Cyber-Sicherheit (M.Sc.)

Studiengang:	Cyber-Sicherheit
Fakultät:	Informatik
Abschluss:	Master of Science (M.Sc.)
Studienform:	Vollzeit, Präsenzstudium
Unterrichtssprachen:	Deutsch und Englisch
Studienbeginn:	Wintertrimester
Regelstudienzeit:	21 Monate
Kontakt Fachstudienberatung:	Studiendekan Informatik

I) Studiengangbeschreibung

Der Informationssicherheit kommt eine Schlüsselrolle bei der Konzeption und Entwicklung sowie beim Betrieb von technischen Systemen und komplexen IT-Infrastrukturen zu. Vom Smart Home über medizinische Implantate und industrielle Produktionsanlagen bis hin zu unternehmenskritischen, softwaregestützten Geschäftsprozessen findet eine globale Vernetzung statt, die mit vielfältigen Angriffsmöglichkeiten und einem nach wie vor anhaltenden Defizit an IT-Sicherheitsmaßnahmen einhergeht.

Der Studiengang Cyber-Sicherheit befasst sich mit Informationsverarbeitungsprozessen, deren Planung, formaler Modellierung, Implementierung und Einsatz mit einem Fokus auf technische und organisatorische Informationssicherheit. Neben fundierten theoretischen Methoden werden insbesondere auch praxisrelevante Fähigkeiten, u.a. zur Identifizierung und Beseitigung von sicherheitsrelevanten Schwachstellen, zur Entwicklung und Implementierung von Sicherheitskonzepten und zur Erkennung und Abwehr von Angriffen auf IT-Systeme vermittelt. Zudem werden beispielsweise rechtliche und ethische Fragestellungen sowie ausgewählte Themen rund um den Faktor Mensch in der Informationssicherheit behandelt.

Der Master-Studiengang bereitet auch auf eine weiterführende wissenschaftliche Beschäftigung mit der Informationssicherheit vor, zum Beispiel im Rahmen einer Promotion.

II) Studienvoraussetzungen

Für den Master-Studiengang sind solide Kenntnisse in den Standardbereichen der Informatik und insbesondere in den mathematischen Methoden erforderlich, wie sie beispielsweise im Bachelor-Studiengang Informatik an der Universität der Bundeswehr München vermittelt werden. Darüber hinaus werden gute Deutsch- und Englischkenntnisse in Wort und Schrift vorausgesetzt; einige Lehrveranstaltungen werden auf Englisch abgehalten, zudem wird die Lektüre englischer Fachbücher und wissenschaftlicher Veröffentlichung erwartet.

Darüber hinaus werden sehr gute Grundkenntnisse in folgenden Bereichen empfohlen:

- Betriebssysteme und Rechnernetze
- Lineare Algebra und Mathematische Strukturen
- Maschinennahe Programmierung und imperatives Programmieren in Hochsprachen
- Rechnerarchitektur und Digitaltechnik

Ein (Vor-)Praktikum ist für die Aufnahme des Studiums nicht erforderlich. Es ist aber hilfreich, sich im Rahmen eines freiwilligen Praktikums oder Projektes (z.B. während des Bachelor-Studiums) schon mit den Anforderungen realer Einsatzszenarien auseinandergesetzt zu haben.

Zur Vorbereitung auf das Studium wird empfohlen, Informatik- und Mathematik-Inhalte aus dem Bachelor-Studium zu wiederholen bzw. zu ergänzen.

III) Fähigkeiten und Neigungen

Die entscheidenden Voraussetzungen sind die Fähigkeit zum strukturierten, abstrakten Denken und der kreative Umgang mit Softwaresystemen. Wer Spaß am Programmieren und Fehlersuchen hat, gerne selbst verteilte Systeme betreibt und analysiert sowie ein vertieftes Interesse an den mathematischen Konzepten hinter Kryptographie und Datenanalyse hat, bringt auf jeden Fall beste Voraussetzungen für das Studium mit.
Informationssicherheit betrifft aber auch die ingenieurmäßige Konstruktion von Systemen für Anwender. Daher sind Kommunikations- und Präsentationsfähigkeiten gefragt, um ein System im Dialog mit den Anwendern zu

Studieninformationen – Universität der Bundeswehr München

ihrem Nutzen zu entwickeln. Auch die gesellschaftlichen, psychologischen, ökonomischen und politischen Voraussetzungen und Wirkungen der Systeme sind zu betrachten. Schließlich ist auch Teamfähigkeit eine wichtige Eigenschaft.

Zudem ist Informationssicherheit ein Gebiet mit sehr hoher Änderungsgeschwindigkeit. Wichtig ist daher die Bereitschaft, sich immer wieder mit neuen Themen zu befassen und sich die erforderlichen Fähigkeiten anzueignen.

IV) Aufbau des Studiengangs

Am Anfang des Master-Studiums sind Veranstaltungen in Kerngebieten der Informationssicherheit zu belegen. Auf technischer Ebene gehören hierzu Kryptologie sowie Netz-, System-, Anwendungs- und Hardwaresicherheit. Pflichtmodule aus dem Bereich der organisatorischen Informationssicherheit umfassen Datenschutz und Privacy sowie Security- und IT-Management.

Für die übrigen Inhalte können Module aus einem großen Wahpflichtangebot gewählt werden. Es kann auch eines der folgenden drei Vertiefungsfelder gewählt werden:

- Enterprise Security
- Public Security
- Security Intelligence

Praktika sind sowohl im Pflicht- als auch im Wahlpflichtbereich zu belegen. Hinzu kommen ein Seminar sowie die Master-Arbeit, deren Bearbeitungszeit in der Regel fünf Monate beträgt.

V) Berufsbilder

Absolventinnen und Absolventen des Master-Studiengangs Cyber-Sicherheit sind vielseitig in allen Bereichen von Bundeswehr, Behörden, Wirtschaft und Gesellschaft einsetzbar, die in besonderem Maße auf die Vertraulichkeit, Integrität und Verfügbarkeit der eingesetzten IT-Dienste und verarbeiteten Daten angewiesen sind. In der Praxis werden sie sich mit der Konzeption, Planung, Realisierung, Überprüfung, Modifikation und Wartung von informationsübertragenden und -verarbeitenden Systemen mit einem Fokus auf die charakteristischen Sicherheitsaspekte in jeder Lebenszyklusphase der IT-Systeme befassen. Dabei kann es sich um Waffeneinsatz-Systeme und Führungsinformationssysteme der Bundeswehr handeln, um multimediale Kommunikationssysteme in Unternehmen, in Staaten oder rund um den Globus, oder um Steuerungssysteme für Maschinen, Industrieanlagen, Verkehr oder die Vermittlung von Telefongesprächen. Auch in den kleinen Dimensionen breiten sich Einsatzgebiete für Cyber-Sicherheit rapide aus: Smartphones, Smartwatches, Mobile Computing und medizinische Körpersonden und andere eHealth-Anwendungen weisen einen hohen Schutzbedarf auf.

Konkrete Berufstätigkeiten sind:

- Entwicklung sicherer Systeme und Anwendungen zur Datenverarbeitung und deren Betrieb,
- Einführung und Erneuerung von IT-Infrastrukturen in Umgebungen mit erhöhtem Schutzbedarf,
- Analyse und Verbesserung bestehender IT-Infrastrukturen unter IT-Sicherheitsaspekten,
- Angriffsprävention, Einsatz von Detektionsmechanismen und Reaktion auf Sicherheitsvorfälle,
- Tätigkeiten in verschiedenen Ausbildungsinstitutionen, einschließlich Lehre und Forschung.

Absolventen des Master-Studiengangs werden verstärkt im akademischen Bereich und in leitenden Funktionen in IT-Abteilungen eingesetzt.

VI) Weiterführende Information

Für weitere Informationen zum Studium an der Universität der Bundeswehr München allgemein besuchen Sie bitte die Seite www.unibw.de/studienberatung.