Hack the Grid: Mission OT-Sicherheit für Energie- und Wasserversorgung

Cybersecurity Challenge für technische Fachkräfte in kritischen Infrastrukturen

Dieser praxisorientierte Kurs richtet sich an Fachkräfte aus der Energie- und Wasserversorgung und vermittelt, wie OT-Systeme vor Cyberangriffen geschützt werden. Schwerpunkte sind die Identifikation von Schwachstellen und die Implementierung von Sicherheitsmaßnahmen zum Schutz kritischer Infrastrukturen.

Hack the Grid: OT-Sicherheit trainieren und praxisnah erleben

Sie möchten die Schwachstellen in der Cyber-Infrastruktur im Bereich der Energie- und Wasserversorgung unter möglichst realen Bedingungen kennen und verstehen lernen und dabei auch noch Spaß haben?

Dann sind Sie hier genau richtig! Mithilfe des spielebasierten Trainingsansatzes „Capture the Flag" nehmen Sie als technische Fachkraft die verschiedenen Perspektiven von Angreifenden und Verteidigenden ein, wodurch Sie Schwachstellen in einer fiktiven Anlage finden, Bedrohungen proaktiv erkennen und geeignete Abwehrstrategien entwickeln.

Durch den effektiven und innovativen Gamification-Ansatz bietet unser Vertiefungsseminar »Hack the Grid: Mission OT-Sicherheit" eine einzigartige Möglichkeit, praktische Fähigkeiten in einer interaktiven Lernumgebung zu erwerben und digitale Herausforderungen zu meistern.

Kursdetails auf einen Blick

- Für **IT-Sicherheitsbeauftragte, IT-Administratoren, Mitarbeitende der Feld- und Leittechnik**
- **Offene Schulung** oder I**nhouse Training**
- Dauer: **3 Tage à 8 Stunden**
- Format: **Präsenz**
- Kosten: 2.100,00 Euro (zzgl. MwSt.)

RED vs. BLUE: Schwachstellen erkennen und Abwehrstrategien entwickeln

Unsere Schulung simuliert reale Umgebungen aus der Energie- und Wasserversorgung. Dabei können Sie sich als teilnehmende Person sowohl in die Rolle der Angreifenden (RED-Team) als auch der Verteidigenden (BLUE-Team) versetzen. Durch die Schulung lernen Sie, potenzielle Schwachstellen zu identifizieren, Angriffsstrategien zu entwickeln und Ihr Unternehmen proaktiv vor Bedrohungen zu schützen. Besonders durch den Perspektivwechsel auf die Angreifer-Seite sind Sie nach dem Training in der Lage, Angriffsvektoren und Risiken auf Ihre Infrastruktur der Energie- und Wasserversorgung neu einzuschätzen. Unsere Schulung ist die umfassende Antwort auf die komplexen Herausforderungen unserer vernetzten Welt. Seien Sie bestens vorbereitet, um Ihre Expertise auf die nächste Stufe zu bringen.

Damit Sie optimal auf diese Cybersicherheits-Challenge vorbereitet sind, sollten Sie vorab eines unserer Praxistrainings abgeschlossen haben oder bereits über Erfahrungen und Anwendungswissen verfügen.

Nach dem Seminar können Sie:

- **Grundlagen der OT-Sicherheit** verstehen und anwenden.
- Sicherheitsrisiken in der **Operational Technology (OT)** erkennen und Maßnahmen zur **Absicherung kritischer Infrastrukturen** ableiten.
- Strategien zur **Implementierung von Sicherheitsmaßnahmen für die Schutzsysteme und Netzwerke** in der Energie- und Wasserversorgung entwickeln.

Alle Kursdetails und die Anmeldung finden Sie hier:

https://s.fhg.de/cyberattacken

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Tag 1
- Einführung technische Grundlagen
- Capture- the-Flag-Ansatz
- Netzwerksegmentierung und Netzwerkscans
- Praktische Umsetzungen an der Schulungsplattform

Tag 2
- Netzwerk- und Assetmonitoring
- Überwachung des Netzwerkverkehrs
- Angriff auf das Prozessnetz und Angriffserkennung
- Praktische Umsetzungen an der Schulungsplattform

Tag 3
- Logging und Use Case SIEM
- Incident Response
- Spielbasierte Umsetzung: Angriff vs. Verteidigung

Zugangsvorraussetzung:

Erfahrungen und Anwendungswissen in folgenden Bereichen werden vorausgesetzt:

- Netzwerkgrundlagen und -sicherheit
- Netzwerkprotokolle in der Energieversorgung
- Netzwerkmonitoring
- Angriffserkennung und -abwehr
- Absicherung und Härtung von ICS-Komponenten

Im Idealfall haben Sie vorher an einem unserer Praxistrainings teilgenommen

Fachlicher Ansprechpartner am Fraunhofer IOSB-AST

M.Sc. Dennis Rösch
Tel. +49 (0) 3677 461188
dennis.roesch@iosb-ast.fraunhofer.de

Fraunhofer IOSB-AST
Am Vogelherd 90
98693 Ilmenau

Lernlabor Cybersicherheit