Lehrgang

Experte für Cybersecurity in der Energieversorgung

Cybersecurity ist in unserer vernetzten Welt ein wesentlicher Bestandteil des Alltags. Besonders Unternehmen und Behörden werden immer wieder Ziele von Cyberangriffen.

Dementsprechend werden in Unternehmen immer mehr Expert:innen mit breitem Grundwissen über die verschiedensten Disziplinen der Informationssicherheit benötigt. Doch auch Industriewissen ist immer mehr gefordert um die aktuellen Bedrohungen einschätzen und entgegenwirken zu können.

Dieser Praxis-Lehrgang ermöglicht Ein- oder Umsteigenden in die Informationssicherheit sich das erforderliche Grundlagenwissen anzueignen, um fundierte Entscheidungen in Cybersecurity-Themen treffen zu können. Des Weiteren sind die Teilnehmenden dazu in der Lage sich in den jeweilig relevanten Bereichen spezialisieren zu können.

Protect Your Grid

IHK Industrie- und Handelskammer Nürnberg für Mittelfranken

OMICRON

Zielgruppe:

Der Lehrgang richtet sich an Techniker:innen, Ingenieur:innen und IT-Mitarbeitende die mit der Planung, dem Betrieb oder der Modernisierung von Anlagen der Energieversorgung betraut sind.

Voraussetzungen:

Grundlagen der elektronischen Datenverarbeitung

Lehrgangsziel:

Die Teilnehmenden sind mit den Grundlagen Informationssicherheit, IT-Sicherheit und OT-Sicherheit vertraut.

Sie sind in der Lage Sicherheitsanforderungen zu definieren und diese an Fachexperten zu kommunizieren.

Sie besitzen Kenntnisse zur Bewertung von Sicherheitskonzepten in sowohl IT- als auch OT-Umgebungen.

Sie sind in der Lage Fachgespräche in den weiten Teilen der Cybersecurity zu führen.

Die Teilnehmenden sind mit den Grundlagen von Betriebssystemen, Netzwerktechnik sowie OT-Systemen vertraut.

Sie verstehen Zusammenhänge zwischen Hardware und Softwareeigenschaften und wie diese bei einem Cyberangriff ausgenutzt werden können.

Durchführung:

Unsere Trainer:innen vermitteln das Wissen in Theorie und Praxis. Die Teilnehmenden vertiefen die neuen technischen Fachkenntnisse in Fallbeispielen, Demonstrationen und praktischen Übungen in unserer Testumgebung. Für einen möglichst hohen Lernerfolg ist die Gruppengröße auf 15 Personen begrenzt.

Modul 1

IT-Security

- Grundlegende Begriffsdefinitionen und Abgrenzungen zum Datenschutz
- Basiskenntnisse zu Betriebssystemen, Programmierung und Umgang mit der Kommandozeile
- Grundlagen der Netzwerktechnik und Kryptographie
- Grundlegendes Wissen und Konzepte zu Datenbanken, Webdiensten und Identity & Access Management (IAM)

Modul 2

OT-Security

- Besonderheiten der OT-Security
- Wichtige Standards
- Bewährte Methoden und Herausforderungen
- Beispiele aus der Praxis: Angriffe und deren Erkennung

Modul 3

Hacking - Angriffsvektoren, Angriffsmethoden und Abwehrstrategien

- Einführung in grundlegende Begriffe und Methoden der Cyberbedrohungen
- Ausnutzen von Schwachstellen
- Schutzstrategien (Cyber Defense)

Modul 4

Governance Risk Compliance (GRC)

- Standards und deren Umsetzung
- Security-Konzepte
- Praktische Umsetzung

Modul 1: IT-Security

Die Teilnehmenden lernen grundlegende Begriffe der IT-Sicherheit kennen und zu unterscheiden. Sie erwerben in diesem Modul auch ein Verständnis der wichtigsten Konzepte von Betriebssystemen und Anwendungen sowie Diensten (zum Beispiel Active Directory, PKI, SQL Server, Webserver, etc.) die oft mit der IT assoziiert werden.

Grundlegende Begriffsdefinitionen und Abgrenzungen zum Datenschutz

- Unterscheidung Sicherheit, Informationssicherheit, IT-/OT-Sicherheit, Cybersecurity
- Wesentliche Begriffsdefinitionen in der Informationssicherheit
- Abgrenzung IT-Sicherheit vs. OT-Sicherheit

Basiskenntnisse zu Betriebssystemen, Programmierung und Umgang mit der Kommandozeile

- Konzeptueller Unterschied Windows / *Nix
- Prozesse, Threads und Scheduling
- Einfache Programme entwickeln

Grundlagen der Netzwerktechnik und Kryptographie

- Verschlüsselung und Hashwerte
- Key Exchange, PKI
- Zusammenspiel von einzelnen ISO/OSI-Schichten

Grundlegendes Wissen und Konzepte zu Datenbanken, Webdiensten und Identity & Access Management (IAM)

- Aufbau einer klassischen Webseite
- Structured Query Language (SQL)
- “Need to Know”- und “Least Privilege”-Prinzipien

Modul 2: OT-Security

Die Teilnehmenden lernen warum sich bestehende Konzepte aus der IT nicht 1:1 auf die OT-Umgebungen übertragen lassen. Sie lernen dabei wichtige Standards und Richtlinien kennen und einzuordnen sowie bewährte Umsetzungsmethoden für die Bereiche Verschlüsslung, Fernwartung, Angriffserkennung, Schwachstellenmanagement und Konnektivität . Mittels relevanter Praxisbeispiele kann das erlernte Wissen direkt angewandt werden.

Besonderheiten der OT-Security

- Überblick über OT (SCADA, OT-Komponenten und -protokolle)
- Möglichkeiten und Grenzen der Anwendbarkeit von IT-Lösungen in OT-Umgebungen durch Anforderungen an Lebenszyklus, Determinismus und Netzwerkstabilität

Wichtige Standards

- IEC62443
- NIST CSF
- BDEW Whitepaper

Bewährte Methoden und Herausforderungen

- Verschlüsselung in der OT
- Schwachstellenmanagement
- IIoT- und Cloud-Computing

Beispiele aus der Praxis: Angriffe und deren Erkennung

- Relevante Angriffe der jüngsten Vergangenheit
- Detektion von Angriffen mit IDS / SzA

Modul 3: Hacking - Angriffsvektoren, Angriffsmethoden und Abwehrstrategien

Die Teilnehmenden lernen Methoden und Bedrohungen kennen, die durch Hacking und andere Angriffsvektoren entstehen können. Dabei werden die Grundlagen für Risikoanalysen geschaffen. Sie erlenen dabei Strategien, um sich gegen diese Bedrohungen zu verteidigen.

Einführung in grundlegende Begriffe und Methoden der Cyberbedrohungen

- Was ist Hacking?
- Angriffsmethoden und Angriffsvektoren
- Threat und Risk

Ausnutzen von Schwachstellen

- Angriffsarten
- OSINT
- Webhacking

Schutzstrategien (Cyber Defense)

- Strategien und Vorgehensweisen
- Security Engineering
- Security Operation

Modul 4: Governance Risk Compliance (GRC)

Teilnehmende verstehen welche Bedeutung Standards einnehmen und wie die Erfüllung dieser die Sicherheit verbessert. Sie lernen dabei verschiedene Aspekte eines Security-Konzepts kennen und wie ausgewählte Maßnahmen praktisch implementiert werden können.

Standards und deren Umsetzung

- ISO 27001 i.V.m. ISO 27019
- BSI IT-Grundschutz
- etc.

Security-Konzepte

- ISMS
- Risikomanagement
- Physische Sicherheit

Praktische Umsetzung

- Richtlinien und Prozesse
- Notfallpläne
- Backup & Restore

Kursinfo

Zertifikatslehrgang, Vollzeit, 60 Stunden

Der Zertifikatstest wird am Ende des Lehrgangs durchgeführt.

Voraussetzungen für den Erwerb des IHK-Zertifikats sind:

- regelmäßige Teilnahme am Lehrgang (80%)
- mindestens 50% der erreichbaren Punkte müssen erzielt werden

Anmeldung

IHK Akademie Mittelfranken
Walter-Braun-Straße 15
D-90425 Nürnberg

Die aktuellen Termine sowie das Online-Anmeldeformular finden Sie unter:

https://www.ihk-akademie-mittelfranken.de/weiterbildungen/details/experte-fuer-cybersecurity-in-der-energieversorgung-ihk-1103

Lehrgangsort

OMICRON Schulungszentrum
Goethestraße 20
D-91054 Erlangen

Kontakt Lehrgangsorganisation

OMICRON Academy
Gerhild Schmidts
+49 9131 9073 5252
academy.germany@omicronenergy.com

Preis und Teilnahmebedingungen

EUR 6.390,00 pro Person (excl. Umsatzsteuer)
incl. Seminarunterlagen in digitaler Form

Es gelten die Allgemeinen Geschäftsbedingungen der IHK Nürnberg für Mittelfranken, die auf www.ihk-nuernberg.de einsehbar und herunterladbar sind.

OMICRON arbeitet mit Leidenschaft an wegweisenden Ideen, um Energiesysteme sicherer und zuverlässiger zu machen. Mit unseren neuartigen Lösungen stellen wir uns den aktuellen und zukünftigen Herausforderungen unserer Branche. Wir unterstützen unsere Kund:innen mit vollem Einsatz: Wir gehen auf ihre Bedürfnisse ein, bieten ihnen hervorragenden Vor-Ort-Support und teilen unsere Expertise und unsere Erfahrungen mit ihnen.

In der OMICRON-Gruppe entwickeln wir innovative Technologien für alle Bereiche elektrischer Energiesysteme. Im Fokus stehen elektrische Prüfungen an Mittel- und Hochspannungsbetriebsmitteln, Schutzprüfungen, Prüfungen digitaler Schaltanlagen und Cyber Security. Kund:innen in aller Welt vertrauen auf unsere einfach zu bedienenden Lösungen und schätzen deren Genauigkeit, Schnelligkeit und Qualität.

Wir sind seit 1984 in der elektrischen Energietechnik tätig und verfügen über fundierte, langjährige Erfahrung in der Branche. Rund 1.250 Mitarbeiter:innen an über 20 Standorten unterstützen unsere Kund:innen in mehr als 170 Ländern und unser technischer Support kümmert sich 24 Stunden am Tag, 7 Tage die Woche um sie.

Für mehr **INFORMATIONEN**

Eine detaillierte Übersicht über unsere Produkte und Services, weiterführende Literatur und Kontaktinformationen unserer weltweiten Niederlassungen finden Sie auf unserer Webseiten:

www.omicroncybersecurity.com
www.omicronenergy.com

oder Sie kontaktieren uns direkt per E-Mail:
info@omicroncybersecurity.com