Cyber Security Analysis

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	4 Monate in Vollzeit oder 8 Monate in Teilzeit
Unterrichtssprache	Deutsch
Kursstart	Startet alle 14 Tage
Vorkenntnisse	Keine Vorerfahrung
Abschluss	Zeugnis auf Hochschulniveau
Inklusive	Berufscoaching, 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

Durch die hohe Digitalisierung aller Lebensbereiche wird auch die IT- und Netzwerksicherheit immer wichtiger. Denn Attacken auf digitale Systeme bedeuten nicht nur einen materiellen Schaden, sondern wirken sich auch negativ auf das Image aus. Mit Deiner Weiterbildung Cyber Security Analysis bist Du auf der sicheren Seite.

Deine Weiterbildung startet mit den grundlegenden Funktionen von Betriebssystemen, Rechnernetzen und verteilten Systemen. Du erfährst alles über OSI-Referenzmodelle, TCP/IP-basierte Protokolle, Client-Server-Systeme, Cloud Computing und Mobile Computing. Mit diesem Wissen geht es an die Grundlagen der IT-Sicherheit, Netzwerk- und Kommunikationssicherheit. Du vertiefst Deine Kenntnis für ein intelligentes IT-Sicherheitsmanagement, um daraus Maßnahmen praktisch umzusetzen. Dann geht es weiter mit dem spannenden Feld der Netzwerkforensik. Dazu begibst Du Dich auf die Suche nach aktuellen Netzwerkspuren, um herauszufinden, wie sich die Protokolle zueinander verhalten und aufeinander aufbauen. Damit Du Netzwerkangriffe gegen TCP und UDP entsprechend aufdecken bzw. verhindern kannst. Weiter geht’s mit dem System Pentesting. Ein wichtiger Prozess, um Schwachstellen in IT-Systemen zu finden und zu beheben, bevor Angreifer sie ausnutzen können. Dafür werden "Pentester" oder ethische Hacker eingesetzt, um die gefundenen Sicherheitsprobleme zu beheben.

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. Einführung in die Netzwerkforensik

Netzwerk-Forensik ist die Kunst und Wissenschaft der Erfassung, Aufzeichnung und Analyse von Netzwerkereignissen, um Angriffe aufzudecken. Dies erfordert eine vertiefte Kenntnis der wichtigsten Internet-Protokolle, wie sie verwendet werden und wie sie angegriffen werden können.
Kursinhalte
Warum Netzwerk-Forensik? Ziele der Untersuchungen
Beweiserhebung im Netzwerk
Erkennung von Eindringlingen
(D)Dos-Erkennung und Entschärfung
Marktverfügbare Werkzeuge
Grundlegende Protokoll-Schichtung Internet-Protokoll-Hierarchie
Verbindung und verbindungslose Protokolle
Lesen von RFCs und zugehöriger Dokumentation
TCP vs. UDP Verbindungsloses UDP
TCP-Verbindungsaufbau
Fehlende Pakete und Weiterleitung
SOCKS-Proxying
Angriffe gegen TCP und UDP
Das Internet-Protokoll IP-Adressen, IPv4 und IPv6
Erlangen einer IPv4- und IPv6-Adresse
Die Rolle der ICANN
IP-Firewalls und Übersetzung von IP-Netzwerkadressen
SOCKS-Proxying
Routing des Link-Layers ARP (Adressauflösungsprotokoll)
Dynamisches RIP-Routing
BGP-Peering
Autonome Systemnummern
Angriffe gegen Routing
Domänennamen-System Hostnamen-Hierarchie
DNS als verteilte Datenbank
DNSSEC
SPF, DMARC und andere Sonderaufzeichnungen
Gemeinsame Protokolle der Anwendungs-Schicht HTTP
HTTP/2
SMTP
Transportschicht-Verschlüsselung SSH
IPSEC
TLS
Man-In-The-Middle-Attack
Zertifikate und Zertifizierungsstellen
Systeme zur Erkennung und Verhinderung von Eindringung Sensor- und Ereignistypen
Netflow-Überwachung
Regeln, falsch positive und falsch negative Ergebnisse
SIEMs
Technologien zur Angriffsvorbeugung
Korrelations- und Anreicherungsdatenquellen Anreicherung von Daten
DNS-Datenquellen: DNSBLs, passives DNS, DNS-Repositorien
AS-Nummern, IP-Blöcke, GeoIP- und WhoIs-Daten
Zertifikat-Transparenz
Korrelationsmethoden
Fakten zum Modul: Niveau: Bachelor · 5 ECTS-Punkte · Modulprüfung: Examen, 90 Minuten

4. 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: SOC Analyst, IT Forensiker, Penetration Tester

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