Technische Hochschule
Brandenburg
University of
Applied Sciences

„Master ohne Bachelor – jetzt durchstarten!“

Informationsveranstaltung zum Quereinstieg für Meisterinnen und Meister in den Studiengang Security Management

Begrüßung

Prof. Dr. Andreas Wilms
Vizepräsident für Lehre und Internationales

Technische Hochschule Brandenburg
University of Applied Sciences

Projekt MasterPlan: Bachelor ohne Master

Katharina Lenz
Akademische Mitarbeiterin im Projekt MasterPlan

LAND BRANDENBURG
Ministerium für Wissenschaft, Forschung und Kultur

EUROPÄISCHE UNION
Europäischer Sozialfonds

Gefördert durch das Ministerium für Wissenschaft, Forschung und Kultur aus Mitteln des Europäischen Sozialfonds und des Landes Brandenburg

Projekt MasterPlan: Bachelor ohne Master

Ziel des Pilotprojekts

- Entwicklung und Erprobung eines Verfahrens zur Kompetenzfeststellung für Personen ohne ersten berufsqualifizierenden Hochschulabschluss für den Zugang zu einem Masterstudiengang

Hintergrund

- Förderung der Durchlässigkeit ins Hochschulsystem
- 9 Abs. 5 Brandenburgisches Hochschulgesetz

Pilotstudiengang

- Besonderer weiterbildender Masterstudiengang Security Management (M. Sc.)

Projektphasen

Zielgruppe

Beruflich qualifizierte Personen mit…

- erfolgreich abgeschlossener, einschlägiger Aufstiegsfortbildung (Meisterprüfung oder ähnliche Prüfung) und
- mind. einem Jahr einschlägiger Berufserfahrung

Eingangsprüfung

1. Bewerber-portfolio

2. Zugangs-arbeit

3. Verteidigung und Interview

Obligatorische Vorkurse

Rahmenbedingungen

Förderung

- Gefördert durch das Ministerium für Wissenschaft, Forschung und Kultur aus Mitteln des Europäischen Sozialfonds und des Landes Brandenburg

LAND BRANDENBURG
Ministerium für Wissenschaft, Forschung und Kultur

EUROPÄISCHE UNION
Europäischer Sozialfonds

Kosten

- Die Teilnahme an der Eingangsprüfung ist im Rahmen des Projekts MasterPlan kostenlos
- Für die Teilnahme ist eine Einwilligung zur Datenerhebung im Rahmen des ESF 2014 – 2020 notwendig

Masterstudiengang Security Management: Informationen zu Inhalten und Aufbau

Prof. Dr. Ivo Keller
Studiengangsleiter Security Management

Technische Hochschule
Brandenburg
University of
Applied Sciences

Security Management (M.Sc.) Studiengang

Brandenburg, 28.6.2017

Prof. Dr. Ivo Keller
Studiendekan
Security Management

Ivo.keller@th-brandenburg.de
03381 355-278

Organisatorisches zum Studiengang

Vorlesungen in Modulen, jeweils

freitags	8:30 bis 18:00
samstags	8:30 bis 16:00
montags	8:30 bis 18:00

Aufbau des Studiengangs

ITK-Security
(SSLM, IKT 1 und 2)

Mathematische und physikalische Grundlagen
(Netzwerk, Krypto, Forensik)

Recht und BWL
(Recht, Physical, U-Führung)

Security Management
(GL-SecMan, SecMan International)

Vertiefungen
(WPF)

Wiss. Arbeiten & Schreiben
(Semesterarbeiten 1 und 2, Projekt)

Verteilung der Module in Vollzeit

Sem.	Modul							∑ CP
1	Grundlagen des Security Managements (6CP)	Recht, Compliance und Datenschutz (6CP)	Sichere IKT-Infrastrukturen und IT-Dienste (6CP)	Mathematisch-technische Grundlagen der IT-Sicherheit (6CP)	Netzwerksicherheit (6CP)	Wissenschaftliches Schreiben (6CP)		30
2	Security- und Krisenmanagement im internationalen Kontext (6CP)	Organisatorische Aspekte des Sicherheitsmanagements (6 CP)		Secure Software Lifecycle Management (6CP)	Projekt (6CP)			30
3	Wahlpflichtmodul 1 (3CP)	Wahlpflichtmodul 2 (3CP)		Wahlpflichtmodul 3 (3CP)				9
	Masterarbeit incl. Kolloquium (21CP)							21
								90

Verteilung der Module in Teilzeit

Sem.	Module			ECTS
1	Grundlagen des Security Managements (6CP)	Mathematisch-technische Grundlagen der IT-Sicherheit (6CP) (Krypto und Forensik)	Sichere IKT – Infrastrukturen und IT-Dienste (6CP)	15
2	Security- und Krisenmanagement im internationalen Kontext (6CP)	Organisatorische Aspekte des Sicherheitsmanagements (6 CP) (Physical Security und Unternehmens-Führung)		15
3	Netzwerksicherheit (6CP)	Recht, Compliance und Datenschutz (6CP)	Wissenschaftliches Schreiben (6CP)	15
4	Secure Software Lifecycle Management (6CP)	Projekt (6CP)		15
5	Wahlpflichtmodul 1 (3CP)	Wahlpflichtmodul 2 (3CP)		6
	Masterarbeit incl. Kolloquium (21CP)			
6	Wahlpflichtmodul 3 (3CP)			24
				90

Pflichtmodule

- Security- und Krisen-Management, generell und international
- Sichere IKT-Infrastrukturen und IT-Dienste
- Organisatorische Aspekte des Security Management
  - Recht
  - Unternehmensführung
  - Physische Sicherheit im Unternehmen
- Netzwerksicherheit
- Kryptographie
- Forensik
- Secure Software Lifecycle Management (SSLM)
- Wissenschaftliches Schreiben
- Projekt

Lehrende aus der Praxis – unsere Honorarprofessoren

Prof. Dr. Heinz-Dieter Schmelling

Praxis: Chief Security Officer Portigon AG

Lehre: Grdl. SecMan und SecMan im internationalen Kontext

Prof. Dr. Eberhard von Faber

Praxis: Chief Security Advisor T-Systems

Lehre: Sichere IKT-Infrastrukturen und IT-Dienste

Prof. Dr. Igor Podebrad

Praxis: Bereichsleiter Threat Defense in der Commerzbank

Lehre: IT-Forensik

Prof. Dr. Oliver Weissmann

Praxis: XIV-Consult

Lehre: Unternehmensführung/ Business Continuity Management

Kooperationspartner des Studiengangs

Fraunhofer

T · · Systems ·

COMMERZBANK

GRS Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Dussmann Group

VICCON GMBH CONSULTING

Deloitte.

ZAB Brandenburg Economic Development Board

HISOLUTIONS

Gegenbauer

DIE STADT IM FLUSS BRANDENBURG AN DER HAVEL

TELCO TECH NETWORK SECURITY ENGINEERED IN GERMANY

VALORA Consulting

codenomicon

SecurIntegration

iSQI

RITTAL

Profilrichtungen

- Informationssicherheit,
- IT-Forensik,
- Business Continuity und Krisen-Management,
- IT und Cyber Security,
- Bankensicherheit und
- Gebäude-, Anlagen- und Personensicherheit

Auszug aus den Wahlpflichtmodulen

- Datenschutz in der vernetzten Welt
- Predictive Analytics
- Business Continuity Management (BCM)
- Risikoanalysen und Risikomanagement
- Information Security Management System (ISMS)
- Sicherheit von Rechenzentren
- Social Engineering
- Penetration Test
- Payment Card Industry Data Security Standard (PCI DSS)
- KRITIS - Sicherheitsanforderungen an kerntechnische Anlagen
- Cybersecurity/Cyberwar
- Technische Aspekte der IT-Forensik
- IT Infrastructure Libary (ITIL)

Beispiel Predictive Analytics

Ziel:

Kompetenz im Umgang mit

- Methoden zur Verarbeitung von Prozessdaten, Benutzerverhalten und Meinungen
- Visualisierungstools (z.B. Rapid Miner)

Inhalte:

- Aufbereitung nicht-numerischer Daten aus heterogenen Quellen (Big Data)
- Maschinelles Lernen, Clusterung und Visualisierung am Beispiel Fraud im Onlinehandel

Beispiel Datenschutz in der vernetzten Welt

Ziel:

- Nutzer-zentrierte Datenhaltung, minimal erforderliche Daten bei gleichem Nutzen

Inhalte:

- Tools zur Textindexierung (z.B. Solr/Lucene)
- Verantwortung der Datenverarbeitung
- Datensicherheit als Voraussetzung für unternehmerische Existenz
- Sicheres Agieren in Cloud und Web 2.0
- Nachhaltige Compliance, serviceorientierte Organisation und Datensouveränität, technische Umsetzung von 80-/20-Prinzipien

Beispiel Penetration Testing

Themen

- Kenntnisse über potenzielle Cyber-Risiken
- Angreifertypen: Von Script Kiddies bis Advanced Persistant
- Rechtliche Rahmenbedingungen, Dokumentation und Handlungsempfehlungen
- Testverfahren und Aggressivität
- Vorstellung gängiger Hacking Tools (Nmap, OWASP Zed, Metasploit, Nessus u.a.)
- Live-Hacking
- Durchführung eines Penetrationstests
- Fundierte Einschätzung der Ergebnisse

Beispiel Sichere Rechenzentren

Ziel:

- Besondere Anforderungen an die Sicherheit und Verfügbarkeit von Rechenzentren

Inhalte:

- Auswirkung von organisatorischer, technischer, Planung, Konzeption und Auslegung von Rechenzentren
- Lage und Architektur
    - Kühlungsoptionen
    - Aktiver und passiver Brandschutz
- BSI-Grundschutz, Risikoanalysen von Rechenzentren und Bitkom-Leitfäden, Geheimschutz der Wirtschaft sowie Zertifizierungen (BSI, TÜV, ECB-S, eco) von Rechenzentren

Beispiel Cyber Security

Ziel:

- Bedrohungen durch Cyberwar und die Wirksamkeit von Gegenmaßnahmen einschätzen können.

Inhalte:

- Spezifika des Cyberwar im Vergleich zu anderen Manipulationsformen
- Cyberwar als Herausforderung für das Sicherheitsmanagement
- Cyberwar und der Schutz von KRITIS
- Cyberwar aktuelle Fälle und Angriffstechniken
- Cyberdefence-Strategien im Vergleich

Beispiel ITIL

Ziel:

- Anwenden des ITIL-Modells
- Bewerten von Unternehmens- und Sicherheitsprozessen

Inhalte:

Einführung in ITIL

- ITIL-Modell
- Praxisszenarien
- 5 Phasen des ITIL-Lebenszyklus‘
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation und
  - Continual Service Improvement

Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Vielen Dank für die Aufmerksamkeit

Viel Erfolg beim Studium

Technische Hochschule Brandenburg
University of Applied Sciences

„Master ohne Bachelor – jetzt durchstarten, aber wie?“

Voraussetzungen für die Eingangsprüfung, Ablauf des Brückensemesters

Dr. Christine Tschöll
Akademische Mitarbeiterin im Projekt MasterPlan

LAND BRANDENBURG
Ministerium für Wissenschaft, Forschung und Kultur

EUROPÄISCHE UNION
Europäischer Sozialfonds

Gefördert durch das Ministerium für Wissenschaft, Forschung und Kultur aus Mitteln des Europäischen Sozialfonds und des Landes Brandenburg

Inhalt

A Die Eingangsprüfung

B Zugangsvoraussetzungen

C Aufbau der Eingangsprüfung

D Anmeldung und Bewertung

E Termine

F Immatrikulation Master Security Management

G Beratung

A Die Eingangsprüfung

Durch die Eingangsprüfung soll festgestellt werden, ob die berufliche Qualifikation der Bewerberinnen und Bewerber als Zugangsvoraussetzung mit der eines für den Studiengang relevanten **(Bachelor-)Abschlusses gleichwertig** ist.

Es ist keine Prüfung im eigentlichen Sinn, vielmehr stellen die Quereinsteigerinnen und Quereinsteiger **innerhalb eines Brückensemesters ihre Fähigkeiten für ein Studium unter Beweis**.

B Zugangsvoraussetzungen

Zur Eingangsprüfung kann zugelassen werden, wer

1. eine **berufliche Weiterqualifikation** durch einschlägige **Meister- oder vergleichbare Prüfung** abgeschlossen hat (beispielsweise geprüfter Meister für Schutz und Sicherheit, geprüfter IT-Projektleiter, geprüfter Industriemeister Elektronik u.v.m) und

2. den Nachweis über eine **einschlägige berufspraktische Erfahrung** von mindestens **einem Jahr** im Anschluss an die Meisterprüfung erbringt.

C Aufbau der Eingangsprüfung

Die Eingangsprüfung besteht aus:

1. **der Prüfung des Bewerberportfolios,**
2. **einer Zugangsarbeit,**
3. **einer Verteidigung mit Interview sowie**
4. **obligatorischen Vorkursen.**

D Eingangsprüfung: Anmeldung und Bewertung

Die Zulassung zur Eingangsprüfung erfolgt auf **Antrag** an den „Ausschuss für den Zugang zum Studiengang Security Management" (Zulassungsausschuss). Dieser wird (inklusive aller notwendigen Unterlagen) **schriftlich beim Studierendensekretariat** der Technischen Hochschule Brandenburg (THB) eingereicht.

Die **Bewertung** erfolgt entlang der Kompetenzdimensionen des **Eingangskompetenzprofils Security Management** (EKP SecMan) mithilfe eines Punktesystems.

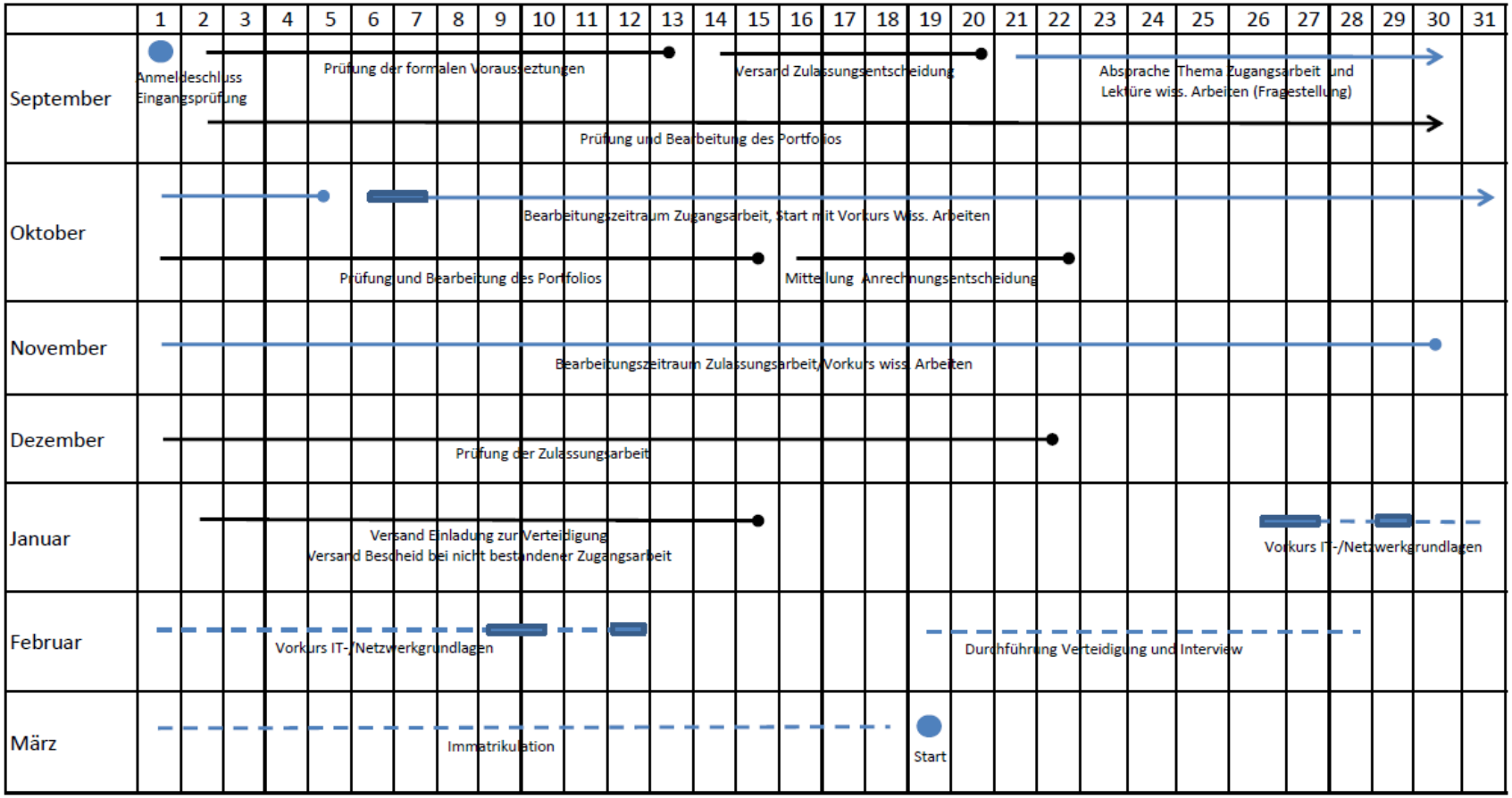
E Termine

- Die Eingangsprüfung findet **einmal im Semester** statt:
  - Wintersemester: Anmeldung jeweils **bis zum 1. September**
  - Sommersemester: Anmeldung jeweils **bis zum 1. März**

- Der zeitliche Ablauf kann dem **Terminplan** für das jeweilige Semester entnommen werden.

E Termine

Technische Hochschule Brandenburg
Terminplan Eingangsprüfung Security Management, Wintersemester 2017/18



Vorlesungszeit SoSe 18: Mo, 19.03.2018 bis Sa, 30.06.2018

F Immatrikulation Master Security Management

- **Nach Erhalt der Bescheinigung** über die bestandene Eingangsprüfung können sich die Quereinsteigerinnen und Quereinsteiger **im regulären Verfahren** um einen Studienplatz für den Masterstudiengang **Security Management** bewerben.

- Die Bescheinigung über die **bestandene Eingangsprüfung** tritt dabei **an die Stelle des Hochschulzeugnisses**.

G Beratung

Wir stehen Ihnen gerne zur Verfügung:

- Für Fragen zum **Zugang für Studieninteressierte ohne ersten berufsqualifizierenden Hochschulabschluss**

  Katharina Lenz, M.A.

  Dr. Christine Tschöll

- Bei Fragen zu Inhalten und Organisation des **Masterstudiengangs Security Management**

  Prof. Dr. Ivo Keller

  Annegrit Seyerlein-Klug

Fragen, Anmerkungen, Unklarheiten?

Kontakt

Projekt MasterPlan

Katharina Lenz und Dr. Christine Tschöll

E-Mail: masterplan@th-brandenburg.de

Tel.: 03381 355 – 796/788

Studiengang Security Management

Prof. Dr. Ivo Keller und Annegrit Seyerlein-Klug

E-Mail: secman@th-brandenburg.de

Tel.: 03381 355 – 278/290

Technische Hochschule
Brandenburg
University of
Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit