Open Competence Center for Cyber Security

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

HSAS, FAU, RUB, LMU & EKUT, FUB

>Zertifikatsangebot "Open C3S"<

Darmstadt, den 14. Mai 2014

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; Größe der Auswertungseinheit: N]

N = Fallzahl; F = davon fehlend

Die nachfolgende EQF-Bewertung wurde von den modulverantwortlichen Professoren durchgeführt.

Zusammenfassende Mediane

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

MD	Min.	Max.	N	F
6	**3**	**7**	**75**	**0**

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

MD	Min.	Max.	N	F
6	3	7	25	0

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

MD	Min.	Max.	N	F
6	3	7	25	0

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

MD	Min.	Max.	N	F
6	3	7	25	0

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

	Module des Zertifikatangebots > "Open C3S" < entsprechend den Modulbeschreibungen Stand September 2013	**Erlernte Kompetenzlevel je EQF-Kategorie in den Teilprozessen über alle Fälle**
1	**Datenträgerforensik 1 (HSAS)** (2 Monate / 150 Lernstunden / 5ECTS) * Nach erfolgreichem Abschluss des Moduls hat der Studierende grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann verschiedene Werkzeuge zur Analyse und Wiederherstellung von Dateien auf Datenträgern einsetzen und verfügt über grundlegende Kenntnisse, die in dem zweiten Modul "Datenträgerforensik" weiter ausgebaut werden können. Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz. - In diesem Modul gehen wir auf die forensische Untersuchung von sogenannten Massenspeichern (engl. mass storages) ein. Massenspeicher sind Peripheriegeräte, die zur Speicherung großer Datenmengen dienen, wobei als Speichermedium meist magnetische oder optische Träger sowie neuerdings Flash- Speicherbausteine eingesetzt werden. Massenspeicher sind für forensische Untersuchungen von großer Bedeutung, da sie oft einschlägige Informationen enthalten und zudem Rückschlüsse auf Benutzer, Besitzer und Zugriffe ermöglichen. In dem ersten Modul von Datenträgerforensik werden grundlegende Konzepte vermittelt und erste praktische Übungen ohne Fokus auf ein Dateisystem durchgeführt. - Einführung, Festplattentechnik, Festplatten kopieren **- Praktische Übung:** Kopieren von Festplatten mit HPA, Datenträger kopieren - Datenträgeranalyse **- Praktische Übung:** Arbeiten mit The Sleuth Kit und Autopsy - Analyse von Dateisystemen **- Praktische Übung:** Arbeiten mit X-Ways und EnCase	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse 6 6 6 1 0 Fertigkeiten 6 6 6 1 0 Kompetenz 6 6 6 1 0 Über alle Kategorien 6 6 6 3 0

2

Datenträgerforensik 2 (HSAS)

(2 Monate / 150 Lernstunden / 5ECTS)

* Nach erfolgreichem Abschluss des Moduls hat der Studierende einen Überblick über die verbreitetsten Datei- und Betriebssysteme sowie deren Funktionsweisen. Er hat grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern sowie gängiger Dateisysteme der Windows- Betriebssystemfamilie und bei den Unix-Derivaten. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann mit verschiedenen Werkzeugen zur Analyse und Wiederherstellung von Dateien auf Datenträgern umgehen und verfügt sowohl über analytische als auch methodische Fähigkeiten im Umgang mit diesen.Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz

- In diesem Modul werden die Dateisysteme FAT, ExtX und NTFS näher betrachtet. Dieses Modul stellt somit die ideale Ergänzung zu Datenträgerforensik 1 dar und vertieft die Grundlagen, die in dem vorangeführten Modul behandelt wurden. Die einzelnen Studienbriefe sind in sich geschlossen und auch die praktischen Übungen sind auf die einzelnen Dateisysteme speziell abgestimmt.

- FAT- Dateisysteme
- NTFS-Dateisystem
  Praktische Übung: Beispielhafte Einrichtung eines NTFS-Datei-systems; Analyse mit x-Ways, Encase: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen

- Linux/Unix Extended Dateisysteme (Ext3)
  Praktische Übung: Beispielhafte Einrichtung eines Ext4-Dateisystems; Analyse mit The Sleuth Kit, x-Ways: Filesystem erkunden, gelöschte Da-teien suchen, gelöschte Dateien wiederherstellen

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	7	7	7	1	0
Fertigkeiten	7	7	7	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	7	6	7	3	0

3

Einführung in die Informatik (HSAS)

(150 Lernstunden / 5 ECTS)

* Die Studierenden haben Kenntnisse über Instrumente und Methoden der Informatik. Sie haben insbesondere grundlegende Kenntnisse in der praktischen, technischen und theoretischen Informatik.
  Sie können Darstellungsformen und -formaten von Informationen in Rechnern interpretieren und umwandeln. Die Grundzüge von Rechnern und die Aufgaben unterschiedlicher Software wurden erlernt. Grundlegende Kenntnisse der IT- Sicherheit wurden erworben.
  Die praktischen Übungen versetzen den Studierenden in die Lage, an einem Rechner Datenformate und die Konfiguration eines Arbeitsplatzrechners zu analysieren. Der Studierende kann virtuelle Maschinen und darauf basierende Anwendungen und Konfigurationen einrichten. Darüber hinaus kann er fundamentale Maßnahmen zur IT-Sicherheit eines Arbeitsplatzrechners umsetzen und deren Wirkung überprüfen. Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).

- In diesem Modul werden die technischen Kenntnisse vermittelt, die ein IT-Sicherheitsexperte braucht, um ein Rechnersystem verstehen und zusammenstellen zu können. Auf der Grundlage des Verständnisses der Hardware-Architektur werden die vom Betriebssystem und den Anwenderprogrammen bewerkstelligten Verarbeitungsschritte klar. In diesem Gesamtzusammenhang werden die grundsätzlichen IT-Angriffsmöglichkeiten und IT-Schutzmechanismen verständlich.

- Informationsverarbeitung im Computer
  Praktische Übung: Codierung einer Textdatei
- Rechnersysteme
- Software
- IT-Sicherheit
  Praktische Übung: Angriffsszenario in einer sicheren Umgebung nachbilden

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	5	5	5	1	0
Über alle Kategorien	6	5	6	3	0

4

Internet - Technologien (HSAS)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die grundlegenden Strukturen und möglichen Transportwege der Informationen im weltweiten Netz. Der Teilnehmer ist mit der für den Betrieb des Internets erforderliche Hard- und Software vertraut und kann deren Bedeutung für die IT- Sicherheit beurteilen. Er kann die aus dem Informationsfluss resultierenden digitalen Spuren bewerten und Ermittlungsansätze ableiten sowie Eigenschaften wichtiger Dienste nachvollziehen und diese einsetzen. Darüber hinaus hat er einen Überblick über die Sicherheitsaspekte der Netze und kann mögliche Tools sowohl bewerten als auch einsetzen.

  Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).

- Internet
- Netzwerktechnik
- Internet-Dienste
- World Wide Web

EQF-Kategorien

Kategorien	MD	Min.	Max.	N	F
Kenntnisse	7	7	7	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	5	5	5	1	0
Über alle Kategorien	6	5	7	3	0

5

Einführung in die Programmierung im IT-Security-Umfeld (HSAS)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Die Studierenden können aus einer abstrakten Aufgabenstellung ein ablauffähiges Programm entwickeln. Wenn die Programmierung konkret wird, so findet die Programmiersprache Python Verwendung. Python ist eine leistungsfähige Skriptsprache, die im Forensik-Umfeld häufig verwendet wird. Die Grundkonstrukte von Programmen und deren Umsetzung in Python wurde erlernt. Die Studierenden haben erste Erfahrungen mit programmbasierten Sicherheits-Schwachstellen und verstehen einfachen Angriffsmechanismen. Die Studierenden können mit den selbst erstellten Programmen häufig in der Praxis vorkommende Aufgabenstellungen bewältigen wie z. B. das Durchsuchen eines Rechners nach auffälligen Bildern (Zuwachs an Methodenkompetenz). Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung).

  In diesem Modul werden die Kenntnisse in Informatik und Programmieren vermittelt, die ein IT-Sicherheitsexperte braucht, um für ein Rechnersystem spezifische Programme zur Analyse des IT-Sicherheitsstands vornehmen zu können sowie um sicherheitsrelevante Vorgängen überprüfen zu können. Damit ist auch die Grundlage für einen guten Einstieg zum Erlernen weiterer Programmiersprachen gelegt.

- Grundlagen Python
  Praktische Übung: Erstellen eines Programms, dass Dateien sucht und diese anhand des Dateityps kategorisch sortiert. In einer gleichnamigen txt-Datei werden Informationen über die Datei festgehalten.
- Datenbanken mit Python
  Praktische Übung: Ergänzung und Optimierung der praktischen Übung aus SB1, txt-Dateien durch Datenbankeinträge ersetzen, Suchanfragen über sqlite3 realisieren
- Penetration Testing mit Python
  Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme
- Forensik mit Python
  Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme
- Netzwerkanalyse mit Python
  Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme

EQF-Kategorien

Kategorien	MD	Min.	Max.	N	F
Kenntnisse	7	7	7	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	7	3	0

6

Grundlagen digitaler Forensik (FAU)

(150 Lernstunden / 5 ECTS)

* Die Teilnehmer beherrschen die terminologischen Grundlagen der digitalen Forensik und können Beziehungen zwischen Konzepten der klassischen Forensik und der digitalen Forensik herstellen
* Die Teilnehmer haben ein einfaches Werkzeug zur Analyse von Partitionstabellen erstellt und dadurch ein Verständnis für die Komplexität forensischer Software entwickelt
* Die Teilnehmer können forensische Gutachten aufgrund von allgemeinen Qualitätskriterien bewerten

- klassische (analoge) Forensik: Beispiele, Theorie der Entstehung von Spuren
- Terminologie: Identifizierung, Klassifizierung, Individualisierung, Assoziation
- Quantifizierung der Assoziation: Rechenbeispiele
- Digitale Spuren
- Kurze Einführung in die Datenträgeranalyse: Partitionssysteme (DOS, GPT)
- Regeln für den Aufbau forensischer Gutachten, Qualitätskriterien für forensische Dokumentation

Übungen:
- Einübung der Terminologie an Beispielen
- Digitale Spuren und digitale Forensik: Abgrenzung und Gemeinsamkeiten
- Programmierung von mmls (für DOS- und GPT-Partitionen). Untersuchung folgender Fragestellungen:
  - Wie behandeln unterschiedliche Betriebssysteme die nicht-essentiellen Daten in der Partitionstabelle?
  - Wie werden erweiterte Partitionen standardmäßig von verschiedenen Betriebssystemen angelegt?
  - Wie verhalten sich Betriebssysteme bei nicht standardmäßiger Codierung von erweiterten Partitionen (z.B. Zyklen)?

- **Projekt:** Schreiben eines forensischen Berichts zu einem individuellen Fall. Dieser basiert auf der Frage, ob Manipulationen in einem gegebenen Partitionssystem vorliegen.

- **Präsenzphase:** Vorstellung und Verteidigung des Berichts in einer mündlichen Prüfung (Rollenspiel)

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	5	5	5	1	0
Über alle Kategorien	6	5	6	3	0

7

Reverse Engeneering (FAU)

(150 Lernstunden / 5 ECTS)

* Die Studierenden können den Begriff „Reverse Engineering" einordnen und definieren. Sie können die typischen Einsatzgebiete von Reverse Engineering benennen. Die Strukturen von Microsoft Windows sind ihnen bekannt. Den Aufbau von Programmdateien in Windows können sie beschreiben und analysieren. Sie können die Methoden zur Decompilierung von Maschinenprogrammen benennen und anwenden. Verschiedene Optimierungsverfahren der Compiler, die eine Decompilierung erschweren, können sie erkennen und benennen. Die üblichsten Werkzeuge zur Programmanalyse können die Absolventen einsetzen, Vorteile und Nachteile einer statischen und dynamischen Programmanalyse sind ihnen bekannt, und sie können diese bedarfsabhängig einsetzen. Sie haben detaillierte Kenntnisse über Malware sowie verschiedene Methoden und Tricks der Malware-Autoren. Die Absolventen können „einfache" Malware selbstständig analysieren. Sie beherrschen die Grundlagen für den Einstieg in das weite Gebiet der Malware-Analyse.

- Einführung in Reverse Engineering
- Microsoft Windows
- Programmanalyse
- Werkzeuge zur Programmanalyse: IDA und OllyDbg
- Malware und Malware-Analyse

- **Präsenzwochenende:** Vorlesung, Übungen in Gruppen: Analyse verschleierter Binaries, Analyse von Malware

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	7	7	7	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	7	3	0

8

Grundlagen der Systemprogrammierung (FAU)

(150 Lernstunden / 5 ECTS)

* Die Studierenden kennen die Einsatzszenarien der systemnahen Programmierung, und ihre Prinzipien und Methoden sind ihnen bekannt. Sie können die Grundprinzipien aktueller Rechnerarchitekturen und Betriebssysteme benennen und einordnen. Die Intel IA-32-Architektur ist ihnen im Detail vertraut. Sie sind in der Lage, Assemblerprogramme für diese Architektur zu schreiben und zu verstehen. Die Unterschiede einer systemnahen Programmierung in Assembler und C sind ihnen bewusst. Den Studierenden sind die Stärken und Schwächen der Programmiersprache C bekannt. Durch eigenständiges Programmieren sind sie in der Lage, Programmierprojekte in C und Assembler umzusetzen und den Sinn sowie die Notwendigkeit effizienter Algorithmen und Datenstrukturen zu erkennen. Die Absolventen haben fundierte Grundkenntnisse, die eine Maschinenprogrammanalyse bei Reverse Engineering erfordert.

- Grundlagen Rechnerarchitektur
- Grundlagen Betriebssysteme
- Intel x86 Architektur und x86 Assembler (Starke Vertiefung der allgemeinen Grundlagen)
- Die Programmsprache C
- Sortieralgorithmen und Sortierbäume als Programmierprojekt
- Übungen
- Präsenzwochenende

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

9

Weiterentwicklung von Werkzeugen für die Mobilfunkforensik (FAU)

(150 Lernstunden / 5 ECTS)

* Die Studierenden kennen den Aufbau und die Funktionsweise von Android und Android-Applikationen. Sie können die grundlegenden Methoden zur Vorbereitung einer forensischen Analyse von Android-Mobiltelefonen anwenden. Darüber hinaus sind sie in der Lage, unterschiedliche Verfahren und Werkzeuge zur Analyse zu benennen und anzuwenden. Die Studierenden können einfache Applikationen für Android programmieren. Sie haben Kenntnisse in der Analyse von Android-Applikationen. Sie kennen die Schritte einer sicherheitskritischen Betrachtung von Android-Applikationen. Die Absolventen verfügen über Fähigkeiten, eine forensische Analyse von Mobiltelefonen auf der Basis von Android durchzuführen.

- Einführung in Android
- Einführung in Mobilfunkforensik für Android
- Aufbau von Android-Applikationen
- Analyse von Android-Applikationen
- Schreiben von Android-Apps
- Obfuscation

- **Projekt:** Im Rahmen des Projekts soll eine vollständige forensische Analyse eines Mobiltelefons durchgeführt werden. Dabei sollen sowohl die installierten Applikationen als auch ihre verwendeten Datenstrukturen analysiert werden. Die durchgeführte Untersuchung soll in einem möglichst gerichtsverwertbaren Bericht zusammengefasst werden.

- **Präsenzphase:**
  Vorlesung, vertiefende Übungen, Präsentation und Verteidigung der Projektergebnisse

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	7	7	7	1	0
Fertigkeiten	7	7	7	1	0
Kompetenz	7	7	7	1	0
Über alle Kategorien	7	7	7	3	0

10

Netzsicherheit 2 (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können.
  Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.
  Sie haben 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 haben ein „gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten entwickelt.

- 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
  Praktische Übung: Erzeugung eines eigenen (digitalen) SSL-Zertifikats.
- SSH
- OpenPGP
  Praktische Übung: Erzeugung eines eigenen PGP-Schlüssels zumVer- und Entschlüsseln von Dateien.
- S/MIME
  Praktische Übung: Manipulation S/MIME signierter Mails ohne Gültigkeit der Signatur zu beeinflussen.
- DNSSEC
  Neben den Systemen werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Als Grundlage werden kurz die Transportprotokolle TCP und UDP behandelt.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

11

Netzsicherheit 3 (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Den teilnehmenden Studierenden soll ein weit gefächertes Wissen über die häufigsten Schwachstellen in Webapplikationen vermittelt werden.
  Außerdem sollen sie lernen, wie sie derartige Schwachstellen manuell finden können, ohne die Hilfe von automatisierten Webapplikations-Scannern in Anspruch zu nehmen. Darüber hinaus lernen die Studierenden entsprechende Schutzmaßnahmen sowie deren Wirksamkeit kennen.

- Im Laufe der Lehrveranstaltung sollen die Studierenden eine fiktive Online-Banking-Applikation angreifen und dabei die im Laufe der Veranstaltung erlernten Methoden und Techniken einsetzen.

Dieses beinhaltet folgende Themengebiete:
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Session Hijacking
- Session Fixation
- SQL Injection (SQLi)
- Local/Remote File Inclusion (LFI/RFI)
- Path Traversal
- Remote Code Execution (RCE)
- Logical Flaws
- Information Leakage
- Insufficient Authorization

Das Wissen der Studierenden wird zudem durch externe Experten aus der In-dustrie und IT-Sicherheits-Szene, die in Vorträgen über verschiedene Thematiken der Webapplikations-Sicherheit referieren werden, angereichert.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

12

Grundlagen der Kryptologie 1 (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Erfolgreiche Studierende kennen das Grundvokabular symmetrischer Kryptogaphie. Anforderungen an symmetrische Verfahren der Kryptographie sind bekannt. Sie verstehen die praktische Relevanz symmetrischer Verfahren. Symmetrische Verfahren können anhand ihrer Funktionsweisen unterschieden werden.
  Die Teilnehmer verstehen die Notwendigkeit der Authenzität von Nachrichten und können erläutern, wie diese mit Hilfe symmetrischer Kryptographie erreicht werden kann.

- Historische Chiffren und Stromchiffren: Schiebe-/ Substitutionschiffren und das One Time Pad.
  Praktische Übung: Angriff auf das One Time Pad bei sich wiederholendem Schlüssel.
- Blockchiffren: DES und AES
  Praktische Übung: Analyse und Vergleich von DES und AES anhand von Brute Force Schlüsselsuche und Verschlüsselung (bit-) komplementärer Klartexte.
- Message Authentication Codes (MACs)

EQF-

Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

13

Grundlagen der Kryptologie 2 (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls haben die Studierenden das Grundvokabular der asymmetrischen Kryptographie verinnerlicht. Sie können den Unterschied zwischen asymmetrsichen und symmetrischen kryptographischen Verfahren erläutern und die praktische Relevanz asymmetrischer Verfahren darstellen.
  Die Teilnehmer kennen die beiden großen Klassen zahlentheoretischer Probleme, auf denen die asymmetrische Kryptographie aufbaut. Sie sind in der Lage neue Verfahren diesen Klassen zuzuordnen.

- Publick-Key Kryptographie: RSA und ElGamal
  Praktische Übung: Empirische Erfassung der Komplexität der Berechnung des DLOG.
- Digitale Signaturen
- Hash Funktionen
  Praktische Übung: Empirische Validierung der Diffusionseigenschaft von MD5

EQF-

Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

14

Analyse Kryptographischer Protokolle (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach einem erfolgreichen Abschluss des Moduls kennen die Studierenden die Grundlagen beweisbarer Sicherheit kryptografischer Verfahren. Sie kennen grundlegende kryptografische Protokolle und können dieses an Hand der garantierten Sicherheitseigenschaften differenzieren. Erfolgreiche Teilnehmer können neue Protokolle auf Sicherheitseigenschaften untersuchen. Sie sind in der Lage einen Sicherheitsbeweis zu skizzieren.

- Das 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 beschreibt. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt.

Die Vorlesung umfasst folgende Themen:
- Kryptographische Grundlagen (kurze Wiederholung der Wahrscheinlichkeitstheorie, Informationstheorie, etc.)
- Beweisbare Sicherheit
- Commitment Schemes
- Zero-Knowledge-Protokolle
- Key Exchange Protokolle
- TLS

EQF-

Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

Kryptanalytische Methoden und Werkzeuge (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Die Studierenden sind mit wesentlichen praktischen Komponenten und Werkzeugen der Kryptanalyse vertraut. Sie haben einen umfangreichen Überblick über Algorithmen und Techniken, die heutzutage zur Analyse bestehender Systeme eingesetzt werden. Des Weiteren haben sie nicht nur Kenntnisse über die neuesten Analyseverfahren, sondern auch die Grenzen bezüglich Rechen,- Speicher- und finanzieller Aufwand.
  Mit dem vermittelten Wissen, ist es den Teilnehmern zum Ende des Kurses möglich, unterschiedliche Methoden zur Analyse von bestehenden Systemen erfolgreich anzuwenden sowie die Limitierungen von Sicherheitsanalysen einschätzen zu können.

15

- Sicherheit vs. Rechenleistung
  Einführung, Plattformen (CPU, GPU, Spezialhardware), Metriken
  Praktische Übung: Vergleich von Sicherheitsanalysen und Angriffswerkzeugen auf verschiedenen Rechnerplattformen.
- Sicherheitsaspekte kryptographischer Geheimnisse mit besonderem Fokus auf die Wahl von Passwörter als Geheimnis sowie zufällig gewählter Sicherheitsparameter
  Praktische Übung: Durchführen eines parametrisierten Wörterbuchangriffs mittels personalisierter Passwortlisten.
- Einführung in die Kryptanalyse von Sicherheitssystemen, Standardangriffe auf symmetrische und asymmetrische Kryptosysteme
  Praktische Übung: Implementierung und Optimierung eines kryptanalytischen Angriffs bezüglich Laufzeit/Speicherbedarf.
- Analyse kryptographischer Implementierungen, Reverse-Engineering-Angriffe, Seitenkanalangriffe, Fehlerinjektionsangriffe
  Praktische Übung: Implementierungsangriffe auf ein gegebenes Kryptosystem.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

16

SPAM (Pishing, Social Engeneering) (RUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Die Studierenden haben grundlegende und vertiefende Kenntnisse der E-Mail-Struktur sowie des verwendeten SMTP-Protokolle. Sie sollen die Fähigkeit erhalten, technische Protokolle unter Sicherheitsaspekten zu betrachten. Dem gegenüber sollen die Studierenden aber auch die Grenzen der technischen Sicherheit erkennen und Grundkenntnisse in organisatorischen, juristischen und wirtschaftlichen Alternativen erwerben.

- 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, die Wort-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.

Praktische Übung:
In praktischen Übungen, wie zum Beispiel der Untersuchung und Erweiterung von Anti-Spam Techniken sollen die Studierenden Handlungskompetenzen auf dem Gebiet der IT Sicherheit erwerben.

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	6	6	6	1	0
Fertigkeiten	6	6	6	1	0
Kompetenz	6	6	6	1	0
Über alle Kategorien	6	6	6	3	0

17

Computerstrafrecht (LMU und EKUT)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls haben die Studierenden Kenntnisse über die Grundzüge des Computerstrafrechts und die verschiedenen Facetten der Computer- und Internetkriminalität. Sie sind in der Lage, grundsätzliche Aussagen über das Phänomen Computerkriminalität zu treffen und Einschätzungen hinsichtlich der Strafbarkeit einzelner, damit verbundener Verhaltensweisen abzugeben. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompentenz.

- Das Modul befasst sich in mehreren Studienbriefen mit dem Phänomen der Computerkriminalität. Um die damit auftretenden Probleme richtig einordnen zu können, wird in Studienbrief 1 zunächst ein Mindestmaß an Grundwissen vermittelt. Diese Einführung in das materielle Strafrecht stellt die Basis für die in den weiteren Studienbriefen vertiefte Auseinandersetzung mit den Tatbeständen dar, die üblicherweise unter den Begriff der Computer- und Internetkriminalität subsumiert werden. Die Studienbriefe fassen die damit zusammenhängenden und dahinterstehenden rechtlichen Probleme in Themenkomplexen zusammen. Beispielfälle und Bezugnahmen auf einschlägige Rechtsprechung sollen helfen, die oft abstrakte Materie greifbar und nachvollziehbar zu machen. Die Darstellung erfolgt dabei anhand der einschlägigen Delikte des Strafgesetzbuches sowie einzelner Tatbestände des Nebenstrafrechts, die im Einzelnen näher erklärt und dargestellt werden. Darüber hinaus werden aber auch Grundzüge der mit dem Medium Internet verbundenen verfassungsrechtlichen Fragen sowie rechtliche Rahmenbedingungen für die Anbieter von Inhalten behandelt.

Praktische Übung: Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	1	0
Fertigkeiten	4	4	4	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	4	3	4	3	0

18

Computerstrafprozessrecht (LMU und EKUT)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Die Studierenden erwerben Grundkenntnisse des Strafprozessrechts. Sie können die Grundzüge des Computerstrafprozessrechts in Bezug zur formationstechnologie und zum Verfassungsrecht setzen. Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage, verfahrensrechtliche Maßnahmen auf ihre Zulässigkeit zu überprüfen und hierzu kritisch Stellung zu nehmen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompentenz.

- Das Modul befasst sich in mehreren Studienbriefen mit den Auswirkungen der Informationstechnologie auf das Strafprozessrecht. Unter Bezugnahme auf die im Modul Computerstrafrecht erworbenen materiellrechtlichen Grundkenntnisse werden im Modul grundlegende Kenntnisse im Bereich des Verfahrensrechts und des formellen Strafrechts vermittelt. Auch in diesem Modul wird regelmäßig Bezug auf einschlägige Rechtsprechung genommen und Wert auf eine fallbezogene Wissensvermittlung gelegt. Angesichts der besonderen Bedeutung des Strafverfahrensrechts werden aber auch Grundzüge verfassungsrechtlicher Fragestellungen behandelt.

Praktische Übung: Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	1	0
Fertigkeiten	4	4	4	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	4	3	4	3	0

19

Europäisierung & Internationalisierung des Strafrechts (LMU und EKUT)

(2 Monate / 150 Lernstunden / 5 ECTS)

* Nach erfolgreichem Abschluss des Moduls haben die Studierenden Kenntnisse über die Grundzüge internationalen Rechts und supranationaler Regelungsmodelle. In den Modulen Computerstrafrecht oder Computerstrafprozessrecht erworbene Kenntnisse werden vor diesem Hintergrund neu betrachtet. Die Studierenden sind in der Lage, grundsätzliche Aussagen über die Probleme der internationalen strafrechtlichen Zusammenarbeit zu treffen und die aktuelle Entwicklung kritisch zu hinterfragen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompentenz.
- Das Modul widmet sich in mehreren Studienbriefen dem Prozess der Europäisierung und Internationalisierung des Strafrechts. Die in den Modulen Computerstrafrecht und Computerstrafprozessrecht nur gestreiften Aspekte der zunehmenden Internationalisierung des Strafrechts werden an dieser Stelle vertieft. Die zunehmende Europäisierung des Rechts macht es besonders im Strafrecht notwendig, bisherige nationalstaatliche Regelungsansätze zu überdenken. Dazu ist es unerlässlich, sich auch mit den durch das Europarecht definierten Vorgaben auseinanderzusetzen.

Praktische Übung: Übungsfälle am Ende der Studienbriefe, Kontrollaufgaben

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	4	4	4	1	0
Fertigkeiten	4	4	4	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	4	3	4	3	0

20

Einführung Cyberwar (FUB)

(2 Monate / 150 Lernstunden / 5ECTS)

* Die Studierenden
- verstehen die Grundbedingungen und Inzentive des.
- haben Kenntnisse über die gängigen Definitionen sowie rechtliche und strategische Einordnungen des Cyberwars.
- haben Kenntnisse über militärische Cyber-Angreifer, seine Motive Ressourcen und Optionen und können sie mit anderen Angreifern vergleichen.
- haben die Fähigkeit, proportionale Schutzbedarfe besser ermitteln zu können.
- können militärische und zivile Ziele sowie Operationstypen des Cyberwars nennen.
- haben die besondere Bedeutung des Schutzes der zivilen Informationsgesellschaft und der Wirtschaft erfasst.
- können Strukturmerkmale des Cyberwars in ihrer praktischen Relevanz beurteilen.
- haben Kenntnisse über internationale und nationale Einordnungen und Regulierungen und können ihre Bedeutung für praktische Probleme des IT- Schutzes ermessen.

- Was ist Cyberwar?
- Der militärische Cyber-Angreifer
- Ziele und Operationstypen des Cyberwar
- Merkmale des Cyberwar
- Einordnung des Cyberwar

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	3	3	3	1	0
Fertigkeiten	3	3	3	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	3	3	3	3	0

21

Einführung Cybercrime (FUB)

(2 Monate / 150 Lernstunden / 5ECTS)

* Nach Abschluss diese Moduls sind grundlegende Kenntnisse zu Cybercrime vermittelt. Es ist erklärt, was Cybercrime ist, wie es sich entwickelt hat und entwickeln wird und welche besonderen Bedingungen hier für die Strafverfolgung gelten. Kriminalistische, politische und gesellschaftliche Perspektiven standden dabei im Vordergrund. Der Cyberkriminelle ebenso wie einige Kernmerkmale des Cybercrime sind verstanden. Mit diesem Wissen können folgend Phänomene des Cybercrime eingeordnet und bewertet werden.

- Was ist Cybercrime?
- Der Cyberkriminelle - Ressourcen & Movie
- Cybercrimes
- Merkmale Cybercrime
- Einordnung des Cybercrime

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	3	3	3	1	0
Fertigkeiten	3	3	3	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	3	3	3	3	0

22

Taktik in der IT-Sicherheit 1 (FUB)

(2 Monate / 150 Lernstunden / 5ECTS)

* Nach Abschluss dieses Moduls können die Absolventen taktische Cybersecurity besser verstehen und konzipieren. Sie können eine bessere und umfassendere, in die Zukunft gerichtete Schutzplanung für Unternehmen und Institutionen ausrichten und technische Spezifikationen und Akquisitionen gezielter zu formulieren. Es ermöglicht den Teilnehmern, wie ein Angreifer zu denken und entsprechend Angriffe besser zu detektieren, zu analysieren und zu antizipieren. Das Modul wird zeitaktuell am Stand der Offensivtätigkeiten und -fähigkeiten unterrichtet werden. Es wird technische und nicht-technische Aspekte adressieren. Dieses erste der beiden Taktikmodule wird in die Theorie der Taktik sowie in taktisches Denken einführen.

- Was ist Taktik?
- Taktisches Denken I
- Taktisches Denken II
- Taktisches Denken III
- Taktisches Denken in Cybersecurity

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	3	3	3	1	0
Fertigkeiten	3	3	3	1	0
Kompetenz	3	3	3	1	0
Über alle Kategorien	3	3	3	3	0

23

Taktik in der IT-Sicherheit 2 (FUB)

(2 Monate / 150 Lernstunden / 5 ECTS)

Nach Abschluss dieses Moduls können die Absolventen taktische Cybersecurity besser verstehen und konzipieren. Sie können eine bessere und umfassendere, in die Zukunft gerichtete Schutzplanung für Unternehmen und Institutionen ausrichten und technische Spezifikationen und Akquisitionen gezielter zu formulieren. Es ermöglicht den Teilnehmern, wie ein Angreifer zu denken und entsprechend Angriffe besser zu detektieren, zu analysieren und zu antizipieren. Das Modul wird zeitaktuell am Stand der Offensivtätigkeiten und -fähigkeiten unterrichtet werden. Es wird technische und nicht- technische Aspekte adressieren. Dieses zweite der beiden Taktikmodule wird aufbauend auf den Erkenntnissen des ersten Moduls eine Theorie taktischer Cybersecurity einführen, die eine umfassendere, holistische und nachhaltige Planung von Cybersecurity ermöglichen wird.

- Prinzipien taktischer Cybersecurity
- Defensive Cybertaktik
- Offensive Cybertaktik
- Taktische Planung I
- Taktische Planung II

EQF-Kategorien	MD	Min.	Max.	N	F
Kenntnisse	5	5	5	1	0
Fertigkeiten	5	5	5	1	0
Kompetenz	5	5	5	1	0
Über alle Kategorien	5	5	5	3	0

24	**Informationsethik und Datenschutz für Ermittler und Verteidiger (FUB)** (2 Monate / 150 Lernstunden / 5ECTS) * Nach Abschluss dieses Moduls können die Teilnehmer die ethischen Dimensionen des Handelns von Strafverfolgern oder Verteidigern ethisch besser bewerten und einordnen. Ihnen sind die Werte Sicherheit und Freiheit bekannt und sie sind in der Lage, Konflikte zwischen diesen Werten auch in komplexen technischen Kontexten frühzeitig zu erkennen und zu formulieren. Dabei ist die Kenntnis der Gesetzeslage inbegriffen. - Einführung in die Informationsethik - Informationsethik und Sicherheitsrationalität - Einführung in den Datenschutz - Informationsethik und Datenschutz für kriminalistische Tätigkeiten - Informationsethik und Datenschutz für militärische Tätigkeiten	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse 3 3 3 1 0 Fertigkeiten 3 3 3 1 0 Kompetenz 3 3 3 1 0 Über alle Kategorien 3 3 3 3 0
25	**Cybersecurity aus Sicht der Sicherheitspolitik (FUB)** (2 Monate / 150 Lernstunden / 5ECTS) * Nach Abschluss dieses Moduls haben die Teilnehmer die Grundlagen der Sicherheitspolitik in Anwendung auf die Themen Cyberwar und Cybercrime verstanden. Es wurde vermittelt, in welchen politischen Interessensgefilden und Rahmenbedingungen diese Phänomene stehen, welche Gremien, Nationen und Beschlüsse relevant sind. Damit sind folgend die Bewegungen der Sicherheitspolitik in diesem Bereich besser verständlich und analysierbar. Zudem wird es möglich, abzusehen, wie sich die Cybersicherheitspolitik entwickeln wird. - Cybersecurity und Sicherheitspolitik - Cybersecurity in der Sicherheitspolitik - Regulierung von Cybersecurity - Internationale und nationale sicherheitspolitische Regulierungen - Mögliche Prinzipien einer Cybersicherheitspolitik und zukünftige Herausforderungen	EQF-Kategorien / MD / Min. / Max. / N / F Kenntnisse 3 3 3 1 0 Fertigkeiten 3 3 3 1 0 Kompetenz 3 3 3 1 0 Über alle Kategorien 3 3 3 3 0

Open Competence Center for Cyber Security
TP 2: Anrechnungsanalysen und Anrechnungsmanagement

Dr. Mario Stephan Seger
Institut für Soziologie der TU Darmstadt
Residenzschloss
64283 Darmstadt

Tel.: 0 61 51 – 16 67 59
E-Mail: seger@ifs.tu-darmstadt.de

Gefördert vom:
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
AUFSTIEG DURCH BILDUNG >> OFFENE HOCHSCHULEN