301	Security by Design	Lokales Profilmodul	5
T3INF4375	Data Security	Lokales Profilmodul	5
T3INF4902	Wahlmodul Informatik	Lokales Profilmodul	5
T3INF4113	Methodenkompetenz in der IT Sicherheit	Lokales Profilmodul	5
T3_3300	Bachelorarbeit	Kernmodul	12

## Ausprägung des Studienschwerpunkts

Der Studienschwerpunkt IT Security baut auf einen großen Teil an Grundlagenmodulen auf, die bereits im aktuellen Curriculum sind. Beispiele hierfür sind Software oder Web Engineering. Auch der Wahlmodulbereich wird ausgebaut und wird verstärkt IT-Sicherheitsthemen anbieten. Diese Wahlmodule sind jedoch nicht nur für den Schwerpunkt wählbar, sondern für den gesamten Studiengang Informatik. Das bestehende Kernmodul „IT Sicherheit“ dient als Grundlagenvorlesung für den Studienschwerpunkt. Aufbauend auf dieser Basis werden durch folgenden Module Schwerpunkte im neuen Studienschwerpunkt IT Sicherheit gesetzt:

### Security by Design

Dieses Modul widmet sich der Entwicklung sicherer Software. Behandelt wird der gesamte Software-Lebenszyklus, von Spezifikation und Architektur über Implementierung und Test bis hin zu Rollout und Wartung.

### Network Security

Die steigende Vernetzung, technologische Trends wie Cloud Computing, IoT und Microservices erhöhen die Komplexität von Firmennetzwerken. Gleichzeitig nehmen Angriffe an Anzahl, Komplexität und Schadenspotenzial jedes Jahr zu. Dieses Modul vermittelt praktisch, wie Unternehmensnetzwerke vor Angriffen geschützt werden können. Dazu wird neben den theoretischen Grundlagen auch die Verteidigungs- und Angriffsperspektive eingenommen, und für Sicherheitsübungen wie Pentests genutzt.

### Data Security

Daten nehmen heutzutage eine zentrale Position im Geschäftsmodell vieler Firmen ein und werden zunehmend zum lukrativen Angriffsziel, beispielsweise durch Ransomware. Neben technischen Maßnahmen zum Datenschutz wie Verschlüsselung, Authentifizierung und Datensicherung beinhaltet dieses Modul organisatorische, rechtliche und ethische Aspekte des Datenschutzes.

### Methodenkompetenz in der IT Security

IT-Sicherheit lässt sich nicht allein mit technischen Maßnahmen erreichen. Dieses Modul behandelt methodische, organisatorische, soziale und rechtliche Aspekte der Sicherheit. Die Studierenden lernen Methoden, Prozesse und organisatorische Best Practices, erlangen soziale und personale Kompetenz im Umgang mit IT-Sicherheit, und kennen wichtige Normen und Gesetze. Im Seminar untersuchen die Studierenden verschiedene Szenarien aus Fallstudien und lernen so, bei Angriffen und Sicherheitsverletzungen auf Produkte und Unternehmen angemessen zu reagieren.

## Umsetzung im Studienbetrieb

Das Studienzentrum Informatik plant die Einführung des Studienschwerpunkts in Absprache mit den Partnerunternehmen ab 2023. Es sollen dadurch keine weiteren Kurssäulen eröffnet werden, d.h. es ist nicht beabsichtigt, die Kapazität des Studienzentrums kurzfristig aus diesem Anlass zu erweitern. Nach aktuellen Schätzungen werden eine oder zwei von den mittelfristig sechs angebotenen Kursgruppen der Informatik den Studienschwerpunkt IT Security übernehmen.

## Network Security (T3INF4300)

### Network Security

#### FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
T3INF4300	3. Studienjahr	1	Prof. Dr. Andreas Judt	Deutsch

#### EINGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung, Übung, Labor	Lehrvortrag, Diskussion, Gruppenarbeit

#### EINGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Programmwurf	Siehe Pruefungsordnung	ja

#### WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	60	90	5

#### QUALIFIKATIONSZIELE UND KOMPETENZEN

##### FACHKOMPETENZ

Die Studierenden kennen Verfahren zu Sicherung von Unternehmensnetzwerken und können aktuelle Technolgien kompetent einsetzen.

##### METHODENKOMPETENZ

Die Studierenden können qualifiziert Verfahrung zur Netzwerksicherheit auf die Aufgaben des Unternehmens anwenden.

##### PERSONALE UND SOZIALE KOMPETENZ

-

##### ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden haben ein Verständnis für Netzwerksicherheit in Unternehmen entwickelt und können ihr Wissen in die Umsetzung kompetent einbringen.

#### LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Sichere Unternehmensnetze	36	39
Perimeterschutz, z.B. Firewall, IDS, IPS, Sandboxing Security Information and Event Management (SIEM) Systeme Mail- und andere Gateways SIEM Technology im Netzwerk Verwaltung von Zertifizierungsstellen NAC, Authentifizierungstechnologien Malware, Viren, Trojaner, Spyware Hochverfügbarkeit, Clustering, Hardening Distributed Denial of Service (DDoS) Angriffe Next Generation Firewalls Anwendung von Kryptographie auf Netzwerke, Fallstricke IoT Security		
Labor Netzwerksicherheit	24	51
Praktische Anwendung sicherer Unternehmensnetzwerke		

## BESONDERHEITEN

---

-

## VORAUSSETZUNGEN

---

-

## LITERATUR

---

- Michael Collins: Network Security Through Data Analysis: From Data to Action, O'Reilly UK Ltd.; Auflage: 2nd edition (2017)  
Firewalls for Dummies: <http://www.bradreese.com/blog/firewalls-for-dummies.pdf>  
Andrew S. Tanenbaum et.al.: Computer Networks, Pearson Education Limited, 5 Auflage, 2013  
James Kurose et.al.: Computer Networking: a Top-Down-Approach, Prentice Hall, 7. Auflage, 2016  
Charlie Kaufman et.al.: Network Security, Radia Perlman Series in Computer Networking and Security, 2. Auflage, 2002  
William Stallings: Network Security Essentials: Applications and Standards, Pearson Education Limited, 6. Auflage, 2016  
Levente Buttyan: Security and Cooperation in Wireless Networks, Cambridge University Press, 2007  
William Stallings et.al.: Computer Security: Principles and Practice, Prentice Hall, 3. Auflage, 2014  
Matt Bishop: Computer Security: Art and Science, Pearson Education, 2. Auflage, 2017  
Johannes Buchmann: Einführung in die Kryptographie, Springer Spektrum, 6. Auflage, 2016  
Alfred Menezes et.al.: Handbook of Applied Cryptography, CRC Press, 1996  
Jonathan Katz et.al.: Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall/CRC, 2007

## Security by Design (T3INF4301)

### Security by Design

#### FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
T3INF4301	3. Studienjahr	1	Prof. Dr. Andreas Judt	Deutsch

#### EINGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung, Übung, Labor	Lehrvortrag, Diskussion, Gruppenarbeit

#### EINGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Programmentwurf	Siehe Pruefungsordnung	ja

#### WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	72	78	5

#### QUALIFIKATIONSZIELE UND KOMPETENZEN

##### FACHKOMPETENZ

Die Studierenden können sichere IT Systeme architektonisch entwickeln und software- sowie hardwaretechnische Entscheidungen treffen.

##### METHODENKOMPETENZ

Die Studierenden können ihr Wissen in IT-Projekten anwenden und sich am Design sicherer IT Systeme kompetent beteiligen.

##### PERSONALE UND SOZIALE KOMPETENZ

-

##### ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden haben ein Verständnis für die Entwicklung sicherer IT-Systeme und können Entscheidungen fachlich fundiert treffen.

#### LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Design sicherer Systeme	48	24
Sicherer Einsatz von Betriebssystemen Design sicherer Softwarearchitekturen Hardwareauswahl und -beschränkung Codegenerierung Testen, Zertifizieren, Erproben		
Labor Sichere Systeme	24	54
Konzeption und prototypische Umsetzung sicherer IT Systeme anhand konkreter fachlicher Vorgaben		

#### BESONDERHEITEN

-

**LITERATUR**

ISO/IEC 27034-1:2011-11, Informationstechnik - IT Sicherheitsverfahren - Sicherheit von Anwendungen

I. Miklečić und H. Pohl, „ISO 27034-basiertes Certified Secure Software Development & Testing,“ 2015. <http://www.datensicherheit.de/aktuelles/iso-27034-basiertes-certified-secure-software-development-testing-24841>

S. Lipner und M. Howard, „Entwicklungszyklus für sichere Software,“ Microsoft, 5 2005. [Online]. Available: <https://msdn.microsoft.com/de-de/library/ms995349.aspx>

National Institute of Standards and Technology, „Source Code Security Analyzers, [https://samate.nist.gov/index.php/Source\\_Code\\_Security\\_Analyzers.html](https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html)

National Institute of Standards and Technology, „Software Security Assessment Tools Review,“ 2 3 2009. [Online]. Available:

<https://samate.nist.gov/docs/NAVSEA-Tools-Paper-2009-03-02.pdf>

Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley; 2. Auflage, 2008

Charles P. Pfleeger et.al.: Security in Computing, Prentice Hall, 5. Auflage, 2015

Peter Lipp et.al.: Trusted Computing - Challenges and Applications, Springer, 2008

David Challenger et.al: A Practical Guide to Trusted Computing, IBM Press, 2007

ISO/IEC 27034-1:2011-11, Informationstechnik - IT Sicherheitsverfahren - Sicherheit von Anwendungen

I. Miklečić und H. Pohl, „ISO 27034-basiertes Certified Secure Software Development & Testing,“ 2015. <http://www.datensicherheit.de/aktuelles/iso-27034-basiertes-certified-secure-software-development-testing-24841>

S. Lipner und M. Howard, „Entwicklungszyklus für sichere Software,“ Microsoft, 5 2005. [Online]. Available: <https://msdn.microsoft.com/de-de/library/ms995349.aspx>

National Institute of Standards and Technology, „Source Code Security Analyzers, [https://samate.nist.gov/index.php/Source\\_Code\\_Security\\_Analyzers.html](https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html)

National Institute of Standards and Technology, „Software Security Assessment Tools Review,“ 2 3 2009. [Online]. Available:

<https://samate.nist.gov/docs/NAVSEA-Tools-Paper-2009-03-02.pdf>

Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley; 2. Auflage, 2008

Charles P. Pfleeger et.al.: Security in Computing, Prentice Hall, 5. Auflage, 2015

Peter Lipp et.al.: Trusted Computing - Challenges and Applications, Springer, 2008

David Challenger et.al: A Practical Guide to Trusted Computing, IBM Press, 2007



## Data Security (T3INF4375)

### Data Security

#### FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
T3INF4375	3. Studienjahr	1	Prof. Dr. Andreas Judt	Deutsch

#### INGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung, Übung, Labor	Lehrvortrag, Diskussion, Gruppenarbeit

#### INGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Programmentwurf	Siehe Pruefungsordnung	ja

#### WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	72	78	5

#### QUALIFIKATIONSZIELE UND KOMPETENZEN

##### FACHKOMPETENZ

Die Studierenden kennen Verfahren zu Sicherung der Daten von Anwendern und Applkationen in einem Unternehmensumfeld.

##### METHODENKOMPETENZ

Die Studierenden können qualifiziert Verfahren zur Datensicherheit auf die Aufgaben des Unternehmens anwenden.

##### PERSONALE UND SOZIALE KOMPETENZ

-

##### ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden haben ein Verständnis für Datensicherheit in Unternehmen entwickelt und können ihr Wissen in die Umsetzung kompetent einbringen.

#### LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Data Security	48	39
Cloud Security, Zusammenarbeit mit Cloud-Providern Sicherheitsaspekte bei Data Mining und Big Data Sicherheit von Daten und Benutzern in Unternehmensanwendungen Cloud Modelle: IaaS, SaaS, PaaS Public vs Private Cloud Grundsätzliche Sicherheitsanforderungen (Datenschutz, Authentifizierung, Benutzeradministration / Rollenkonzept, Verschlüsselung, Datensicherung)		
Labor Data Security	24	39
Praktische Anwendung der Sicherheitskonzepte bei Cloud, Data Mining und Big Data		

#### BESONDERHEITEN

-

## LITERATUR

- Alan Calder, Steve G. Watkins: It Governance: An International Guide to Data Security and ISO27001/ISO27002, Kogan Page; Auflage: 6. Auflage (2015)
- Jonathan LeBlanc, Tim Messerschmidt: Identity and Data Security for Web Development: Best Practices, O'Reilly UK Ltd.; Auflage: 1 (2016)
- Cloud Security Alliance: <https://cloudsecurityalliance.org/>
- Cloud Control Matrix: [https://cloudsecurityalliance.org/group/cloud-controls-matrix/#\\_overview](https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)
- Mapping ISO27002/27017/27018 with CCM:  
<https://cloudsecurityalliance.org/media/news/open-peer-review-ccm-v3-0-1-with-iso-270022701727018-candidate-mapping/>
- Bundesamt für Sicherheit in der Informationstechnik: Sichere Nutzung von Cloud-Diensten, BSI-MIBro16/201
- International Standard ISO/IEC 27018:2014: Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

## Methodenkompetenz in der IT Sicherheit (T3INF4113)

### Methodological Competence in IT-Security

#### FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
T3INF4113	1. Studienjahr	1	Prof. Dr. Andreas Judt	Deutsch

#### INGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung, Übung	Lehrvortrag, Diskussion

#### INGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Kombinierte Prüfung - Klausur und Referat	Siehe Pruefungsordnung	ja

#### WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	72	78	5

#### QUALIFIKATIONSZIELE UND KOMPETENZEN

##### FACHKOMPETENZ

Die Studierenden die Vorgehensweise bei Angriffen und Sicherheitsverletzungen auf Produkt und Unternehmen. Sie kennen verschiedene Szenarien aus Fallstudien und können in in solchen Situationen angemessen reagieren.

##### METHODENKOMPETENZ

Die Studierenden können ihr Wissen in IT-Projekten anwenden und in Projektteams eine angemessene Vorgehensweise umsetzen.

##### PERSONALE UND SOZIALE KOMPETENZ

-

##### ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden haben ein Verständnis für die aktuelle Rechtslage in Sicherheitsfragen der IT vertieft, kennen Fälle aus der Praxis und können ihr Wissen auf Situationen in der betrieblichen Praxis anwenden.

#### LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Methodenkompetenz	48	27

## LERNEINHEITEN UND INHALTE

### LEHR- UND LERNEINHEITEN

Einbettung eines IT Sicherheitsbeauftragten in die Unternehmensstruktur  
Aktuelle Gesetzeslage in der IT Sicherheit (StGB, BGB, TKG, ...)  
Rechnersicherheit  
OpenSource Recht  
Internationales IT Recht  
Aktuelle Normen zu IT Security, z.B. ISO 27001  
§201, StGB: Verletzung der Vertraulichkeit des Wortes  
§202a, StGB: Ausspähen von Daten  
§202c, StGB: Vorbereiten des Ausspähens und Abfangens von Daten („Hacker-Paragraph“)  
§303a, StGB: Datenveränderung  
§303b, StGB: Computersabotage  
§823, BGB: Schadensersatzpflicht  
§826, BGB: Sittenwidrige vorsätzliche Schädigung  
§88, TKG: Fernmeldegeheimnis  
§89, TKG: Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen  
§90, TKG: Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen  
§148, TKG: Strafvorschriften

### PRÄSENZZEIT

### SELBSTSTUDIUM

Fallstudien zur Methodenkompetenz

24

51

Konkrete Fallstudien von externen Angriffen und Sicherheitsverstößen, betrachtet werden sowohl rechtliche als auch technische Aspekte der Fälle

### BESONDERHEITEN

Das Modul vertieft das Grundlagenwissen des Moduls IT Sicherheit (T3INF4301)

### VORAUSSETZUNGEN

IT Recht 1

### LITERATUR

-  
Verschiedene ISO-Normen, z.B. ISO 27001  
BSI Grundschriftshandbuch  
EU Datenschutzgrundverordnung  
H. Redeker, IT Recht, C.H. Beck, 6. Auflage, 2016