Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Technisches Intensivtraining

Mit der mobilen Schulungsplattform Cyberangriffe erkennen, verstehen und abwehren

Das Lernlabor Cybersicherheit für die Energie- und Wasserversorgung trägt wesentlich zur Gewährleistung der Cybersicherheit in der deutschen Energie- und Wasserversorgung bei. Durch die enge Verzahnung mit der Vorlaufforschung sowie die Nutzung modernster Laborinfrastruktur bietet es Qualität und Expertise. Auf dieser Grundlage entwickelt das Lernlabor praxisnahe Weiterbildungen, um die gesamte Bandbreite der Cybersicherheit in IT- und OT-Systemen der Energie- und Wasserversorgung abzudecken.

Ganzheitliche Abwehrstrategien und praxisnahe Umsetzung

In diesem Training wird die Herangehensweise von Hackern auf Systeme und Prozesse der Energieversorgung strukturell erläutert und durch Beispielangriffe auf die Schulungsplattform nachvollzogen. Die gesamte Cyber-Kill-Chain wird durchlaufen und das mehrstufige Verfahren bei einem Angriff nachgestellt. Aus diesem Bewusstsein über das Handeln von Angreifern werden gezielt strukturelle Schwachstellen und Bedrohungen aufgearbeitet und praktische Gegenmaßnahmen zur Absicherung entwickelt. Vor allem präventive Maßnahmen zur Netzwerkabsicherung und Systemhärtung stehen im Vordergrund.

Der Praxisbezug durch die eigenständige Konfiguration der technischen Komponenten und Implementierung der entwickelten Sicherheitsmaßnahmen steht besonders im Fokus.

Mobile Schulungsplattform für umfassendes Lernen

Den Teilnehmern wird die Möglichkeit geboten, die Themen sehr hardwarenah an einer Schulungsplattform zu bearbeiten. Ziel der Schulung ist die Abwehr verschiedener Angriffsarten und die Sicherstellung der Prozesse innerhalb der Energieversorgung durch präventive Absicherung der Netzwerkinfrastruktur und Härtung der ICS-Komponenten. Neben der Präventivverteidigung und dem Perimeterschutz werden Monitoring und Analysewerkzeuge untersucht und angewendet.

Die Schulungsplattform bildet einen realen Prozess aus der Feldebene der Energieversorgung ab mit Eingliederung in eine Netzwerkstruktur mit Kopplung zu überlagerten Netzwerkebenen.

Lernlabor Cybersicherheit für die Energie- und Wasserversorgung

Auf einen Blick

- Für technisches Personal
- Individuell gestaltbar
- Inhouse bei Ihnen oder im Lernlabor Ilmenau/Görlitz
- Dauer: 2-3 Tage
- Angriffsmethoden auf Versorgungsstrukturen
- Netzwerksicherheit und Monitoring
- Infektion und Übernahme von Systemen
- Härtung von Komponenten

Lernziele

- IT-Gefahren für Automatisierungstechnik in der Energietechnik vertiefend kennenlernen
- Ein Bewusstsein für sicherheitskritische Konfigurationen und Prozesse entwickeln
- Sichere Konfigurationen vornehmen und Netzwerke absichern

Sie erwartet im technischen Intensivtraining

Unsere technischen Intensivtrainings werden individuell nach Ihren Bedürfnissen gestaltet. Um in die inhaltliche Tiefe und praktische Umsetzung zu gehen, werden die Trainings als zwei- oder dreitägig ausgelegt und können beispielhaft wie folgt aussehen:

Tag 1

- Angriffsbeispiele und -methoden
- Einführung in die Schulungsplattform und Angriffsdemonstration
- Netzwerkgrundlagen und -sicherheit
- Netzwerkprotokolle in der Energieversorgung

Tag 2 - optional

- Nachstellen der Angreiferperspektive anhand der Cyber-Kill-Chain vom Internet bis zum Prozessnetz
- Ermitteln und Ausnutzen von Schwachstellen
- Infektion und Übernahme von Systemen
- Lateral Movement im Unternehmensnetzwerk

Tag 3

- Netzwerkmonitoring und -analyse
- Sichere Konfiguration von Fernwirktechnik
- Absicherung und Härtung von ICS Komponenten
- Sicherheit von heterogener Systemlandschaft

Zielgruppe der technischen Intensivtrainings

- IT-Sicherheitsbeauftragte
- IT-Administratoren
- Mitarbeiterinnen und Mitarbeiter der Feld- und Leittechnik
- Technische Mitarbeiterinnen und Mitarbeiter in der Energie- und Wasserversorgung

> „Das Hands-On Cybersecurity Intensivtraining nach unseren Vorgaben in enger Zusammenarbeit mit dem Fraunhofer IOSB-AST stellt eine effektive Ergänzung im Rahmen des Mitarbeitertrainings für eine aktive Cyberverteidigung dar."
>
> **Arslan Brömme,**
> **National Information**
> **Security Officer Germany, Vattenfall**

Lernlabor Cybersicherheit für die Energie- und Wasserversorgung

Standort Ilmenau

Dipl.-Ing. Steffen Nicolai
Tel. +49 3677 461-188
Mobil +49 170 2981 852
steffen.nicolai@iosb-ast.fraunhofer.de

Fraunhofer IOSB, Institutsteil
Angewandte Systemtechnik (AST)
Am Vogelherd 90
98693 Ilmenau

Standort Görlitz

Prof. Dr.-Ing. Jörg Lässig
Tel. +49 3581 7925354
Mobil +49 173 7366285
joerg.laessig@iosb-ast.fraunhofer.de

Fraunhofer IOSB, Institutsteil
Angewandte Systemtechnik (AST)
Wilhelmsplatz 11
02826 Görlitz