

»Das Seminar »IT-Sicherheit für Kritische Infrastrukturen« 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

GEFAHRENLAGEN & AWARENESS FÜR VERSORGUNGSUNTERNEHMEN

IT-SICHERHEIT FÜR DIE ENERGIE- UND WASSERVERSORGUNG

Die Herausforderung: Der gestiegenen Bedrohungslage entgegentreten.

Cyberangreifer entwickeln immer leistungsfähigere Werkzeuge und Methoden für digitale Energie- und Wasserinfrastrukturen. Parallel entstehen jedoch Abhängigkeiten von automatisierten Prozessen und IT-Systemen. Schützen Sie ihre Strukturen durch gezielte IT-Sicherheitsvorkehrungen. Dafür sind branchenspezifisches Wissen zur aktuellen Gesetzeslage und fundierte Angriffsanalysen notwendig. In diesem Workshop erlernen Sie ebendiese Fähigkeiten.

Inhalte des Workshops

Welche Angriffe auf Kritische Infrastrukturen gab es bereits, und wie liefen diese ab?

Welche Auswirkungen hatten diese Angriffe?

Wie kann ich die Schwachstellen im eigenen Unternehmen schließen?

Welche Gesetze gelten für Kritische Infrastrukturen?

Welcher Aufwand muss, welcher sollte im Bereich IT-Sicherheit betrieben werden?

Wie sensibilisiere ich meine Mitarbeitenden nachhaltig?

Während des Workshops werden verschiedene Cybersicherheitsthemen diskutiert und anhand vieler praxisnaher Beispiele und Vorführungen verinnerlicht. Dafür werden die einzelnen Pha-

sen 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 nahegebracht, und wir befähigen Sie, die geeigneten IT-Sicherheitsmaßnahmen entsprechend einzuleiten und umzusetzen.

Ihr Nutzen

- » Nach dem Seminar können Sie viele verschiedene Angriffsbeispiele und deren Risiko auf eigene Unternehmen beurteilen.
- » Sie wissen, wie typische strukturelle Schwachstellen aussehen, und können Maßnahmen einleiten, welche den Gesetzen sowie aktuellen Standards entsprechen.
- » Sie wissen, wie Sie den gesetzlichen Rahmen für Ihr Unternehmen beurteilen.
- » Sie sind in der Lage, eine Vielzahl an Angriffsversuchen abzuwehren.

INFORMATIONEN IM ÜBERBLICK

Keine Voraussetzungen

Führungskräfte, Mitarbeitende aus dem Management, IT-Sicherheitsbeauftragte, Mitarbeitende der Energie- und Wasserversorgung

1 Tag Präsenz

600,-

Ilmenau, Görlitz, inhouse

Veranstaltet durch

Fraunhofer
IOSB
Institutsteil Angewandte Systemtechnik AST

Hochschule
Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES

Referenten:



Adam Bartusiak,
wiss. Mitarbeiter
Fraunhofer IOSB-AST,



Oliver Nitschke,
wiss. Mitarbeiter
Fraunhofer IOSB-AST



Weitere Infos und
aktuelle Termine
buchen unter:

www.cybersicherheit.fraunhofer.de/it-sicherheit-energie-und-wasserversorgung