Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Awareness Workshop

Präsenz und Online

Sicherheit stärken, Risiken minimieren: Ihr Weg zur IT-Sicherheit in der 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 gestiegenen Bedrohungslage durch geschärftes Sicherheitsbewusstsein begegnen

Durch die zunehmende Digitalisierung in den Energie- und Wasserinfrastrukturen erhöht sich die Anfälligkeit gegenüber Cyberattacken, während den Angreifenden immer leistungsfähigere Werkzeuge und Methoden zur Verfügung stehen. Gleichzeitig steigt die Abhängigkeit von automatisierten Prozessen und IT-Systemen immer weiter an.

Eine Reihe von unterschiedlichen gesetzlichen Anforderungen, aber auch vorhanden Richtlinien zur Absicherung der eigenen Infrastrukturen bilden hier einen Rahmen.

Neben den technischen Komponenten müssen auch die Mitarbeitenden entsprechend geschult werden, da diese derzeit die am häufigsten ausgenutzte Schwachstelle von Cyberangriffen darstellen.

Die Lösung: Wissen, welche Gefahren drohen und wie man ihnen begegnen kann

Um den Gefahren der IT-Sicherheit für Versorgungsunternehmen im Bereich Energie und Wasser entgegenzutreten, illustrieren vergangene Angriffsbeispiele die möglichen Gefahren und eine Analyse der Angriffe bildet Handlungsempfehlungen gegen diese ab. Essentiell für den eigenen Schutz ist die zukünftige und aktuelle Gesetzeslage sowie branchenspezifische Standards und Normen. Sie lernen, Gefährdungen und Risiken einzuschätzen und häufige Versäumnisse zu vermeiden, sowie vorhandene branchenspezifische Standards anzuwenden.

Weiterhin werden Sie selbst für die existierenden Gefahren im beruflichen Alltag sensibilisiert und werden in die Lage versetzt, dieses Wissen an Ihre Mitarbeiter*innen und Kolleg*innen weiterzugeben.

Auf einen Blick

- Für Führungskräfte und Mitarbeiter
- Individuell gestaltbar
- Inhouse bei Ihnen oder im Lernlabor Ilmenau/Görlitz
- Dauer: 1 Tag
- Relevante Gefahren in der Energieversorgung
- Live-Hacking von Automatisierungstechnik
- Sichere Authentifizierung
- Unternehmenskultur der IT-Sicherheit

Lernziele

- Typische Angriffsabläufe verstehen
- Verschiedene Angriffsbeispiele und zenarien kenne
- Rechtliche Rahmenbedingungen kennen und deren Auswirkungen verstehen
- Standards und Normen voneinander abgrenzen und einschätzen können
- Eigenes Handeln sicherer gestalten können
- Mitarbeiter für Themen der Cybersicherheit sensibilisieren können

Sie erwartet im Workshop

Während des Workshops werden verschiedene Cybersicherheitsthemen diskutiert und anhand vieler praxisnaher Beispiele und Vorführungen verinnerlicht. Dafür werden die einzelnen Phasen von Angriffen und die ausgenutzten technischen und organisatorischen Schwachstellen untersucht und aufgezeigt. Möglichkeiten der Verhinderung von solchen Angriffen stehen besonders im Vordergrund. Die Unterstützung von Richtlinien und Standards wird Ihnen Nahe gebracht und wir befähigen Sie, die geeigneten IT-Sicherheitsmaßnahmen entsprechend einzuleiten und umzusetzen.

Bei uns bekommen Sie Antworten auf die folgenden Fragen

- Welche Angriffe auf Kritische Infrastrukturen gab es bereits, und wie liefen diese ab?
- Welche Auswirkungen hatten diese Angriffe?
- Wie hätten die Angriffe verhindert werden können?
- Welche Standards und Normen existieren bereits, wie können sie umgesetzt werden?
- Welche Gesetze gelten für Kritische Infrastrukturen und die Energieversorgung?
- Welcher Aufwand muss, welcher sollte betrieben werden?
- Wie kann ich mich selbst vor Cyberangriffen schützen?
- Wie sensibilisiere ich meine Mitarbeiter nachhaltig?

»

Das Seminar hat mich durch die sehr kompetenten Vorträge und erfrischenden Diskussionen überzeugt. Für meine strategische Arbeit konnte ich aus dem Tag viel mitnehmen und kann deshalb das Seminar sehr weiterempfehlen."

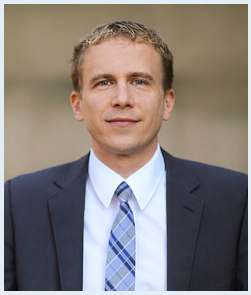
Susanne Kufeld, Leiterin DB-Lagezentrum und globales Krisenmanagement, zivile Verteidigung

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