Fraunhofer
IOSB

Institutsteil Angewandte Systemtechnik AST

TECHNISCHES INTENSIV-TRAINING

LERNLABOR CYBERSICHERHEIT

ENERGIE- UND WASSERVERSORGUNG

CYBERATTACKEN MEISTERN!

Mit der mobilen Schulungsplattform Cyberangriffe erkennen, verstehen und abwehren

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 Sicherheitsmaßmahen stehen besonders im Fokus.

AUF EINEN BLICK:

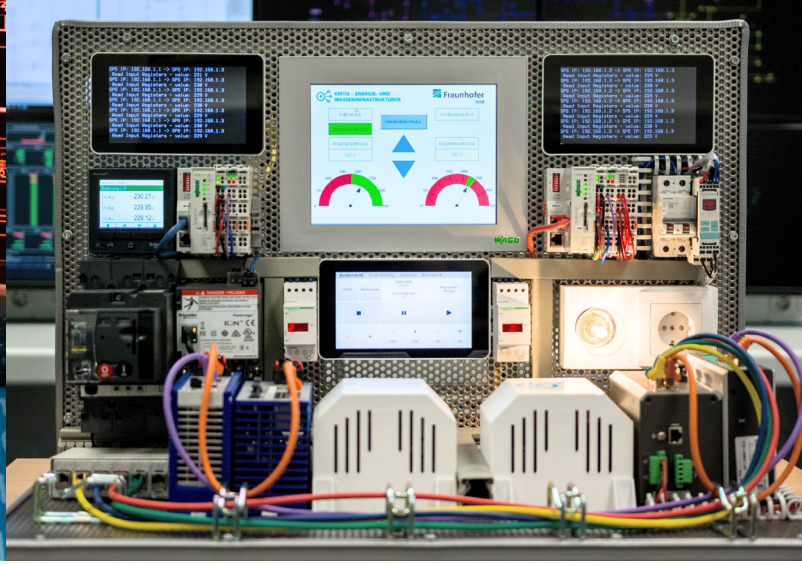
- Für technisches Personal
- Individuell gestaltbar
- Inhouse bei Ihnen oder im Lernlabor Ilmenau / Görlitz
- Dauer: 2 oder mehr Tage
- Angriffsmethoden auf Versorgungsstrukturen
- Netzwerksicherheit und Monitoring
- Härtung von Komponenten und Systemen
- Übung an realen Komponenten

GESPRÄCHSPARTNER

Dipl.-Ing. Steffen Nicolai
Fraunhofer IOSB-AST
+49 3677 461-112
steffen.nicolai@iosb-ast.fraunhofer.de

M.Sc. Dennis Rösch
Fraunhofer IOSB-AST
+49 3677 461-188
dennis.roesch@iosb-ast.fraunhofer.de

Prof. Dr.-Ing. Jörg Lässig
Fraunhofer IOSB-AST
+49 3581 792-5354
joerg.laessig@iosb-ast.fraunhofer.de



Sie erwartet in den technischen Intensivtrainings

Unsere technischen Intensivtrainings werden individuell nach Ihren Bedürfnissen gestaltet. Um in die inhaltliche Tiefe und praktische Umsetzung zu gehen, werden die Trainings als mindestens zweitägig 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

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

Zielgruppe der technischen Intensivtrainings

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

Mobile Schulungsplattform

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 Monitoringund 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.

Lernziele

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

Individuelle Lernziele und Inhalte können in unseren Trainings berücksichtigt und integriert werden.

Das sagen unsere Kunden über uns

„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...

... ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen.

Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT- und OT-Infrastruktur.

www.iosb-ast.fraunhofer.de
www.cybersicherheit.fraunhofer.de/energie

Hochschule Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES