

Pressemitteilung

Wilhelm Büchner Hochschule

Miriam Thomi

30.04.2025

<http://idw-online.de/de/news851369>

Studium und Lehre
Informationstechnik
überregional



Safety first! Cyber Security an der WBH

Cyberkriminelle stellen Unternehmen, Behörden und Organisationen regelmäßig vor neue Herausforderungen. Wir machen Studierende zur Fachkraft für Cyber-Security!

Das Studienangebot der Wilhelm Büchner Hochschule umfasst mehrere Studiengänge im Bereich Cyber Security und deckt damit die Nachfrage von Interessierten eines Bachelor- bzw. Master-Studiengangs oder komprimierter Weiterbildungen ab.

Bachelor in IT-Sicherheit – im Fernstudium und Online-Abendstudium

Der Studiengang erstreckt sich regulär über sechs Semester und vermittelt das notwendige Know-how, um diese immerwährende Gefahr im Blick zu haben und im Fall der Fälle reagieren zu können. Der Studiengang setzt sich aus umfassenden Kompetenzen in der klassischen Informatik und neuesten Erkenntnissen der Cybersicherheit zusammen. Dabei gliedert sich das Studium in Grundlagen- und Kernstudium und deckt insgesamt fünf Studienbereiche ab: Informatik-Grundlagen, Mathematik, Technik, Betriebssysteme, IT Security.

Das Studium enthält zwei Wahlpflichtbereiche: im 1. Wahlpflichtbereich wählen Sie 2 aus 20 der angebotenen Module in den Themenbereichen Wirtschaft / Überfachliche Kompetenzen, Informatik / Medieninformatik und Technische Informatik, im 2. Wahlpflichtbereich 1 aus 7 Modulen.

Mit dem hinzugewonnenen Know-how, sind Absolvent:innen des Studiengangs branchenübergreifend gefragte IT-Fachkräfte:

- in IT-Abteilungen von Unternehmen (Start-up, Mittelstand, Konzern)
- in Entwickler- und Anwenderunternehmen von Software-Produkten
- in staatlichen Einrichtungen (Ministerien, Behörden, Archiven)
- in Unternehmensberatungen mit IT-Schwerpunkt
- in Forschungs- und Entwicklungseinrichtungen

Cyber Security Management (MBA)

Beim zweisemestrigen MBA-Studiengang erhalten Studierende einen tiefergehenden Überblick über den Entwurf, die Entwicklung, die Auswahl und die Nutzung von IT-Sicherheitsarchitekturen, IT-Sicherheitsverfahren und -technologien im Unternehmen. Sie lernen das organisatorisch-technische Konzept des Information Security Management System (ISMS) nach den in der Praxis wesentlichen Standards wie ISO/IEC 27001 kennen, das die Informationssicherheit über alle Ebenen eines Unternehmens hinweg sicherstellt. In Kombination mit den Studieninhalten „Information Governance“, „Economics“ und „Risk Management“ wird das entsprechend vertiefte Wissen in Verbindung mit dem ISMS-Konzept praktisch umsetzbar.

Ein weiterer Bestandteil des MBA ist die Vermittlung moderner Methoden zum Management von IT-Sicherheitsrisiken und zur Gestaltung einer sicheren IT-Landschaft. Dabei wird deutlich, dass für ein gelungenes IT-Sicherheitskonzept das optimale Zusammenspiel des IT-Sicherheits-Managements und der technischen Sicherheit mit einer gelebten Sicherheitskultur unabdingbar ist.

Absolvent:innen des MBA-Studiengangs, der sich vornehmlich an Berufserfahrene richtet, sind dank des erlangten Know-hows in der Lage, entsprechende Projekte zu leiten, und können die erlernten Konzepte und Methoden auf zukünftige Entwicklungen im Bereich Cyber Security Management übertragen. Projekt- und Forschungsarbeiten sowie Fachseminare stärken dabei die Soft Skills und die Persönlichkeitsentwicklung auch im Umgang mit gesellschaftlichen Randbedingungen. Das Skill-Set des MBA-Studiengangs „Cyber Security Management“ qualifiziert Absolvent:innen für leitende Positionen wie die des Chief Information Security Officer.

Master in Cyber Security (M. Sc.)

Der Master „Cyber Security“ ist in der drei- und viersemestrigen Variante studierbar. Der Studiengang vermittelt vertiefte und erweiterte Kenntnisse der Cyber Security, u. a. in den Bereichen angewandte Kryptografie, Sicherheitsprotokolle, Identity Management, Cybercrime. Neben der Theorie werden Angriffs- und defensive Verteidigungstechniken – in Red und Blue Teams – im Labor praktisch geübt. Dabei werden sowohl die Techniken der Angreifer als auch Abwehr und forensische Analyse von fortgeschrittenen Cyberangriffen behandelt. Beide Perspektiven sind notwendig, um das gesamte Feld der Cyber Security zu erfassen und entsprechende Maßnahmen der Verteidigung ergreifen zu können.

Im Rahmen praktischer Übungen haben Studierende die Gelegenheit, ihr erworbenes Wissen anzuwenden. Dies geschieht in einem virtuellen Labor, in dem ein Angriffsteam „Red Team“ und ein Verteidigungsteam „Blue Team“ gebildet wird. Beide Teams wenden ihre erworbenen Kenntnisse in einem konkreten Fallbeispiel an. In einem Assessment im „Purple Team“ werden die Ergebnisse reflektiert. Darüber hinaus werden im Masterstudiengang überfachliche Kompetenzen wie Forschungsmethoden und Projektmanagement vermittelt, und Studierende erhalten die Gelegenheit, speziell gewählte Themen in Forschung und Projektarbeit zu vertiefen.

Der Studiengang qualifiziert Absolvent:innen für die Rolle als Sicherheitsspezialist:in und für leitende Funktionen, zum Beispiel im Rahmen eines Security Operations Center (SOC).

Weiterbildungen in IT-Sicherheit:

Hochschulzertifikat auf Bachelor-Niveau: IT-Sicherheit

Nano Degree auf Bachelor-Niveau: Einführung in die IT-Sicherheit

Nano Degree auf Bachelor-Niveau: IT-Sicherheit-Management

Nano Degree auf Master-Niveau: IT-Security-Management

Tipp: Absolvent:innen eines der genannten Nano Degrees können sich die erlangten Verrechnungspunkte komplett (6 VP von insgesamt 6 erlangten VP), Absolvent:innen des Hochschulzertifikats nahezu komplett (24 VP von insgesamt 30 erlangten VP) auf den Bachelor-Studiengang IT-Sicherheit anrechnen lassen.

URL zur Pressemitteilung: <https://www.wb-fernstudium.de/ueber-uns/hochschule/news-presse-termine/detail/safety-first-cyber-security-an-der-wbh.html?referrer=idw.online>

URL zur Pressemitteilung: <https://www.youtube.com/watch?v=MJWw3OJz48E> Bachelor IT-Sicherheit

URL zur Pressemitteilung: <https://www.youtube.com/watch?v=JdVWjhl9jXk> Master Cyber Security



Cyber Security an der WBH