

# Cyber-Awareness Training für Energie- und Wasserversorgung

## Grundlagenschulung für Gefahrenlage, Angriffsanalyse und Awareness für Versorgungsunternehmen

*Der Kurs vermittelt praxisnahe Kenntnisse zur IT-Sicherheit in der Energie- und Wasserversorgung. Sie lernen, Sicherheitsrisiken zu identifizieren, rechtliche Vorgaben zu berücksichtigen und IT-Sicherheitskonzepte zu entwickeln. Durch praxisorientierte Beispiele und eine enge Verzahnung von Theorie und Praxis werden die Teilnehmer in die Lage versetzt, wirksame Sicherheitsmaßnahmen zu entwickeln und umzusetzen, die den Anforderungen der Branche gerecht werden.*

### Grundlagen der Cybersicherheit für Energie- und Wasserversorger

Sie suchen nach einem umfassenden Einstieg in die Cybersicherheit – speziell für Ihr Unternehmen aus dem Bereich Energie- und Wasserversorgung? Erwerben Sie in diesem Kurs die wichtigsten Kenntnisse im Bereich Cybersicherheit – speziell für Ihr KRITIS-Unternehmen.

Zudem erfahren Sie, wie Sie rechtliche Anforderungen nach NIS-2 und EU-DSGVO erfüllen

können. Lernen Sie außerdem, potenzielle Angriffspunkte in IT- und OT-Systemen zu identifizieren und zu schützen.

Der Kurs vermittelt fundiertes Wissen über Cybersicherheit in der Energie- und Wasserversorgung, insbesondere in Bezug auf die spezifischen Anforderungen dieser Kritischen Infrastruktur.

### Kursdetails auf einen Blick

- Für **Führungskräfte, IT-Nutzer\*innen, Anwender\*innen**
- **Offene Schulung** oder **Inhouse Training**
- Dauer: **1 Tag à 8 Stunden**
- Format: **Präsenz oder Online**
- Kosten: ab 540,00 Euro (USt.-befreit nach §4 Nr. 22a UStG)

## Sicherheitsstrategien und Compliance für Energie- und Wasserversorger

Angesichts der steigenden Zahl an Cyberangriffen und der zunehmenden Digitalisierung ist es entscheidend, die Sicherheitslücken sowohl in IT- als auch in OT-Systemen zu erkennen und abzusichern. Teilnehmende lernen, wie sie durch die Analyse von Schwachstellen Risiken bewerten und gezielte Schutzmaßnahmen einführen können. Dabei wird besonders auf praktische Sicherheitsstrategien und den Umgang mit aktuellen Bedrohungen eingegangen.

Das Seminar behandelt auch die gesetzlichen Vorgaben und Sicherheitsstandards, die für Unternehmen im Bereich der Energie- und Wasserversorgung gelten. Im Fokus stehen dabei unter anderem die NIS-2-Richtlinie und die EU-DSGVO, deren Umsetzung für die IT-Sicherheit und den Datenschutz von entscheidender Bedeutung ist. Zudem wird das Bewusstsein für die spezifischen Anforderungen an die Kritische Infrastruktur geschärft, sodass die Teilnehmenden befähigt werden, die Sicherheit in ihrem Unternehmen zu verbessern.

### Nach dem Seminar können Sie:

- **Gefährdungen** in der Cybersicherheit für Unternehmen der Energie- und Wasserversorgung **erkennen und bewerten**.
- **Sicherheitslücken** in IT- und OT-Systemen **identifizieren** und entsprechende **Maßnahmen** zum Schutz **einleiten**.
- **gesetzliche Anforderungen** wie die EU-DSGVO und NIS-2 **umsetzen** und **im Rahmen aktueller Sicherheitsstandards handeln**.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Cyber-Awareness>

## Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- 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 und wie kann ich die Schwachstellen im eigenen Unternehmen schließen?
- Welche Gesetze gelten für Kritische Infrastrukturen?
- Welche Änderungen erwarten mich mit der EUDSGVO?
- Welche Standards und Normen existieren bereits und wie können sie umgesetzt werden?
- Welcher Aufwand muss, welcher sollte im Bereich IT-Sicherheit betrieben werden?
- Wie kann ich mich selbst vor Cyberangriffen schützen?
- Wie sensibilisiere ich meine Mitarbeitenden nachhaltig?
- [ONLINE] Virtuelle Vorführung und Demonstration von Angriffen auf Mobile Schulungsplattform der Cyber-Kill-Chain

### Zugangsvoraussetzung:

Keine besonderen Voraussetzungen notwendig.

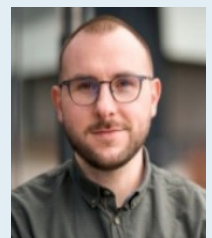
### Teilnahmegebühr:

ONLINE: 540,00 Euro (USt.-befreit nach §4 Nr. 22a UStG)  
PRÄSENZ: 700,00 Euro (USt.-befreit nach §4 Nr. 22a UStG)

### Fachlicher Ansprechpartner am Fraunhofer IOSB-AST

M.Sc. Dennis Rösch  
Tel. +49 (0) 3677 461188  
[dennis.roesch@iosb-ast.fraunhofer.de](mailto:dennis.roesch@iosb-ast.fraunhofer.de)

Fraunhofer IOSB-AST  
Fraunhoferstraße 1  
76131 Karlsruhe



Lernlabor  
**Cybersicherheit**