Open C3S
Open Competence Center for Cyber Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16OH12021 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor/bei der Autorin.


# Open Competence Center for Cyber Security

## E R G E B N I S B O G E N
## EQF-Bewertung

Berufsbegleitender Bachelor-Studiengang

**> Informatik / IT-Sicherheit <**

Darmstadt, den 17. März 2017

Open C³S

**Median (MD) / Minimum (Min.) / Maximum (Max.) der EQF-Stufen ...**

**... über alle Teilprozesse und Kategorien**
**[S. 1; Größe der Auswertungseinheit: N]**

**... je Kategorie über alle Teilprozesse**
**[S. 1; Größe der Auswertungseinheit: N]**

**... je Kategorie in den Teilprozessen**
**[S. 2 ff.; Größe der Auswertungseinheit: N]**

N = Fallzahl; F = davon fehlend

Die EQF-Bewertungen wurde von vier unabhängigen, externen Experten vollständig (alle Module) und von einem Experten partiell durchgeführt.
Die berichteten Ergebnisse stellen den Konsens der Experten dar.
Die EQR-Bewertungen basieren ausschließlich auf den Angaben und Formulierungen im Modulhandbuch (Stand Februar 2016).
Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C³S zu entnehmen.

## Zusammenfassende Mediane

**Median in der Gesamtbetrachtung**
**der EQF-Stufe über alle Teilprozesse, Kategorien und Fälle**

| MD | Min. | Max. | N | F |
|---|---|---|---|---|
| 4 | 2 | 6 | 183 | 39 |

**Kategorie "Kenntnisse"**
**Median der EQF-Stufe über alle Teilprozesse und Fälle**

| MD | Min. | Max. | N | F |
|---|---|---|---|---|
| 5 | 2 | 6 | 144 | 13 |

**Kategorie "Fertigkeiten"**
**Median der EQF-Stufe über alle Teilprozesse und Fälle**

| MD | Min. | Max. | N | F |
|---|---|---|---|---|
| 4 | 2 | 6 | 144 | 13 |

**Kategorie "Kompetenz"**
**Median der EQF-Stufe über alle Teilprozesse und Fälle**

| MD | Min. | Max. | N | F |
|---|---|---|---|---|
| 4 | 3 | 4 | 144 | 13 |

## Werte je Kategorie in den Teilprozessen über alle Fälle
## und je Teilprozess über alle Kategorien und Fälle


Forschungsgruppe Brinkmann/Seger
seger@ifs.tu-darmstadt.de

| | Module des berufsbegleitenden Bachelor-Studiengangs > IT-Sicherheit < entsprechend den Modulbeschreibungen Stand Februar 2016 | Erlernte Kompetenzlevel je EQF-Kategorie in den Teilprozessen über alle Fälle |
|---|---|---|
| 1 | **Mathematik 1**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz**: Die Studierenden verstehen die Arithmetik reeller und komplexer Zahlen und können diese anwenden. Sie können entscheiden, ob Folgen bzw. Reihen konvergent sind oder nicht und ggf. Grenzwerte berechnen. Des Weiteren können Sie die elementaren Funktionen der Analysis erklären und haben Kenntnis über ihre grundlegenden Eigenschaften. Sie können die Definition des Begriffs 'Vektorraum' erklären und können diese auf konkrete Vektorräume anwenden. Darüber hinaus beherrschen Sie den Umgang mit Vektoren und Matrizen. Sie können mit dem Begriff 'Stetigkeit' einer reellen Funktion umgehen und können beurteilen, wann diese Eigenschaft eine gegebene Funktion hat.<br>* **Methodenkompetenz:** Die Studierenden erwerben die Fähigkeit, mit den Lehrinhalten des Moduls aktiv umgehen zu können und können Fragestellungen, Aufgaben und Probleme, die sich aus der Lehrveranstaltung ergeben, selbständig bearbeiten und lösen.<br>* **Sozialkompetenz:** Die Studierenden erlernen die Teamarbeit durch gemeinsames Lösen von Übungsaufgaben an den Präsenzwochenenden. Sie erlangen weiter die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.<br>* **Selbstkompetenz:** Die Studierenden können aufgrund der Teamarbeit problemorientiert diskutieren. Die Studierenden erlangen die Fähigkeit, sich eine Meinung über die Themen von Mathematik I zu bilden und können das erlangte Wissen im Bereich der Informatik einsetzen.<br><br>Inhalte:<br>- Grundlagen (Reelle und komplexe Zahlen)<br>- Zahlentheorie und modulare Arithmetik<br>- Vektoren und Vektorräume (Vektorrechnung im $R^3$, Begriff des Vektorraums, Beispiele für Vektorräume)<br>- Matrizen, Determinanten<br>- Lineare Gleichungssysteme | EQF-Kategorien / MD / Min. / Max. / N / F<br>Kenntnisse: 5 / 3 / 5 / 4 / 1<br>Fertigkeiten: 5 / 4 / 5 / 4 / 1<br>Kompetenz: 3 / 3 / 3 / 4 / 1<br>Über alle Kategorien: 5 / 3 / 5 / 12 / 3 |

**Grundlagen der Programmierung**

(2 Semester/300 Lernstunden / 10 ECTS)

* **Fachkompetenz:** Die Studierenden können beliebige Programme in Java erstellen. Sprachkomponenten, die Sie noch nicht kennen, können Sie sich in kürzester Zeit aneignen. Zudem sind die Studierenden in der Lage, sich selbstständig neue Programmiersprachen beizubringen. Sie schreiben sichere Programme und wissen, wo potenzielle Schwachstellen in einem Programm zu finden sind.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit beliebigen IDEs. Sie können fremde Programme untersuchen und den Kontrollfluss nachvollziehen. Sie sind in der Lage, Schwachstellen und Fehler in einem Programm zu finden und zu beseitigen.
* **Sozialkompetenz:** Durch das gemeinsame Lösen von Aufgaben erlangen die Studierenden die Fähigkeit, eigene Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und ihre Teamfähigkeit zu stärken. In der Präsenzphase erlangen sie u. a. durch Pair-Programming die Kompetenz, eigene Ideen gegenüber einem anderen Programmierer zu kommunizieren, Kompromisse zu bilden und diese im Team umzusetzen.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über eigene Programme und Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.

2

Inhalte:

-**Einführung in das Programmieren**

Eine Einführung in die Programmiersprache Java. Mit Hilfe der Entwicklungsumgebung BlueJ wird den Studierenden der Umgang mit Java und Objektorientierung vertraut gemacht. Themen sind unter anderem:

- Ausdrücke und Algorithmische Kernsprache von Java
- Sprachbeschreibung und Objekttypen
- Eine Einführung in bereits existierende Methoden und Klassen in der Programmiersprache Java
- Polymorphie und Generics
- Testen und Test Driven Development mit JUnit

Darüber hinaus erhalten die Studierenden einen praktischen Einblick in die folgenden programmierrelevanten Technologien/ Techniken:

- Versionsverwaltung mit Git

- **Programmierkonzepte**

Diese Lehrveranstaltung knüpft nahtlos an die Veranstaltung „Einführung in das Programmieren" an. Die Studierenden lernen weitere Komponenten der Programmiersprache Java kennen, wie beispielsweise:

- Exceptionhandling
- I/O-Verarbeitung
- Rekursion
- Komplexität und Verifikation von Algorithmen

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 1 |
| Fertigkeiten | 5 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 3 | 5 | 12 | 3 |

| | | |
|---|---|---|
| 3 | **Einführung in die IT-Sicherheit**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden haben Grundkenntnisse des Sicherheitsmanagements, des Risikomanagements und der -analyse. Die Studierenden haben sich Grundlagen der Zugriffskontrolle und -verwaltung angeeignet, können Mechanismen der Authentisierung unterscheiden und erklären sowie SSO-Technologien beschreiben. Sie sind in der Lage, die unterschiedlichen Angriffe auf Zugriffskontrollsysteme darzustellen. Sie haben Grundkenntnisse der Kryptographie und Steganographie, können symmetrische und asymmetrische Verschlüsselungsverfahren differenzieren, Angriffe auf Kryptosysteme darstellen sowie kryptographische Hashfunktionen und digitale Signatur erklären. Zudem sind die Studierenden mittels ihrer Grundkenntnisse über die Sicherheitsaspekte vernetzter Umgebungen und das DNS in der Lage, diese zu erläutern. Sie können einen E-Mail-Missbrauch und Spam erklären sowie Phishing aufzeigen und ihre Lösungsansätze darstellen.<br>* **Methodenkompetenz:** Die Studierenden können eine Notfallplanung erläutern, die Bedrohungsfaktoren der IT-Sicherheit beschreiben und klassifizieren sowie deren Schutzmaßnahmen skizzieren und anwenden. Der Lernende kann die Phasen eines Hackerangriffs strukturieren, Malware analysieren und einordnen und die entsprechenden Schutzmaßnahmen<br>* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen.<br>* **Selbstkompetenz:** Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.<br><br>Inhalte:<br>- Grundlagen des Sicherheitsmanagements, des Risikomanagements und der -analyse<br>- Notfallplanung<br>- Bedrohungsfaktoren der IT-Sicherheit und deren Schutzmaßnahmen<br>- Grundlagen der Zugriffskontrolle und -verwaltung<br>- Mechanismen der Authentisierung, SSO-Technologien<br>- Darstellung der Angriffe auf Zugriffskontrollsysteme<br>- Einführung in die Kryptographie, symmetrische und asymmetrische Verschlüsselungsverfahren, Darstellung der Angriffe auf Kryptosysteme, kryptographische Hashfunktionen, digitale Signatur<br>- Einführung in die Steganographie<br>- Einführung in die Sicherheitsaspekte vernetzter Umgebungen, Grundlagen des DNS, E-Mail-Missbrauch<br>- Spam, Phishing, Network Security anwenden. | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 5 | 0 |
| Fertigkeiten | 3 | 3 | 4 | 5 | 0 |
| Kompetenz | 3 | 3 | 3 | 5 | 0 |
| Über alle Kategorien | 3 | 3 | 4 | 15 | 0 |

| | | |
|---|---|---|
| 4 | **Konzeptionelle Modellierung**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse über die Grundlagen der Modellierung sowie über das Entity-Relationship-Modell (ER-Modell). Darüber hinaus erwerben Sie fundiertes Wissen über die Datenbanksprache SQL sowie die Auszeichnungssprache XML.<br>* **Methodenkompetenz:** Die Studierenden haben die Fähigkeit zu beurteilen, wann eine Datenbank sinnvoll ist und können zwischen verschiedenen Typen von Datenbanksystemen unterscheiden.<br>* **Sozialkompetenz:** Die Konflikt- und Kommunikationsfähigkeit der Studierenden wird in den gemeinsamen Online-Tutorien und Diskussionsforen geschult.<br>* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die selbstentwickelten Datenmodellierungen und die Datenmodellierungen anderer. Darüber hinaus erlangen sie die Fähigkeit, in herausfordernden Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.<br><br>Inhalte:<br>- Grundlagen der Modellierung<br>- Entity-Relationship Modell (ER-Modell)<br>- Metamodellierung und XML<br>- Datenmodellierung und Domänenmodellierung | EQF-Kategorien / MD / Min. / Max. / N / F<br>Kenntnisse: 4 / 4 / 4 / 4 / 1<br>Fertigkeiten: 4 / 3 / 5 / 4 / 1<br>Kompetenz: 4 / 3 / 4 / 4 / 1<br>Über alle Kategorien: 4 / 3 / 5 / 12 / 3 |

| | | |
|---|---|---|
| 5 | **Mathematik 2**<br>(1 Semester/300 Lernstunden / 10 ECTS)<br><br>* **Fachkompetenz:**<br>Mathematik 2a:<br>Die Studierenden verstehen die Integral- und Differentialrechnung und können diese anwenden. Des Weitern kennen Sie die Grundbegriffe der Zahlentheorie, sowie der modularen Arithmetik und können mit diesen umgehen.<br>Mathematik 2b:<br>Sie können Primzahlen zerlegen und modular Potenzieren. Darüber hinaus kennen Sie das RSA-Kryptosystem und erlangen Wissen über die zugrundeliegende Sicherheit.<br>Die Studierenden wissen, wie Computersysteme Zahlen darstellen und können die Laufzeit eines Algorithmus berechnen. Sie kennen die Begriffe Interpolation, Approximation, numerische Integration und Differentiation. Weiter kennen Sie die elementaren Zählprobleme und können mit Hilfe des Binominialkoeffizienten die Anzahl von Möglichkeiten berechnen. Am Ende kennen Sie die Grundbegriffe der endlichen Wahrscheinlichkeitstheorie und können mit den Begriffen bedingte Wahrscheinlichkeiten und Zufallsgrößen umgehen. Darüber hinaus kennen Sie ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung und können damit umgehen.<br>* **Methodenkompetenz:** Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen.<br>* **Sozialkompetenz:** Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben.<br>* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von Mathematik 2 zu bilden und besitzen darüber hinaus die Kompetenz Sie in den entsprechenden Gebieten der Informatik einsetzen zu können.<br><br>Inhalte:<br>Mathematik 2a:<br>- Differential- und Integralrechnung einer und mehreren Veränderlichen Partielle Ableitungen<br>Mathematik 2b:<br>- Zahlentheorie und modulare Arithmetik (Binäre Zahlendarstellung, Algebraische Grundbegriffe, Teilbarkeit und Primzahlen, Primfaktorzerlegung, größter gemeinsamer Teiler, modulares Potenzieren, RSA-Kryptosystem)<br>- Numerik (Rechnerarithmetik, Algorithmen, Lineare Gleichungssysteme, Interpolation, Approximation, Numerische Integration, Numerische Differentiation)<br>- Kombinatorik und endliche Wahrscheinlichkeitstheorie (Elementare Zählprobleme, Binominialkoeffizient und Teilmengen, Permutation, Partitionen, Grundbegriffe der endlichen Wahrscheinlichkeitstheorie, bedingte Wahrscheinlichkeiten, Zufallsgrößen)<br>- Wahrscheinlichkeitsrechnung (ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung) | EQF-Kategorien / MD / Min. / Max. / N / F<br>Kenntnisse: 5 / 3 / 6 / 4 / 1<br>Fertigkeiten: 5 / 4 / 5 / 4 / 1<br>Kompetenz: 3 / 3 / 3 / 4 / 1<br>Über alle Kategorien: 5 / 3 / 6 / 12 / 3 |

| | | |
|---|---|---|
| 6 | **Rechnerstrukturen**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden erwerben Grundkenntnisse über die computergerechte Darstellung von Daten. Ferner eignen sie sich Grundlagen der Schaltalgebra an und können Schaltnetze bzw. -werke beschreiben und klassifizieren.<br>* **Methodenkompetenz:** Die Studierenden erlangen das Grundwissen über Rechnerarchitektur und können den Aufbau und die Komponenten verschiedener Rechnerarchitekturen darstellen und z.B. das Prinzip des Universalrechners erläutern und Prozessoren, Peripheriegeräte und Speicherorganisation erklären.<br>* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz.<br>* **Selbstkompetenz:** Die Studierenden können den Aufbau und die Funktionsweise von Rechnern verstehen und nachvollziehen. Desweiteren verfügen sie nach Absolvieren des Moduls über Kenntnisse der verschiedenen Abstraktionsebenen von Computern und deren Zusammenwirken. Ihnen wird bewußt, dass IT sehr schnelllebig ist und dass Detailwissen eine kurze Halbwertzeit hat. Sie sind in der Lage sich je nach Bedarf selbst weiterzubilden. Nach Bearbeitung diese Moduls verstehen die Studierenden den Computer als System und haben die grundlegenden Prinzipien verinnerlicht<br><br>Inhalte:<br>- Darstellung von Daten in einer computergerechten Weise<br>- Schaltalgebra<br>- Wichtige Rechnerstrukturen, einschließlich Prozessoren, Peripheriegeräten, Speicherorganisation und Verbindungsstrukturen<br>- Maschinenorientierte Programmiersprachen | EQF-Kategorien / MD / Min. / Max. / N / F<br>Kenntnisse: 4 / 2 / 4 / 4 / 1<br>Fertigkeiten: 3 / 3 / 3 / 4 / 1<br>Kompetenz: 3 / 3 / 3 / 4 / 1<br>Über alle Kategorien: 3 / 2 / 4 / 12 / 3 |

7

**Theoretische Informatik**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erlangen ein Verständnis für grundlegende Konzepte, Begriffe und Zusammenhänge aus den Teilgebieten Automatentheorie, formale Sprachen, Berechnungstheorie und P/NP-Theorie und haben ein Verständnis für grundlegende Beweismethoden entwickelt. Sie haben die Fähigkeit herausbildet, einfache Beweise selbständig zu führen. Des Weiteren haben Sie Kenntnis von der Leistungsfähigkeit unterschiedlicher Beschreibungsmittel und haben die Fähigkeit entwickelt, die Beschreibungsmittel selbständig zu gebrauchen. Darüber hinaus haben Sie das Wissen um den Zusammenhang zwischen der Leistungsfähigkeit und der algorithmischen Beherrschbarkeit unterschiedlicher Beschreibungsmittel erlangt. Die Studierenden haben weiter ein Verständnis für nichtdeterministische Maschinenmodelle und deren Bedeutung entwickelt. Sie können mit den deterministischen und nichtdeterministischen Maschinenmodellen umgehen und haben ein Verständnis für die algorithmische Lösbarkeit/Nichtlösbarkeit von Problemen sowie die inhärente Komplexität von Problemen entwickelt.
* **Methodenkompetenz:** Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können zu gegebenen formalen Sprachen Grammatiken und Automaten entwickeln, welche die gegebene formale Sprache erzeugt und akzeptiert. Darüber hinaus können Sie die Korrektheit ihrer Entwicklung zeigen. Sie können einen gegebenen deterministischen Automaten minimieren und gegebene kontextfreie Grammatiken in die Chomsky-Normalform umwandeln. Weiter können Sie zeigen, ob eine einfache Sprache regulär ist oder nicht und für die Sprache erläutern, zu welcher Klasse von Sprachen sie gehört. Sie beherrschen die grundlegenden Beweismethoden und haben die Fähigkeit, einfache Beweise selbständig zu führen. Sie können einfache Programme bei den unterschiedlichen Berechenbarkeitsmodelle formulieren, ihre Korrektheit beweisen und zeigen ob eine vorgegebene Menge entscheidbar/unentscheidbar ist. Sie können weiter zeigen, ob eine gegebene Menge NP-vollständig ist.
* **Sozialkompetenz:** Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen.
* **Selbstkompetenz:** Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch könne Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.Grundbegriffe: Wörter, Alphabete, Relationen, Operationen über Relationen

Inhalte:
- Formale Sprachen/Automatentheorie: Chomsky Grammatiken, Chomsky Hierarchie,Wortproblem, Reguläre Sprachen, deterministische und nichtdeterministische Automaten, Minimierungsalgorithmus für deterministische Automaten, Kontextfreie Sprachen, CYK-Algorithmus
- Berechnungstheorie: Berechenbarkeitsmodelle (RAM und TuringMaschinen), Churchsche These, Unentscheidbarkeit und TuringReduzierbarkeit
- Komplexitätstheorie: nichtdeterministische Turing- Maschinen, Komplexitätsmaße, Komplexitätsklassen, linear beschränkte Automaten und kontext-sensitive Sprachen, das P=NP? Problem, polynomielle Reduzierbarkeit, NPVollständigkeit

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

8

**Systemsicherheit 1**

(1 Semester/300 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Systemsicherheit 1a: Die Studierenden erwerben Grundkenntnisse über Betriebssysteme, ferner eignen sie sich Grundlagen der Prozessorganisation an, können Prozesse und Threads erklären, das Prozessmodell und die Prozesssteuerung beschreiben und Synchronisation und Context Switch erläutern. Außerdem erwerben sie Grundkenntnisse über Deadlocks.
  Systemsicherheit 1b: Die Studierenden erlangen anhand von UNIX-Beispielen das Basiswissen über Dateisysteme und sie erwerben Kenntnisse über den Aufbau eines Dateisystems. Ferner eignen sie sich Grundlagen der Speicherverwaltung an. Außerdem erhalten sie das Basiswissen über Scheduling und die Ein- und Ausgabe.
* **Methodenkompetenz:** Die Studierenden kennen unterschiedliche Arten von Betriebssystemen und können sie differenzieren und wissen außerdem wie ein ausführbares Programm entsteht. Sie sind in der Lage zwischen Prozessen und Threads zu unterscheiden und das Prozessmodell, die Prozesssteuerung und Context Switch zu erläutern. Die Lernenden können anhand der erlernten Lösungsansätze einen wechselseitigen Ausschluss lösen. Sie sind nach Durcharbeiten dieses Moduls in der Lage eigenständig Deadlocks zu modellieren und sie können Deadlock-Behandlungsstrategien anwenden.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.

Inhalte:

**Systemsicherheit 1a:**
- Eine Einführung in die Grundlagen von Betriebssystemen, ihre Aufgaben und Ausprägungen Prozesse, Threads, Prozessmodell und Prozesssteuerung
- Synchronisation, Context Switch
- Deadlocks

**Systemsicherheit 1b:**
- Grundwissen über Dateisysteme
- Grundlagen der Speicherverwaltung und virtuelle Speicher
- Basiswissen über Scheduling
- Ein- und Ausgabe

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 3 | 3 | 3 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 3 | 3 | 4 | 12 | 3 |

9

**Algorithmen und Datenstrukturen**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse in der Programmiersprache C. Sie lernen grundlegende Datenstrukturen und Algorithmen der Informatik kennen und erlernen, diese bezüglich Effizienz einzuschätzen und in einer konkreten Programmiersprache umzusetzen.
* **Methodenkompetenz:** Die Studierenden erwerben die Fähigkeit, konkrete Programmieraufgaben in einer höheren Programmiersprache zu formulieren. Lernende können hierbei die Gesamtaufgabe strukturieren und in Teilaufgaben zerlegen. Die Studierenden erlernen die Fähigkeit, geeignete Datenstrukturen und Algorithmen zur Abbildung von Programmieraufgaben zu finden, die eine effiziente Umsetzung gestatten.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigenen Programme und die Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.

Inhalte:
- Programmierkurs zur Erlernung der Programmierung in C
- Analysemodell, Lauzeitmodelle und allgemeine Analysetechniken für Algorithmen
- Strukturierte Datentypen wie Arrays, Listen, Bäume und Graphen
- Verschiedene Sortieralgorithmen mit ihren Laufzeitanalysen
- Algorithmen auf Mengen: Suchen, TRIES, Hashing, Union- Find und Priority Queues
- Balancierte Suchbäume, insbesondere AVL-Bäume und BBäume
- Repräsentation von Graphen und fundamentale Algorithmen auf Graphen
- Vertiefung der Graphenalgorithmen: Zusammenhangskomponenten und Bestimmung kürzester Pfade
- Implementierung der vorgestellten Algorithmen in C

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 5 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

10

**Kryptographie 1**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden kennen die Bedeutung von symmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten symmetrischen Primitiven. Darüber hinaus verinnerlichen die Studenten die Sicherheitskonzepte und diverse Angriffsziele von symmetrischen Verfahren. Die Grundprinzipienn asymmetrischer Kryptographie werden verstanden.
* **Methodenkompetenz:** Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von symmetrischen Verfahren nachvollziehen.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit aktuelle symmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue symmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen.

Inhalte:
- In diesem Modul werden zunächst einige grundlegende Begriffe der Datensicherheit erläutert. Danach werden einige historisch wichtige Verschlüsselungsverfahren vorgestellt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verschlüsselungsverfahren, Hashfunktionen und Message Authentication Codes (MAC). Als bedeutende Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 3 | 2 | 3 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 3 | 2 | 4 | 12 | 3 |

| | | |
|---|---|---|
| 11 | **Systemnahe Programmierung**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden haben fundierte Kenntnisse in der Programmierung von IA-32 auf Maschinenebene. Sie können Maschinencode aus der Hochsprache C erzeugen und haben einen Überblick über Verfahren zur Codeoptimierung und Codeverschleierung (Obfuscation). Die Studierenden haben einen Einblick in die Funktionsweise von Malware auf Systemebene und können einfache Malware selbstständig analysieren.<br>* **Methodenkompetenz:** Die Studierenden haben die Fähigkeit, systemnahe Programme zu erstellen und zu verstehen. Die Studierenden können Probleme auf dieser Ebene der Programmierung erkennen und Schwachstellen identifizieren und analysieren.<br>* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz.<br>* **Selbstkompetenz:** Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.<br><br>Inhalte:<br>In diesem Modul werden die folgenden Themengebiete behandelt:<br>- Allgemeine Rechner- und Betriebssystemstrukturen<br>- Innere Strukturen des Betriebssystems Microsoft Windows<br>- Assemblerprogrammierung der Intel-Architektur-32 (IA-32)<br>- Codeerzeugung, Codeoptimierung und Programmanalyse für IA-32<br>- Systemnahe Sicherheitsaspekte, insbesondere Mechanismen von Buffer Overflow und sonstigen Sicherheitslücken sowie Gegenmaßnahmen zur Verhinderung ihrer Ausbeutung<br>- Obfuscation und sonstige Malware-Techniken. Malware- Analyse durch das Analyseprogramm IDA anhand realer Beispiele | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 4 | 4 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 4 | 12 | 3 |

12

**Systemsicherheit 2**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erlangen anhand von Beispielen das Basiswissen über Malware, wie diese Schadsoftware funktioniert und welche Gefahr von ihr ausgeht. Ferner erwerben sie Kenntnisse über die Sicherheitsmechanismen und -modelle von Betriebssystemen und können zwischen unterschiedlichen Angriffsszenarien differenzieren. Außerdem eignen sie sich das Wissen über die entsprechenden Abwehrmechanismen an.
* **Methodenkompetenz:** Die Studierenden können zwischen den unterschiedlichen Malware-Arten differenzieren und können die entsprechenden Schutzmaßnahmen einsetzen. Sie kennen die Sicherheitsmechanismen- und modelle von Betriebssystemen und ihre unterschiedlichen Sicherheitsaspekte. Außerdem wissen die Studierenden wie Programmierfehler ausgenutzt werden können, was Insider-Angriffe sind und wie und welche Abwehrmechanismen sie einsetzen können.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.

Inhalte:
- Malware
- Sicherheitsmechanismen- und modelle
- Vorstellung und Erläuterung der Sicherheitsaspekte von Betriebssystemen.
- Angriffsszenarien
- Abwehrmechanismen

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

13

**Proseminar**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erkennen die Wichtigkeit des exakten wissenschaftlichen Arbeitens. Sie können eine begrenzte Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen.
* **Methodenkompetenz:** Die Studierenden erkennen die Wichtigkeit des methodischen Arbeitens im wissenschaftlichen Umfeld und können diese Methodik bei einem begrenzten, vorgegebenen Thema anwenden.
* **Sozialkompetenz:** Durch die enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden können fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.

Inhalte:
- Der Themenbereich des Proseminars wird vor Semesterbeginn bekanntgeben. Jeder Studierende erhält ein individuelles, begrenztes Thema (z.B. Buchkapitel oder Konferenzveröffentlichung). Dieses wird nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

14

**Einführung in die digitale Forensik**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften des ext4 Dateisystems und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines IT-Forensikers und können mit allgemeinen und speziellen forensischen Tools sicher umgehen. (Allgemeine Tools:Sleuthkit, DFF, X-Ways, spezielle Tools: File Carving, Strings). Des Weiter können Sie forensische Analysen von Anwendungen (SQLite Datenbank-, EXIF-, String-Analyse) durchführen und haben ein grundlegendes Verständnis für die Analyse und Auswertung von Smartphones mit dem Android OS. Sie sind mit diesem Wissen über die Architektur, der Speicherstrategie und Sicherheitskonzept vom Android OS, dem Flash Speicher, der Struktur und dem Inhalt wichtiger Verzeichnisse in der Lage eine forensische Analyse eines Smartphones durchzuführen.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen.
* **Sozialkompetenz:** Die Studierenden erlernen aufgrund gemeinsamer forensischen Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.

Inhalt:
- Klassische forensischeWissenschaften und digitale Forensik.
- Grundlagen der digitalen Forensik.
- Digitale Spuren (Entstehung, Manipulier- und Kopierbarkeit, Personenbezogenheit).
- Einführung in die Dateisystemanalyse (Generelles Konzept, Dateisystem ext4).
- Analyse mit forensischen Tools (Sleuthkit, DFF, X-Ways, Scalpel und strings).
- Anwendungsforensik (SQLite Datenbanken, EXIF und Strings Analyse).
- Mobilfunkforensik anhand von Fallbeispielen (Übersicht über Android OS, Flash Speicher, Struktur und Inhalt von wichtigen Verzeichnissen und Dateien).
- Übersicht über Cloud Forensik, Post Mortem und Live Analyse, Analyse der Windows Registry.
- Praktische Bearbeitung von Aufgaben

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 0 |
| Fertigkeiten | 4 | 4 | 5 | 4 | 0 |
| Kompetenz | 4 | 4 | 4 | 4 | 0 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 0 |

15

**Compilerbau**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse über die Funktionsweise und Arbeitsschritte von Compilern. Sie können die theoretischen Konzepte erklären, die benötigt werden, um ausgehend von einer formalen Sprachdefinition einen Compiler zu konstruieren. Mit Hilfe der Tools Flex und Bison können die Studierenden selbst Compiler für realistische Einsatzszenarien erzeugen.
* **Methodenkompetenz:** Die Studierenden beherrschen die Methodik, für eine gegebene Quellsprache und eine gewünschte Zielsprache einen phasenbasierten Compiler zu bauen. Dabei kommen gewöhnlich Tools zur Anwendung, die eine starke Unterstützung bei der Umsetzung der theoretischen Modelle bieten.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigene Arbeitsweise und die Arbeitsweise anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.

Inhalte:
- Anwendungsgebiete und Aufbau von Compilern
- Lexikalische Analyse auf Basis von regulären Sprachen
- Syntaktische Analyse auf Basis von kontextfreien Grammatiken
- Semantische Analyse durch attributierte Grammatiken und syntaxgesteuerte Definitionen, Erzeugung von Zwischencode
- Optimierung und Codeerzeugung
- Entwicklungswerkzeuge: Scannergenerator Flex und Parsergenerator Bisonerung der Sicherheit anzustellen. Als Grundlage werden kurz auch die Transportprotokolle TCP und UDP behandelt.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 6 | 12 | 3 |

16

**Netzsicherheit 1**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erkennen die wichtigen Strukturen von Sicherheitsmechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein „gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten.

Inhalte:
- Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen:
- Einführung in lokale Netze,
- WLAN (IEEE 802.11),
- VPN (IPSec, PPTP, IP Multicast),
- Mobilfunk (GSM, UMTS),
- Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 4 | 12 | 3 |

17

**Kryptographie 2**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden kennen die Bedeutung von asymmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten asymmetrischen Primitiven. Darüber hinaus verstehen die Studenten die Sicherheitskonzepte und diverse Angriffsziele in der asymmetrischen Kryptographie. Die Studenten können ihr Wissen über die Kryptographie anwenden und Sicherheitslösungen finden
* **Methodenkompetenz:** Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von asymmetrischen Verfahren nachvollziehen.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit aktuelle asymmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue asymmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen. Das umfangreiche Wissen der Studenten befähigt sie Sicherheitslösungen zu finden und einzusetzen.

Inhalte:
- In diesem Modul werden asymmetrische kryptographische Verfahren behandelt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verfahren und deren Einsatz für asymmetrische Basisdienste. Es werden sowohl diskrete Logarithmusverfahren (Diffie-Hellman, Elgamal, elliptische Kurven), als auch das RSA-Verfahren behandelt. Außerdem werden digitale Signaturen eingeführt. Es werden die Grundlagen der symmetrischen und asymmetrischen Schlüsselverteilung behandelt.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 1 |
| Fertigkeiten | 5 | 2 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 2 | 5 | 12 | 3 |

18

**Realisierung von Softwareprojekten**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse über Prozessmodellierung und lernen Zustandsdiagramme zu erstellen. Darüber hinaus erlangen sie Kenntnisse über Secure Coding Policies und Testing Policies.
* **Methodenkompetenz:** Die Studierenden beherrschen die Fähigkeiten ein Softwareprojekt zu entwerfen und umzusetzen sowie ein sicheres Programm zu schreiben.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Durch die Eigenentwicklung von Softwareprojektenerweitern die Studierenden ihre Selbstständigkeit. Die Studierenden lernen somit Verantwortung für ihr Handeln zu übernehmen und steigern ihre Entscheidungsfähigkeit.

Inhalte:
- Model Driven Architecture - UML
- Sichere Softwareentwicklung SDL / Microsoft
- JavaScript
- Grundlegende Kenntnisse in PHP

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

19

**Netzsicherheit 2**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Teilnehmer erwerben die Grundlagen zum Einrichten sicherer Kommunikationskanäle. Darüber hinaus lernen sie verschiedeneWege, wie die einzelnen Anwendungen in der Vergangenheit angegriffen wurden.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.

Inhalte:
- Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail,WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der dritten und vierten Ebene des OSI Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen:
  - SSL,
  - SSH,
  - OpenPGP,
  - S/MIME und
  - DNSSEC
- Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Als Grundlage werden kurz auch die Transportprotokolle TCP und UDP behandelt.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 1 |
| Fertigkeiten | 5 | 3 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 3 | 5 | 12 | 3 |

20

**Netzsicherheit 3**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erwerben grundlegendes Wissen im Bereich der Sicherheit von Webanwendung. Sie sind in der Lage die Sicherheit einer Webanwendung einzuschätzen und Angriffspunkte offenzulegen.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.

Inhalte:
- Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail,WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung desWorldWide Web (www) betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen:
  - Same Origin Policy
  - Cross Site Scripting
  - Cross Site Request Forgery
  - XML
  - Web Services
- Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 6 | 3 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 3 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 3 | 6 | 12 | 3 |

| | | |
|---|---|---|
| 21 | **Weiterführende Themen der Computerforensik**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Des weiteren haben Sie Kenntnis über Methoden der Antiforensik und können dies bei der Analyse berücksichtigen. Sie wissen um versteckte Bereiche, wie HPO und DCO auf einer Festplatte. Sie können unbekannte Datenformate analysieren und haben Kenntnis über das Vorgehen beim Software Reverse Engineering. Die Studierenden kennen weiter das grundlegende Konzept sowie die Eigenschaften der DOS und GPT Partitionen und der FAT und NTFS Dateisysteme und können mit diesem Wissen eine Dateisystemanalyse durchführen. Die Studierenden haben ein Verständnis, wie große Informationsmengen gemanagt und im Strafverfahren verknüpft werden.<br>* **Methodenkompetenz:** Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können Festplatten mit den Dateisystemen FAT und NTFS analysieren. Sie können unbekannte Software anhand von Software Reverse Engineering analysieren. Sie können digitale Beweise verschiedenster Informationsquellen bewerten und können angewandte Methoden der Antiforensik bei der Analyse erkennen. Sie können im Strafverfahren große Informationsmengen miteinander verknüpfen und Wissen um die Handhabe großer Informationsmengen.<br>* **Sozialkompetenz:** Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen.<br>* **Selbstkompetenz:** Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch könne Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.<br><br>Inhalt:<br>- Software Reverse Engineering.<br>- Erkennen und Bewerten verschiedenster Informationsquellen<br>- Informationsverknüpfung im Strafverfahren<br>- Allgemeine Vorgehensweisen bei der Durchführung forensischer Analysen.<br>- Bewertung digitaler Beweise auf Relevanz (technisch, juristisch).<br>- Analyse von Festplattenabbilder und effizientes Auffinden gelöschter Informationen.<br>- Möglichkeiten und Techniken der Antiforensik.<br>- Praktische Bearbeitung von Aufgaben | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 6 | 12 | 3 |

22

**Kryptographische Protokolle**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Die Studenten erkennen die praktische Relevanz der Kryptographie und begreifen die Schwierigkeit, kryptographische Protokolle - wie sie im Internet eingesetzt werden - formal auf ihre Sicherheit hin zu analysieren. Die Studenten kennen wichtige Sicherheitsziele und Sicherheitsmodelle, welche sie auf echte Protokolle anwenden können.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit kryptographischer Fachliteratur und können ihr wichtige Ergebnisse eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Beweistechniken und Sicherheitsmodellen vertraut, welche für formale Sicherheitsanalysen neuer Protokolle angewendet werden können.
* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Verstehen und Anwenden von neuen Modellen und Techniken aus und können wissenschaftlich zielorientiert diskutieren.
* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit, kryptographische Protokolle zu analysieren und eine wissenschaftlich begründete Einschätzung ihrer Sicherheit zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Protokolle aus der aktuellen Fachliteratur zu verstehen und ihre Sicherheit eigenständig zu evaluieren.

Inhalt:

- Dieses Modul bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreiben. Hierbei wird sowohlWert auf die Beschreibungen als auch auf die Sicherheit gelegt. Das Modul umfasst als Einführung allgemeine kryptographische Grundlagen, die Konzepte der beweisbaren Sicherheit und eine Einführung zu kryptographischen Protokollen. Im Folgenden werden einfache Protokolle behandelt. Hierzu zählen Passwort/Nutzername Protokolle, Wechselcodes, das Challenge-and-Response Verfahren, das Diffie-Hellman Protokoll, ElGamal sowie Shamir's No-Key-Verfahren. Des Weiteren werden Zero Knowledge Protokolle und ihre Theorie besprochen. Den Schwerpunkt des Moduls werden Schlüsselaustausch Protokolle bilden. Hierfür werden die Sicherheitsmodelle von Belare - Rogaway sowie Canetti - Krawczyk eingeführt. Den Abschluss des Moduls bildet eine detaillierte Beschreibung und formale Sicherheitsanalyse von TLS, dem wohl am weitesten verbreitete Authentifizierungs- und Schlüsseltausch Protokolls im Internet.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 6 | 4 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 3 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 3 | 6 | 12 | 3 |

23

**Sicherheit mobiler Systeme**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erlernen die wichtigen Strukturen von Sicherheitsaspekten in mobilen Datennetzen, verstehen die darin verwendeten kryptographischen Verfahren sowie das Zusammenspiel verschiedener Protokolle. Die Studierenden können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. Dazu werden auch konkrete Angriffe auf existierende Systeme vorgestellt, um ein tiefergehendes Verständnis zu erlangen.
* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit (englischer) Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Angriffs- und Analysetechniken vertraut, welche auf neue Systeme, Protokolle und Verfahren übertragen werden können.
* **Sozialkompetenz:** Die Studierenden tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die konstruktive Diskussion wird im Rahmen von Übungen erlernt.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit, sich selbständig eine Meinung über die Sicherheit von verschiedenen mobilen Systemen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studierenden entwickeln ein „gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten.

Inhalt:
- In diesem Modul erwerben die Teilnehmer Kenntnisse über Sicherheitsaspekte von verschiedenen mobilen Systemen, insbesondere zur Sicherheit von Smartphones. Im ersten Teil des Moduls liegt der Schwerpunkt auf der Beschreibung der wichtigsten Sicherheitsfunktionen von mobilen Systemen. Im zweiten Teil des Moduls wird die Sicherheit von Smartphones genauer beleuchtet und verschiedene Sicherheitsaspekte werden genauer betrachtet, der Fokus liegt dabei auf Apps für Smartphones. In der Vorlesung werden verschiedene Sicherheitsaspekte von mobilen Systemen vorgestellt. Anhand von konkreten Beispielen wird erläutert, wie verschiedene Arten von mobilen Systemen aufgebaut sind und welche Sicherheitsrisiken diese besitzen.
  Dies umfasst unter anderem die folgenden Themen:

- Design von GSM und UMTS (Sicherheitsaspekte, Lokalisierungsverfahren, Verbindungsmanagement)
- Sicherheit von Satellitentelefonen (GMR)
- Sicherheitsaspekte von DECT
- Design mobiler Betriebssysteme (Android und iOS)
- Analyse von (mobilen) Apps

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 6 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 6 | 12 | 3 |

| | | |
|---|---|---|
| 24 | **Sicherheitsmanagement**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden erwerben fundierte Kenntnisse über die grundlegenden Aspekte der Informationssicherheit und des Managements der Informationssicherheit, insbesondere in den Bereichen Governance in der Informationssicherheit, Risikomanagement, Incident Response Management und den Grundlagen des BSI IT-Grundschutzes.<br>* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen.Weiterhin sind die Studierenden mit verschiedenen Problematiken im Rahmen des Managements von Informationssicherheit vertraut und können diesesWissen an Praxisbeispielen umsetzen.<br>* **Sozialkompetenz:** Durch Erarbeitung von Fragestellungen in der Gruppe lernen die Studierenden die Sichtweisen verschiedener Bereiche der Informationssicherheit kennen und einen entsprechenden Ausgleich der Interessen zwischen den beteiligten Parteien im Unternehmen herbeizuführen.<br>* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit, Informationssicherheit zu managen und sich in diesem Bereich selbständig weiter zu bilden bzw. zu entwickeln. Darüber hinaus erlangen sie die Kompetenz, diesesWissen an die sich ständig ändernden Bedingungen im Unternehmen anzupassen.<br><br>Inhalt:<br>- Das Kapitel Einführung und Motivation soll den Studierenden zunächst die notwendigen Grundlagen vermitteln und für die Grundideen und –ziele der Informationssicherheit motivieren. Dabei werden die Hauptziele der Informationssicherheit dargestellt, vor allem auch im Vergleich zu denen der IT-Sicherheit.<br>- Im Kapitel Governance in der Informationssicherheit lernen die Studierenden anschließend die wesentlichen Konzepte und Ideen der Governance im Bereich der Informationssicherheit kennen. Dabei werden sowohl die grundlegenden Elemente der Governance behandelt, zudem wird aufgezeigt, wie eine effektive Governance betrieben werden kann.<br>- Im Kapitel Grundlagen des Risikomanagements erlernen die Studierenden die Grundzüge des Risikomanagements kennen. Nach einem einleitenden Teil, der unter anderem die grundlegenden Begrifflichkeiten vermitteln, wird aufgezeigt, wie der Prozess des Risikomanagements im Bereich der Informationssicherheit betrieben werden sollte.<br>- Nach diesen einführenden Überlegungen gliedert sich das Kapitel Entwicklung und Management eines Programms zur Informationssicherheit in zwei Abschnitte.<br>- Zunächst wird der Prozess der Entwicklung eines Programms zur Informationssicherheit behandelt. Hier erlernen die Studierenden, aus welchen Komponenten ein Programm zur Informationssicherheit besteht und was beim Aufbau eines solchen beachtet werden muss.<br>- Anschließend wird auf das Thema Management eines Programms zur Informationssicherheit eingegangen. Dabei erlernen die Studierenden, wie ein Programm zur Informationssicherheit aufrecht erhalten werden kann und welche Prozesse dafür aufzubauen sind. Insbesondere wird auch thematisiert, wie die zur Verfügung stehenden Ressourcen möglichst effizient eingesetzt werden können.<br>- Im Abschnitt Grundlagen des Incident Management erlernen die Studierenden, was im "Falle des Falles" zu tun ist. Dabei werden vor allem die Vorkommnisse behandelt, die im Rahmen des Risikomanagements nicht bzw. nicht ausreichend berücksichtigt werden konnten und die somit "unvorhergesehene" Ereignisse darstellen.<br>- Abschließend erlernen die Studierenden im Kapitel Informationssicherheitsmanagement auf Basis von BSI IT-Grundschutz den Aufbau eines Informationssicherheits-Managementsystems auf Basis von BSI IT-Grundschutz kennen. Dabei wird die Vorgehensweise anhand von konkreten Fallbeispielen exemplarisch erarbeitet. | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 5 | 0 |
| Fertigkeiten | 4 | 3 | 4 | 5 | 0 |
| Kompetenz | 3 | 3 | 4 | 5 | 0 |
| Über alle Kategorien | 4 | 3 | 4 | 15 | 0 |

| | | |
|---|---|---|
| 25 | **Spam**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden erwerben grundlegendesWissen im Bereich der Email-Kommunikation. Sie sind in der Lage Spamund Anti-Spam Techniken zu erläutern und kennen rechtliche Aspekte von Spam.<br>* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Sie verstehen die Wirksamkeit von Spam- Filtern und können diese konfigurieren.<br>* **Sozialkompetenz:** Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.<br>* **Selbstkompetenz:** Die Studenten erlangen die Fähigkeit Techniken im Spam-Umfeld aktueller Fachliteratur zu entnehmen und ihre Bedeutungen zu evaluieren.<br><br>Inhalt:<br>- E-Mails bilden heutzutage einen wichtigen Kommunikationskanal. Vor diesem Hintergrund stellt das immer stärker werdende Aufkommen von Spam nicht nur ein ärgernis dar, sondern verursacht auch einen enormen wirtschaftlichen Schaden. Um zu verstehen, wie Spam entsteht, werden zum einen Grundlagen vermittelt, wie dieWort-Ethymologie, die verschiedenen Formen von Spam in unterschiedlichen Medien, die oft verwendeten Definitionen sowie die in der Vorlesung verwendete Definition. Zum anderen werden in einer Fall-Studie das Wirtschaftsmodell sowie die Enttarnungsmöglichkeiten von Spammern besprochen. Ein tieferer Einblick in das SMTP-Protokoll stellt den Protokollfluss zwischen Sender und Empfänger dar und beschreibt die Verlässlichkeit der verschiedenen im E-Mail-Quellcode enthaltenen Daten und deren Manipulationsmöglichkeiten in Form einer Analyse der Header-Felder. Es werden verschiedene Formen der Anti-Spam-Maßnahmen präsentiert. Darunter fallen einfache Methoden wie Black- und Whitelists sowie die daraus resultierenden und leicht abgewandelten Graylists. Ebenfalls werden fortgeschrittene Methoden von Grund auf besprochen, wie bspw. Bayessche Filter. Als weitere Anti-Spam- Techniken werden auch alternative Protokolle angesprochen, die Zeit- und Speicherbeweise als Funktionen einsetzen, ebenso wie SPK und DKIM.Weiterhin wird Spam vom juristischen Standpunkt aus betrachtet, wobei das Opt-In bzw. Opt-Out-Verfahren im Fokus liegt. Ebenso werden die Strafbarkeit sowie die zivilrechtlichen Ansprüche und deren Durchsetzbarkeit angesprochen. Hier wird auch das Spam-Verständnis in den USA mit dem der EU verglichen.Weiterhin werden die juristischen Möglichkeiten für Whitelists diskutiert. Im wirtschaftlichen Bereich werden die Preise für E-Mail, die Wirtschaftlichkeit von Spam sowie der Verfolgungsdruck von Spammern behandelt. | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 4 | 12 | 3 |

| | | |
|---|---|---|
| 26 | **Netzbasierte Angriffserkennung**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden kennen die Grundlagen der Netzsicherheit sowie typische netzbasierte Angriffe. Sie haben Kenntnis über die Platzierung von Sensoren im Netzwerk sowie über Datenformate für netzbasierte Angriffserkennung. Sie können die Vor- und Nachteile von Deep Packet Inspection gegenüber aggregierten Formaten wie NetFlow bzw. IPFIX bewerten. Die Studierenden verstehen, wie unterschiedliche Malware-Samples netzbasierte Angriffe durchführen. Sie kennen die Funktionsweise von Maschinellen Lernverfahren und können deren Einsatz für die Klassifikationsprobleme bewerten. Die Studierenden kennen Detektionsverfahren zur netzbasierten Angriffserkennung und wissen, wie man auf unterschiedliche Angriffe reagiert.<br>* **Methodenkompetenz:** Die Studierenden beherrschen den Umgang mit gängigen Tools für maschinelles Lernen und können wichtige Ergebnisse daraus eigenständig bewerten. Sie sind mit den Grundprinzipien der netzbasierten Angriffserkennung mittels NetFlow oder IPFIX vertraut und können diese bei einer Angriffserkennung anwenden. Sie können weiter mit dem erlangtenWissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen.<br>* **Sozialkompetenz:** Die Studierenden erlernen aufgrund gemeinsamer Angriffsuntersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen.<br>* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit eine Angriffsuntersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.<br><br>Inhalt:<br>- Typische netzbasierte Angriffe.<br>- Datenquellen und -formate für netzbasierte Angriffserkennung (OpenFlow, NetFlow, IPFIX)<br>- Schadsoftware<br>- Maschinelle Lernverfahren zur Angriffserkennung.<br>- Reaktionsmöglichkeiten.<br>- Moderne Netzwerkparadigmen wie Software-Defined Networking (SDN).<br>- Praktische Bearbeitung von Aufgaben. | EQF-Kategorien / MD / Min. / Max. / N / F<br>Kenntnisse: 5 / 4 / 6 / 4 / 1<br>Fertigkeiten: 5 / 4 / 5 / 4 / 1<br>Kompetenz: 4 / 4 / 4 / 4 / 1<br>Über alle Kategorien: 5 / 4 / 6 / 12 / 3 |

27

**User-Centered Security**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden verstehen die der User-Centered Security zugrunde liegenden Probleme. Sie können Systeme im Hinblick darauf untersuchen und beurteilen, wie weit Kriterien der User-Centered Security bedacht und umgesetzt worden sind. Sie können zudem geeignete Entwicklungsprozesse für eigene Systeme einsetzen, die die Aspekte der User-Centered Security beachten. Die Studierenden sind dafür mit den grundlegendenWissenschaftlichen Methoden dieses Bereichs vertraut.
* **Methodenkompetenz:** Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen.
* **Sozialkompetenz:** Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben.
* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von User-Centered Security zu bilden und besitzen darüber hinaus die Kompetenz sie in den entsprechenden Gebieten der Informatik einsetzen zu können.

Inhalt:
- User-Centered Security befasst sich mit der Benutzerfreundlichkeit und Sicherheit von Systemen. In diesem Modul werden die grundlegenden Problemen betrachtet, die auftreten, wenn ein System zugleich benutzerfreundlich und sicher sein soll. Es wird diskutiert, warum benutzerzentrierte Sicherheit überhaupt ein erstrebenswertes Ziel ist und wie sie in Softwareentwicklungsprozesse eingebunden werden kann.
- Dabei werden die wissenschaftlichen Methoden zur Untersuchung von Systemen und dem Umgang damit erlernt und es werden exemplarisch die Bereiche Authentifizierung und Internetsicherheit besprochen.
- Im Zusammenhang mit der benutzerzentrierten Authentifizierung werden die Schwächen von Passwörtern und mögliche Alternativen, wie grafische Passwörter, biometrische Verfahren und Mehrfaktorauthentifizierung untersucht.
- Im Bereich der Internetsicherheit werden Schwierigkeiten bei der Verwendung von PKIs, OpenPGP und dem Design vonWarnmeldungen untersucht und daran allgemeine Verbesserungsmöglichkeiten vermittelt.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 5 | 5 | 0 |
| Fertigkeiten | 4 | 4 | 5 | 5 | 0 |
| Kompetenz | 3 | 3 | 4 | 5 | 0 |
| Über alle Kategorien | 4 | 3 | 5 | 15 | 0 |

28

**Incident Management**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erlangen mit diesem Modul das Basiswissen über das Incident Management und das Risikomanagement. Sie können die Schritte des Incident Management Prozesses nachvollziehen und sind imstande grundlegende Begriffe des Incident Management zu erklären und einzuordnen und können zwischen den spezifischen Rollen im Incident Management differenzieren. Ferner sind die Studierenden in der Lage einen Risikomanagementprozess mit seinen einzelnen Phasen zu erklären und kennen die bekannten Methoden und Werkzeuge des Risikomanagements.
* **Methodenkompetenz:** Die Studierenden sind in der Lage den Incident Management Prozess selber anzuwenden und eine Risikoberechnung aus der Wahrscheinlichkeit und der Schadenshöhe durchzuführen. Ferner können die Studierenden die einzelnen Schritte des Risikomanagementprozesses nachvollziehen und anwenden.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden haben sich ein Grundwissen über das Incident Management angeeignet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.

Inhalt:
- Grundwissen des Incident Management
- IT-Service Management (ITSM)
- IT-Security Management
- Risikomanagement

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 3 | 4 | 4 | 1 |
| Fertigkeiten | 3 | 3 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 3 | 4 | 1 |
| Über alle Kategorien | 3 | 3 | 4 | 12 | 3 |

| | | |
|---|---|---|
| 29 | **Elektronische Identitäten**<br>(1 Semester/150 Lernstunden / 5 ECTS)<br><br>* **Fachkompetenz:** Die Studierenden erwerben ein Verständnis für die grundlegenden Konzepte von elektronischen Identitäten. Sie kennen weit verbreite Verfahren und können neue Verfahren untersuchen und beurteilen.<br>* **Methodenkompetenz:** Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen.<br>* **Sozialkompetenz:** Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben.<br>* **Selbstkompetenz:** Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Thematik der elektronischen Identitäten zu bilden und besitzen darüber hinaus die Kompetenz sie in den entsprechenden Gebieten der Informatik einsetzen zu können.<br><br>Inhalt:<br>- Grundprinzipien von elektronischen Identitäten<br>- Kryptographische Grundlagen für elektronische Identitäten<br>- Hoheitliche elektronische Identitäten (z. B. elektronische Ausweise, Reisepässe)<br>- Elektronische Identitäten in Netzwerken (z. B. PKIs, OpenID, OAuth)<br>- Elektronische Identitäten in Organisationen (z. B. SSO-Systeme, Identitätsmanagement) | |

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 3 | 4 | 4 | 1 |
| Kompetenz | 3 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

30

**Ethisches Hacking**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden kennen die fundamentalen Begriffe und Prinzipien, welche die Gefahrensituation eines Computersystems beschreiben. Sie sind in der Lage Interessengruppen für die Angriffe auf IT-Infrastrukturen zu identifizieren und deren zentrale Handlungsprinzipien sowie Strategien darzustellen. Darüber hinaus können sie die grundlegenden Positionen und ethische Handlungslinien der Verteidiger charakterisieren, welche deren Basis der digitalen Selbstverteidigung bilden. Die Studierenden sind in der Lage, die Phasen eines Hacking-Angriffs zu skizzieren und deren strukturelle Chronologie zu beschreiben. Sie können die Vorgehensweise der Hacker in jeder einzelnen Phase in ihrer Methode und den verwendeten Technologien, Protokollen und Tools beschreiben. Darüber hinaus sind die Studierenden befähigt, verschiedene Angriffsformen zu charakterisieren und zu unterscheiden, sowie passende Verteidigungsstrategien zu benennen und geeignete Mittel und Wege aufzuzeigen. Sie verstehen die Wege der Informationsbeschaffung aus öffentlichen Quellen oder des Social Engineerings und den dabei verfolgten Angreiferprinzipien der Tarnung und Täuschung.
* **Methodenkompetenz:** Die Studierenden sind in der Lage den Gefährdungsgrad einer IT-Infrastruktur einzuschätzen und daraus ableitend die Voraussetzung für einen erfolgreichen Hacking-Angriff zu benennen und zu charakterisieren. Aus der bei Hacking- Angriffen verfolgten Chronologie und Methodik sind die Studierenden außerdem in der Lage Mittel und Strategien zur Früherkennung der jeweiligen Bedrohungsszenarien geeignete Schutzmaßnahmen zu skizzieren und anzuwenden. Dafür sind sie in der Lage, die dazu nötigen Tools auszuwählen und in einem Anwendungsszenario zielführend einzusetzen. Aus der Kenntnis der Durchführung eines erfolgreichen Angriffs auf ein computergesteuertes Informationssystem sind die Studierenden in der Lage einen solchen Angriff zu planen und im Zuge eines Sicherheitstests selbst auszuführen und dabei gleichzeitig ethische und rechtliche Leitlinien zu befolgen.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen.
* **Selbstkompetenz:** Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.

Inhalt:
- Definition und Anwendung der Begriffe Angriff, Hacking, Hacker, Ethisches Hacking und Cyberkriminalität
- Taktische Prinzipien und das Dilemma des Verteidigers
- Tätermotivation und Zielauswahl
- Die Anatomie des möglichen Opfers
- Reconnaissance und automatisierte Informationsbeschaffung
- DNS-Enumeration, DNS-Cache Snooping
- Fingerprinting und Schwachstellenermittlung
- Google als Hacking Tool
- Social Engineering
- Schwachstellenermittlung an einem Zielsystem
- Ausführung eines Angriffs und Kompromittierung des Systems
- Spurenbeseitigung
- Technische und nicht-technische Methoden des ethischen Hackings
- Techniken, Tools und Anwendungsbeispiele

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 6 | 12 | 3 |

31

**Anonymität im Netz**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden kennen die fundamentalen Begriffe und Prinzipien, welche die Gefahrensituation eines Computersystems beschreiben. Sie sind in der Lage Interessengruppen für die Angriffe auf IT-Infrastrukturen zu identifizieren und deren zentrale Handlungsprinzipien sowie Strategien darzustellen. Darüber hinaus können sie die grundlegenden Positionen und ethische Handlungslinien der Verteidiger charakterisieren, welche deren Basis der digitalen Selbstverteidigung bilden. Die Studierenden sind in der Lage, die Phasen eines Hacking-Angriffs zu skizzieren und deren strukturelle Chronologie zu beschreiben. Sie können die Vorgehensweise der Hacker in jeder einzelnen Phase in ihrer Methode und den verwendeten Technologien, Protokollen und Tools beschreiben. Darüber hinaus sind die Studierenden befähigt, verschiedene Angriffsformen zu charakterisieren und zu unterscheiden, sowie passende Verteidigungsstrategien zu benennen und geeignete Mittel und Wege aufzuzeigen. Sie verstehen die Wege der Informationsbeschaffung aus öffentlichen Quellen oder des Social Engineerings und den dabei verfolgten Angreiferprinzipien der Tarnung und Täuschung.
* **Methodenkompetenz:** Die Studierenden sind in der Lage den Gefährdungsgrad einer IT-Infrastruktur einzuschätzen und daraus ableitend die Voraussetzung für einen erfolgreichen Hacking-Angriff zu benennen und zu charakterisieren. Aus der bei Hacking- Angriffen verfolgten Chronologie und Methodik sind die Studierenden außerdem in der Lage Mittel und Strategien zur Früherkennung der jeweiligen Bedrohungsszenarien geeignete Schutzmaßnahmen zu skizzieren und anzuwenden. Dafür sind sie in der Lage, die dazu nötigen Tools auszuwählen und in einem Anwendungsszenario zielführend einzusetzen. Aus der Kenntnis der Durchführung eines erfolgreichen Angriffs auf ein computergesteuertes Informationssystem sind die Studierenden in der Lage einen solchen Angriff zu planen und im Zuge eines Sicherheitstests selbst auszuführen und dabei gleichzeitig ethische und rechtliche Leitlinien zu befolgen.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen.
* **Selbstkompetenz:** Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.

Inhalt:
- Kommunikation in Netzwerken bei Anwesenheit innerer und äußerer Angreifer
- Definition und Anwendung der Begriffe Anonymität, Unverkettbarkeit, Unbeobachtbarkeit
- Konzepte von Unterscheidbarkeit, Verkettbarkeit und Pseudonymität
- Privacy mit unterschiedlichem Schutzniveau von Kommunikationsdaten
- Rechtliche Rahmenbedingungen von Anonymität und Datenschutz im Internet
- Anonymisierungstechnologien, Overlay-Netzwerke
- Anonymisierer, Digitales Mixen, Java Anon Proxy (JAP)/JonDo
- TOR-Netzwerke und Hidden Services
- Bedrohungsmodelle, Mechanismen zum Schutz privater Netzwerk-Kommunikation
- Selbstschutz in sozialen Netzwerken, DeepWeb und Kriminalität
- Remailer-Systeme und OTR-Technologien
- Techniken zur Identifizierung von Nutzern im Web
- Auswirkungen der anonymisierten Internetnutzung

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 3 | 5 | 5 | 0 |
| Fertigkeiten | 4 | 3 | 5 | 5 | 0 |
| Kompetenz | 4 | 4 | 4 | 5 | 0 |
| Über alle Kategorien | 4 | 3 | 5 | 15 | 0 |

32

**Internetforensik**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden haben IT-forensische Grundlagen erworben, dazu gehören z.B. die wissenschaftliche Methodik, essentielle Prinzipien, Analyseansätze und Modelle zur Vorgehensweise bei der Spurensuche. Desweiteren haben sie einen Überblick über die unterschiedlichen Bedrohungen im Internet und die verschiedenen Angriffsmöglichkeiten bekommen.
* **Methodenkompetenz:** Die Studierenden können zwischen unterschiedlichen IT-Angriffsmöglichkeiten und Betrugsversuchen differenzieren und diese erklären. Desweiteren erlernen sie eine Vielzahl von Techniken zum Aufspüren der Websites und Server, die hinter Phishing, Spam und anderen Formen von Internet-Betrug sich verstecken und sind in der Lage diese anzuwenden.
* **Sozialkompetenz:** Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit derTeamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden haben sich ein Grundwissen über IT-Forensik angeeignet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.

Inhalt:
- Angriffsmöglichkeiten auf IT-Systeme
- Interna von Websites, Webservern, Webbrowsern und Email
- Möglichkeiten der digitalen Spurensuche
- Techniken der Informationssuche

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 4 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 4 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 3 | 4 | 4 | 1 |
| Über alle Kategorien | 4 | 3 | 5 | 12 | 3 |

33

**Seminar**

(1 Semester/150 Lernstunden / 5 ECTS)

* **Fachkompetenz:** Die Studierenden erweitern ihre im Proseminar erworbenen Kompetenzen. Sie können eine komplexere Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen.
* **Methodenkompetenz:** Die Studierenden haben einen vertieften Einblick in die Methodiken wissenschaftlichen Arbeitens können diese Methodiken bei einem größeren, vorgegebenen Thema anwenden.
* **Sozialkompetenz:** Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden können komplexe fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.

Inhalt:
- Der Themenbereich des Seminars wird vor dem Semester bekanntgeben. Jeder Studierende erhält ein individuelles Thema, in der Regel in Form eines initialen Papers. Von diesem ausgehend werden tiefere Literaturrecherchen zur Ergründung des Gesamtthemas durchgeführt. Die Ergebnisse werden nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 5 | 5 | 4 | 1 |
| Fertigkeiten | 5 | 4 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 5 | 12 | 3 |

34

**Projekt**

(2 Semester/300 Lernstunden / 10 ECTS)

* **Fachkompetenz:** Die Studierenden können umfangreiche praktische Arbeiten im Umfeld wissenschaftlicher Forschungsthemen selbstständig durchführen.
* **Methodenkompetenz:** Die Studierenden sind in der Lage, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Informatik zu erkennen.
* **Sozialkompetenz:** Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden können komplexe praktische Fragestellung bearbeiten und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und steuern.

Inhalt:
- Das Projekt kann in allen Teilbereichen der Informatik bearbeitet werden, hat aber in der Regel einen starken Bezug zu aktuellen Forschungsthemen der betreuenden Hochschule. Im Vordergrund stehen praktische Arbeiten im Umfeld eines laufenden Forschungsprojekts, wie z.B. Implementierungen.

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 5 | 4 | 5 | 4 | 1 |
| Fertigkeiten | 5 | 5 | 5 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 5 | 12 | 3 |

35

**Bachelorarbeit**

(1 Semester/450 Lernstunden / 15 ECTS)

* **Fachkompetenz:** Die Studierenden können umfangreiche praktische Arbeiten im Umfeld wissenschaftlicher Forschungsthemen selbstständig durchführen.
* **Methodenkompetenz:** Die Studierenden sind in der Lage, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Informatik zu erkennen.
* **Sozialkompetenz:** Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz.
* **Selbstkompetenz:** Die Studierenden können komplexe praktische Fragestellung bearbeiten und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und steuern.

Inhalt:
- Die Bachelorarbeit kann in allen Teilbereichen der Informatik geschrieben werden. Insbesondere relevant sind die folgenden Themen:
  - Softwareentwicklung
  - IT-Sicherheit im Allgemeinen
  - Netz- und Systemsicherheit
  - Digitale Forensik
  - Kryptographie
  - Theoretische Informatik
  - Compilerbau
  - Softwareentwicklung
  - Algorithmen und Datenstrukturen

| EQF-Kategorien | MD | Min. | Max. | N | F |
|---|---|---|---|---|---|
| Kenntnisse | 6 | 6 | 6 | 4 | 1 |
| Fertigkeiten | 5 | 5 | 6 | 4 | 1 |
| Kompetenz | 4 | 4 | 4 | 4 | 1 |
| Über alle Kategorien | 5 | 4 | 6 | 12 | 3 |