

Cyber Security, Datenschutz und System-Pentesting

IT-Sicherheit / Cybersecurity · Anbieter: IU Akademie IU Internationale Hochschule

FÖRDERUNG & KOSTEN

Kurspreis: auf Anfrage

Förderfähig über: Bildungsgutschein

AZAV-zertifizierter Bildungsträger — Förderung durch die Agentur für Arbeit möglich

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Self-Paced
Dauer	3 Monate in Vollzeit oder 6 Monate in Teilzeit
Unterrichtssprache	Deutsch
Kursstart	Startet alle 14 Tage
Vorkenntnisse	Keine Vorerfahrung
Abschluss	Zeugnis auf Hochschulniveau
Inklusive	Berufскоaching, Notebook / Tablet (geliehen)

Bildungsträger & Kontakt

IU Akademie IU Internationale Hochschule

Juri-Gagarin-Ring 152, 99084 Erfurt

Telefon: 030 22027283

E-Mail: weiterbildung@iu-akademie.de

Web: <https://www.iu-akademie.de>



Kurs online ansehen

01

Kursbeschreibung

In einer Welt, die zunehmend technologiegesteuert ist, nehmen Bedrohungen durch Cyberangriffe, unzureichenden Datenschutz und Sicherheitslücken stetig zu. Deine Weiterbildung in Cyber Security, Datenschutz und System-Pentesting macht Dich fit für diese Herausforderungen. Du lernst wichtige Grundlagen in Betriebssystemen, Rechnernetzen und verteilten Systemen kennen und erhältst die Fähigkeiten, diese professionell zu schützen. Mit Deinem Wissen stehst Du als Expert:in für IT-Sicherheit bereit, um Unternehmen aktiv beim Schutz ihrer sensiblen Daten zu unterstützen. Der Schwerpunkt Deiner Weiterbildung liegt in der erfolgreichen Durchführung von System-Pentestings und dem Verstehen von Datenschutzrichtlinien. Du erwirbst praxisnahe Kompetenzen, um Sicherheitslücken zu erkennen und zu schließen. Unternehmen jeglicher Branchen suchen händeringend nach Fachkräften, die ihre digitale Infrastruktur sicherer gestalten können. Und genau hier liegt Deine Chance: Durch die Weiterbildung eröffnen sich Dir neue berufliche Möglichkeiten, sei es in der IT-Abteilung eines Großunternehmens oder in einer spezialisierten Beratungsfirma. Deine Fähigkeiten sind gefragt und bilden den Grundstein für eine erfolgreiche Karriere in der IT-Sicherheit.

02

Lehrplan & Module

1. Betriebssysteme, Rechnernetze und verteilte Systeme

Betriebssysteme sind eine zentrale Komponente von Rechnern und stellen grundlegende Funktionen für die Arbeit mit diesen Rechnern bereit. In immer größerem Maße stehen Rechner aber nicht alleine, sondern sind in Netzwerke eingebunden, innerhalb derer auf Daten und Funktionen anderer Computersysteme zugegriffen werden kann. Damit werden verteilte Systeme möglich, bei denen die Daten und Funktionen systematisch verschiedenen Rechnern innerhalb eines Netzwerkes zugeordnet werden, um gemeinsam definierte Aufgaben zu bewältigen. Während die verschiedenen Rechner innerhalb eines Netzwerkes oder eines verteilten Systems in der Vergangenheit stationär waren, sind mittlerweile auch viele mobile Rechner im Einsatz, was zu völlig neuen Anwendungsszenarien sowohl im privaten als auch im geschäftlichen Kontext führt.

Kursinhalte

Grundlagen der Betriebssysteme Grundlegender Aufbau von Computersystemen

Dateisysteme

Speicherverwaltung

Prozesse und Threads

Verbreitete Betriebssysteme Grundkonzepte Windows

Grundkonzepte Unix und Linux

Grundkonzepte Apple-Betriebssysteme

Mobile Betriebssysteme

Rechnernetze Grundlagen der Datenübertragung

OSI-Referenzmodell

Netztopologien

TCP/IP und Internet Entstehung des Internets

TCP/IP-Protokollstack

Ausgewählte IP-basierte Protokolle und Dienste

Sicherheit im Internet

Architekturen verteilter Systeme Client-Server-Systeme und verteilte Anwendungen

Grundbegriffe verteilter Systeme: Nebenläufigkeit, Semaphoren, Deadlock

Kommunikation in verteilten Systemen

Dienste-Orientierung: SOA, Webservices und Microservices

Cloud-Anwendungen

Transaktionen in verteilten Systemen

High-Performance Computing Cluster

Mobile Computing Grundlagen, Techniken und Protokolle für Mobile Computing

Mobiles Internet und seine Anwendungen

Mobile Kommunikationsnetze

Sicherheit und Datenschutz in mobilen Systemen

Fakten zum Modul: Niveau: Bachelor · Unterrichtssprache: Deutsch · 5 ECTS-Punkte · Modulprüfung:

Examen, 90 Minuten

2. Einführung in Datenschutz und IT-Sicherheit

Die Studierenden lernen wichtige Konzepte aus dem Bereich IT-Sicherheit kennen. Dabei werden sowohl grundlegende Begriffe eingeführt und diskutiert als auch typische Anwendungsfelder und Einsatzgebiete von IT-Sicherheit vorgestellt sowie typische Verfahren und Techniken beschrieben.

Kursinhalte

Begriffsbestimmungen und Hintergründe Informationstechnik (IT) für die Unterstützung von privaten Aktivitäten und geschäftlichen Prozessen

Sicherheit und Schutz als Grundbedürfnisse

Datenschutz als Persönlichkeitsrecht

IT-Sicherheit als Qualitätsmerkmal von Informationsverbünden

Abgrenzung Datenschutz und IT-Sicherheit

Grundlagen des Datenschutzes Prinzipien

Rechtliche Vorgaben

Übermittlung personenbezogener Daten ins Ausland

Informationelle Selbstbestimmung im Alltag

Grundlagen der IT-Sicherheit Paradigmen der IT-Sicherheit

Modelle der IT-Sicherheit

Rechtliche Vorgaben der IT-Sicherheit

Standards und Normen der IT-Sicherheit Grundlegende Standards und Normen

Spezifische Standards und Normen

Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz Strukturanalyse

Schutzbedarfsfeststellung

Modellierung (Auswahl der Sicherheitsanforderungen)

IT-Grundschutz-Check

Risikoanalyse

Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte Schutz vor Diebstahl

Schutz vor Schadsoftware (Malware)

Sichere Anmeldeverfahren

Sichere Speicherung von Daten

Sichere Vernichtung von Daten

Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen Objektschutz

Schutz vor unerlaubter Datenübertragung

Schutz vor unerwünschtem Datenverkehr

Schutz durch Business Continuity Management

Fakten zum Modul: Niveau: Bachelor · Unterrichtssprache: Deutsch · 5 ECTS-Punkte · Modulprüfung:

Examen, 90 Minuten

3. Grundzüge des System-Pentestings

System-Penetrationstests sind ein wichtiger Prozess, um Schwachstellen in IT-Systemen zu finden und deren Behebung zu unterstützen, bevor Angreifer sie ausnutzen können. Aus diesem Grund setzen viele Organisationen solche "Pentester" oder ethische Hacker ein, um ihre Software- und Hardwarebasis (einschließlich Konnektivität) zu testen und die gefundenen Sicherheitsprobleme zu beheben. Dies ist zu einem Eckpfeiler moderner Sicherheitskonzepte geworden. Um bei diesem Unterfangen erfolgreich zu sein, ist jedoch eine gute Kenntnis der verschiedenen Arten von anvisierten IT-Systemen erforderlich. Wir beziehen uns auf Hosts, Netzwerke, Web Apps und sogar Cloud Computing. In diesem Kurs stellen wir die grundlegenden Aspekte von IT-Systemen sowie die Prozesse, Hilfsmittel und Techniken vor, die die industrielle Praxis der Penetrationstests ausmachen. Ausgerüstet mit diesem Wissen werden die Studierenden die Mechanismen eines bestimmten Angriffs verstehen und sich auf den Weg eigener Penetration Tests begeben.

Kursinhalte

Ziele von Penetrationstests und industrielle Perspektive Organisatorischer Nutzen

Rahmenbedingungen für Ethical Hacking

Rechtliche Aspekte

Verantwortungsvolle Offenlegung von Schwachstellen

Professionelle Penetrationstest-Dienstleistungen und Zertifizierungen

Hintergrundkonzepte Betriebssysteme

Hardware-Architekturen

Netzwerke und Protokolle

Web-basierte Anwendungen

Cloud-Computing

Ablauf von Penetrationstests Planung und Erkundung

Whitebox-, Blackbox- und Graybox-Scanning

Zugang erhalten

Aufrechterhaltung des Zugangs

Analyse und Berichterstattung

Härtung und Entschärfung

Betriebssystembasierte Penetrationstests Häufige Fehlkonfigurationen

Shellcode-Angriffe

Speicherkorruption und Pufferüberlauf-Schwachstellen

Metasploit und Kali-Tools

Härtung des Betriebssystems

Netzwerk-Penetrationstests Scoping und Recon der Netzwerkinfrastruktur

Ausnutzen von Netzwerkdiensten

Seitliche Bewegung im Netzwerk

Kerberos-Angriffe

Werkzeugsatz: Nmap, PowerShell, Bloodhound und Tcpdump

Entwickeln von Korrekturmaßnahmen

Web-App-Penetrationstests Die OWASP-Methodik

Open-Source-Intelligenz (OSINT)

Häufig ausgenutzte Web-App-Schwachstellen

Ausnutzungs-Toolset: BurpSuite, sqlmap, BeEF und ExploitDB

Berichterstattung über Ergebnisse und Abhilfemaßnahmen

Spezialisierte Penetrationstests auf einen Blick Ausnutzungs-Entwicklung

Ethisches Hacking

Penetrationstests für drahtlose und mobile Geräte

Bewertung von Cloud-Bedrohungen und Schwachstellen

Fakten zum Modul: Niveau: Bachelor · 5 ECTS-Punkte · Modulprüfung: Examen, 90 Minuten

03

Enthaltene Zertifikate

Trägerzertifikat: Zeugnis auf Hochschulniveau

04

Voraussetzungen

Vorkenntnisse

Niveau: Keine Vorerfahrung

Zulassungsvoraussetzung: gute Deutschkenntnisse auf B2-Niveau.

Die Weiterbildung ist auf dem inhaltlichen Niveau eines Bachelor Studiengangs. Eine Weiterbildung auf Bachelor-Niveau vermittelt grundlegende Kenntnisse und Fähigkeiten in einem bestimmten Fachbereich.

Technische Voraussetzungen

Laptop mit Internetzugang.

05

Zielgruppen & Berufsperspektiven

- Arbeitssuchende
- Fachkräfte

Mögliche Berufsbilder: Penetration Tester, Ethical Hacker, IT-Sicherheitsbeauftragter

NÄCHSTER SCHRITT

Kursdetails online ansehen und Anbieter kontaktieren

IU Akademie IU Internationale Hochschule · Juri-Gagarin-Ring 152, 99084 Erfurt
030 22027283 · weiterbildung@iu-akademie.de · <https://www.iu-akademie.de>



[Online ansehen](#)