DHBW CAS
Duale Hochschule
Baden-Württemberg
Center for Advanced Studies

**TERMINE**
**jeweils 10.00–17.00 Uhr**

**T3M40304 IT-Sicherheit**
07.04. – 09.04.2022 (S) und 09.05 – 11.05.2022 (S)

**W3M20014 IT-Security Cryptography and Secure Communications**
10.10. – 12.10.2022 (MA) und 03.11. – 05.11.2022 (S)

**W3M20015 IT-Information Security Management**
07.04. – 09.04.2022 (MA) und 09.05 – 11.05.2022 (MA)

**W3M20016 IT-Security Secure Software Engineering in Business Computing**
20.06. – 22.06.2022 (HN) und 28.07. – 30.07.2022 (online)

**W3M20017 IT-Security Attack and Defense**
02.02. – 04.02.2023 (MA) und 06.03. – 08.03.2023 (MA)

**W3M20021 Information Technology Law and Ethics**
31.01. – 02.02.2022 (online) und 10.03. – 12.03.2022 (online)

## KOSTEN

Preis pro Modul zwischen 1.300 € und 1.550 €
zzgl. Prüfungsgebühr 80 €

## VERANSTALTUNGSORTE

DHBW Center for Advanced Studies
Bildungscampus 13
74076 Heilbronn

(oder wie in Klammern angegeben)

## MODULANMELDUNG

DHBW Center for Advanced Studies
Wissenschaftliche Weiterbildung

**www.wissenschaftliche-weiterbildung.dhbw.de/abwehr-von-cyber-risiken**

Ansprechpartner:
Bernd Stadtmüller
Tel.: +49 (0) 7131.3898 - 325
E-Mail: weiterbildung@cas.dhbw.de

1. Auflage, Januar 2022 Fotografie: Adobe Stock

# *Abwehr von Cyber-Risiken*

**Zertifikatsprogramm**

**Ein wissenschaftliches Weiterbildungsangebot des Center for Advanced Studies der Dualen Hochschule Baden-Württemberg (DHBW CAS).**

Der Raub wertvoller Kundendaten, Betriebsspionage, Erpressung – Unternehmen, Organisationen und einzelne User stehen weltweit durch Cyberkriminalität unter permanentem Beschuss. Moderne IT-Sicherheit bietet Schutz und ist eines der wichtigsten Einsatzgebiete der Informatik – Schutzwall und Speerspitze im Kampf um Datenschutz und Informationssicherheit zugleich. Wollen Sie, ausgestattet mit aktuellstem Expertenwissen, dafür sorgen, dass Unternehmen und Menschen in Zukunft vor Cyber-Attacken sicher sind? Dann nutzen Sie jetzt die hochwertigen Ressourcen unseres Zertifikatsprogramms Cyber Security.

## KNOW-HOW UND TOOLS ZUM SCHUTZ VOR CYBER-ATTACKEN

Der Wettlauf mit der Cyberkriminalität hat der „Verfolgungsjagd mit Blaulicht“ eine neue Dimension eröffnet. Wer auf dem Gebiet der Cyber Security über Fachwissen verfügt, bewegt sich in einer spannenden Themen-Matrix und besitzt beste Karriere-Chancen. Unser Zertifikatsprogramms Cyber Security stattet Sie mit dem neuesten Know-how zum Schutz und zur Abwehr von Cyber-Attacken aus und schult Sie im Umgang mit den modernsten Tools. Sie lernen wie Sie Bedrohungsszenarien begegnen, Schwachstellen identifizieren und Gegenmaßnahmen ergreifen, wie sicheres Software-Engineering funktioniert und wie Sie rechtliche und soziale Aspekte managen.

## KOMPETENZ PLUS ECTS-PUNKTE

Tool für Tool, Modul für Modul erweitern Sie mit unserem Zertifikatsprogramm Cyber Security Ihre IT-Kompetenz. Und davon profitieren Sie gleich doppelt: Sie erwerben wertvolles Wissen für Ihre unmittelbare berufliche Anwendung und sammeln ECTS-Punkte für die Perspektive eines späteren Masters. Sie wählen Module für Ihr Berufsbild ganz gezielt aus und bauen neues Know-how Schritt für Schritt auf. Damit ist unser Lernangebot mehr als ein einfaches Weiterbildungsseminar – es ist für Sie ein wichtiger Baustein Ihrer Karriere mit bleibendem Wert.

## ZIELGRUPPE

Sie sind Fach- oder Führungskraft im Unternehmen und wollen Fähigkeiten auf dem Gebiet der Cyber Security auf- und ausbauen? Dann sind bei uns genau richtig.

## ERWEITERBAR ZUM MASTER

Nach bestandener Modulprüfung erhalten Sie 5 ECTS pro Modul, die das DHBW CAS bei Interesse und Vorliegen der hochschulrechtlichen Voraussetzungen gern für seine ingenieurswissenschaftlichen Master-Studiengänge anerkennt.

## TEILNAHMEVORAUSSETZUNG

Neben Lust auf Mehr-Wissen und neue Erfahrungen brauchen Sie zur Teilnahme den Abschluss eines Hochschulstudiums oder alternativ die erforderliche Eignung im Beruf.*

*Die Mindestqualifikation entspricht dem Niveau 6 des Deutschen Qualifikationsrahmens.

### IT-SICHERHEIT

- Grundlagen IT-Sicherheit
- Bedrohungsszenarien
- Sicherheitsziele
- Schwachstellen
- Gegenmaßnahmen
- Methoden
- Werkzeuge
- rechtliche und betriebswirtschaftliche Aspekte
- Sicherheitsmanagement

### IT-SECURITY CRYPTOGRAPHY AND SECURE COMMUNICATIONS

- Grundprinzipien der Kryptographie
- Verschlüsselung
- digitale Signaturen und Zertifikate
- Netzwerk- und Transportsicherungsprotokolle
- Implementierung
- Datenintegrität
- Infrastrukturen für Public-Key-Verfahren

### INFORMATION SECURITY MANAGEMENT

- Prozesse
- Policies
- Procedures
- Sicherheitsmodelle
- Performance Management
- Sicherheitsmanagement
- Risk Management
- Compliance und Assessment

### IT-SECURITY SECURE SOFTWARE ENGINEERING IN BUSINESS COMPUTING

- Designprinzipien
- Bewertungskriterien
- Seitenkanäle
- Technologie- und Methodenauswahl
- Software-Audits
- Buffer-Overflow-Problematik
- Zugangsschutz
- Validierung
- Passwörter und alternative Verfahren

### IT-SECURITY ATTACK AND DEFENSE

- Angriffsvektoren
- typische Einbruchsszenarien
- Schutzmaßnahmen
- Schutzsysteme
- Spuren lesen, Beweise sichern
- Schwachstellen finden
- Maßnahmen zur Sicherung

### INFORMATION TECHNOLOGY LAW AND ETHICS

- IT-Recht
- Schutz digitaler Werke
- Vertragsrecht
- Internetrecht
- Strafrecht
- Datenschutz
- Wettbewerbsrecht
- Rechtschutz
- E-Business
- ethische Aspekte