Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Capture the Flag: Angriffs- und Verteidigungsperspektive

Cybersecurity Challenge für die Energie- und Wasserversorgung

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.

Die Herausforderung: Der Umgang mit ständig neuen Angriffsvektoren und die effektive Abwehr von Cyberangriffen

Die zunehmende Digitalisierung in der Energie- und Wasserversorgung führt zu immer mehr und komplexeren Cyberangriffen. Die Mitarbeitenden in den Unternehmen müssen mit dieser rasanten Entwicklung Schritt halten. Die Schwierigkeit besteht darin, aktiv und zeitnah auf neue Bedrohungen reagieren zu können. Es genügt dabei nicht mehr nur neues Wissen zu erwerben – vielmehr muss dieses selbstständig weiterentwickelt und auf neue Situationen angewendet werden können. Dazu ist es notwendig, neue Perspektiven einzunehmen, um den Angreifenden zu verstehen und sich in seine Lage zu versetzen.

Die Lösung: Expertise ausbauen, Herausforderungen meistern - Entdecken Sie unsere Cybersicherheitschallenge für Energie- und Wasserversorgung

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

Auf einen Blick

- Für IT-Sicherheitsbeauftragte, IT-Administratoren, Mitarbeitende der Feld- und Leittechnik
- Inhouse bei Ihnen oder im Lernlabor Ilmenau/Görlitz
- Dauer: 3 Tage
- RED-Team vs. BLUE-Team
- Anwendung von Defense-in-Depth
- Cyberangriffe durch konkrete Gegenmaßnahmen effektiv verhindern

Nach dem Seminar können Sie:

- Eine Vielzahl an unterschiedlichen Angriffsvektoren und deren Risiken für Ihre Infrastruktur beurteilen.
- Typische strukturelle Schwachstellen erkennen und konkrete Gegenmaßnahmen einleiten.
- Den Ablauf eines Cyberangriffs nachvollziehen und effektive Gegenmaßnahmen einleiten.
- Die eigene Infrastruktur besser gegen potenzielle Cyberangriffe schützen.

Das Seminar bietet Ihnen:

- Aktuelles Forschungswissen in einem anwendungsorientierten Format mit hohem Praxisanteil.
- Hands-on-Fachwissen zu häufigen Schwachstellen und Einfallstoren im Bereich der Cybersecurity.
- Die Möglichkeit, unterschiedliche Angriffsvarianten und Gegenmaßnahmen aus unterschiedlichen Perspektiven gefahrlos auszuprobieren.
- Das Wissen und die Fähigkeiten, geeignete Handlungsempfehlungen für die eigene Infrastruktur abzuleiten.

Voraussetzungen:

Erfahrungen und Anwendungswissen in folgenden Bereichen werden vorausgesetzt:

- Netzwerkgrundlagen und -sicherheit (z. B. ISO/OSI-Referenzmodell, Angriffstechniken wie Brute-Force und Man-in-the-Middle)
- Netzwerkprotokolle in der Energieversorgung (z. B. Modbus/TCP, IEC 60870-5-104)
- Netzwerkmonitoring (z. B. SNMP, Wireshark, Nmap)
- Angriffserkennung und -abwehr (z. B. Firewallregeln, Netzwerkarchitektur, Logging)
- Absicherung und Härtung von ICS-Komponenten (z. B. Passwortmanagement, Konfiguration von Komponenten, Addressfilter)

Im Idealfall haben Sie vorher am Seminar „Präventionstraining OT-Sicherheit in Energie- und Wasserversorgung“ teilgenommen.

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