Fraunhofer ACADEMY

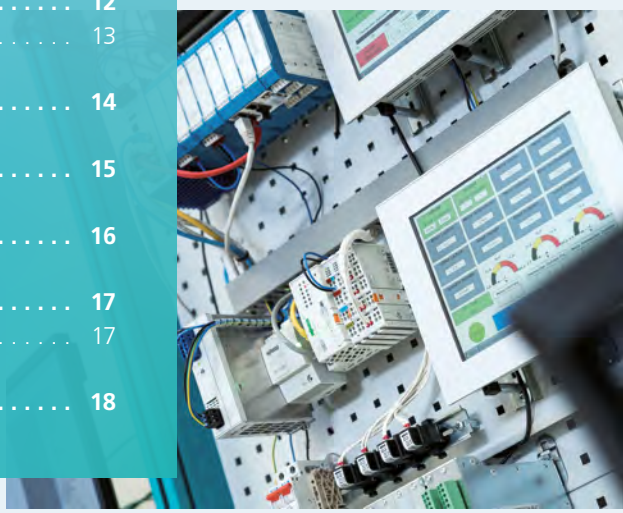
Weiterbildung im
Lernlabor Cybersicherheit

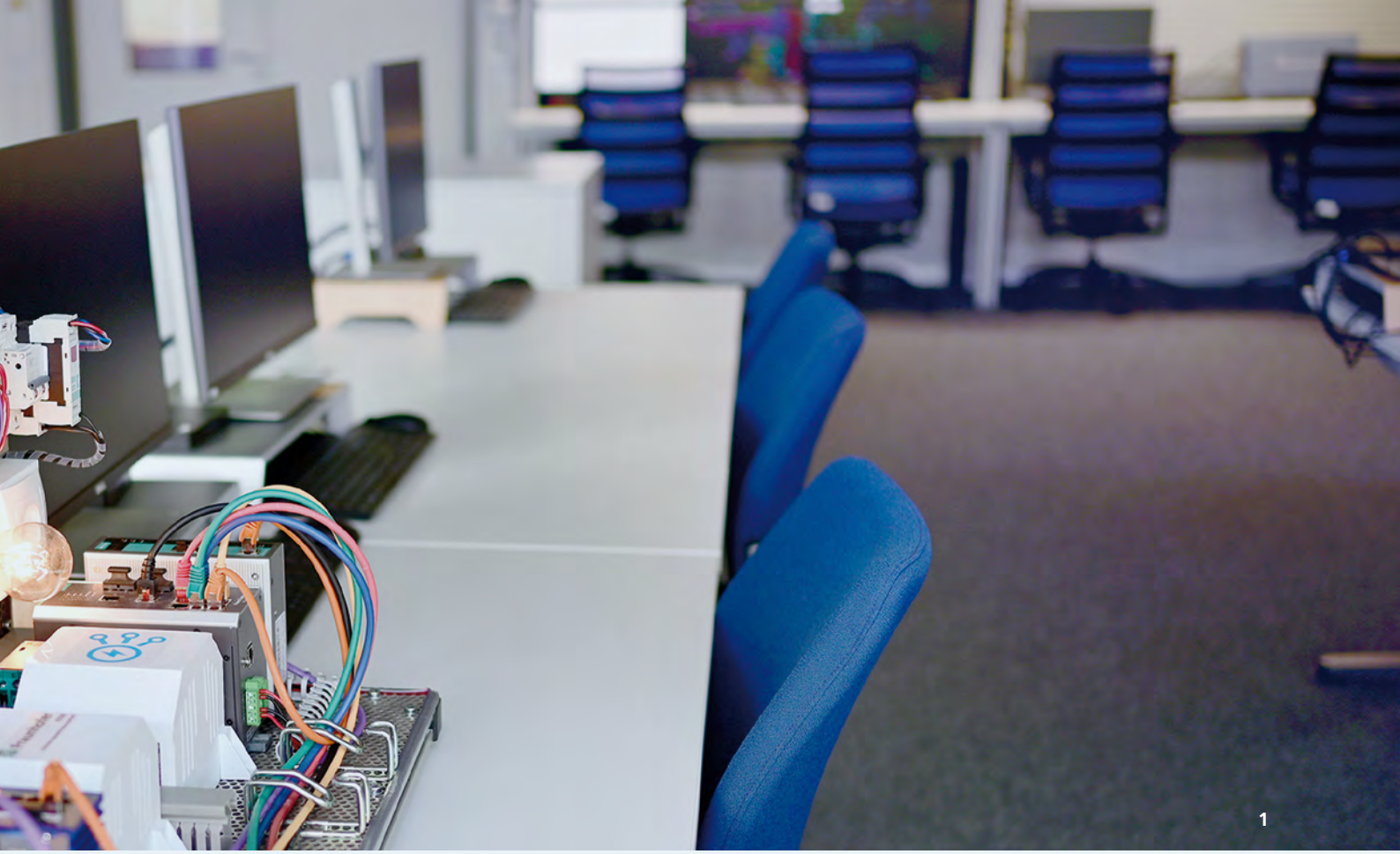
Know-how für mehr IT-Sicherheit

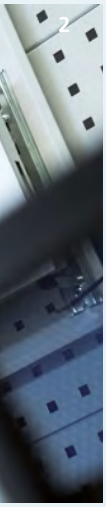
Energie- & Wasserversorgung und Public Safety

www.cybersicherheit.fraunhofer.de

Inhalt







Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy im Bereich Information und Kommunikation. Im Zentrum des umfassenden Angebots des Lernlabors stehen alle Themen rund um die IT-Sicherheit.

Impressionen aus unseren Lernlaboren Cybersicherheit:

1 Der mobile Demonstrator als Schulungsplattform für den Einsatz im technischen Intensivtraining.

2 Echtzeitfähiges Simulationssystem zur wirklichkeitsnahen Nachbildung von Energie- bzw. Wassersystemen.

3 Trainingsinfrastruktur in der Schulungsumgebung im Lernlabor Cybersicherheit Energie- und Wasserversorgung in Ilmenau.

4 Lernlabor Cybersicherheit des Fraunhofer IOSB-AST: als Anwendungsfall dient z. B. ein realer Prozess aus der Feldebene der Energieversorgung, für den verschiedene Angriffsszenarien auf die IT- und OT-Infrastruktur entworfen wurden.

Mehr Sicherheit mit unseren Weiterbildungen

5 Gründe für die Weiterbildung im Lernlabor Cybersicherheit

5

Anerkannte Expertinnen und Experten

Profitieren Sie vom langjährigen Spezialwissen unserer Expertinnen und Experten aus der Forschung und unseren Entwicklungs- und Beratungsprojekten. In Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen erhalten Sie verwertbare, neueste Erkenntnisse auf allen Gebieten der Cybersicherheit.

Bei uns bekommen Sie Wissen aus erster Hand

Unsere Kurse sind nicht nur auf dem aktuellsten Stand der Forschung, sie orientieren sich auch passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Im Team trainieren und erarbeiten Sie Lösungskonzepte in den Bereichen, die für Sie tatsächlich relevant sind.

Maßgeschneiderte Inhouse-Seminare

Integrieren Sie die Weiterbildung zum Thema Cybersicherheit direkt in Ihr Unternehmen, für mehrere Mitarbeitende oder Abteilungen. Dafür passen wir die Inhalte individuell auf Ihre Bedarfe an. Wir beraten Sie gerne, welche Lösung für Sie die optimale darstellt.

Für jede Situation das passende Seminar

Ein Universalkonzept bei IT-Sicherheitslösungen gibt es nicht! Die Komplexität und das Spektrum an Problemfeldern ist einfach zu groß. In unserem breiten Themenangebot finden Sie jedoch garantiert die passende Weiterbildung. Zugeschnitten auf Ihren Kenntnisstand und auf Ihr Spezialgebiet. Ob als Onlineseminar, Präsenzseminar oder Mix aus beidem.

Lernlabore

An zahlreichen Standorten in Deutschland können Sie in unseren modernen Lernlaboren mithilfe hochwertiger technischer Infrastruktur reale Bedrohungsszenarien nachstellen und durchspielen. Anhand konkreter Anwendungsfälle wird so das Gelernte für Sie erfahrbar und direkt umsetzbar.

Kompetenzaufbau auf allen Ebenen

IT-Sicherheitswissen betrifft nicht mehr nur Spezialistinnen und Spezialisten, auch entscheidungsbefugte Personen, Fachkräfte und Anwendende sollten lernen, Sicherheitsrisiken abzuschätzen und diese zu beherrschen. Hierfür benötigen die Mitarbeitenden eine Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und die Konsequenzen von IT-Sicherheitsproblemen in ihrem Verantwortungsbereich. Das Lernlabor richtet sich deshalb an folgende Zielgruppen mit jeweils spezifischen Seminaren:

Führungskräfte, die Entscheidungsprozesse verantworten müssen, benötigen einen verständlichen Überblick über aktuelle Gefahren, Sicherheitsstrategien und Methoden.

Sicherheitsexpertinnen und -experten mit einer IT-Sicherheits-ausbildung oder entsprechender Berufserfahrung können ihr Wissen auf den neuesten Stand bringen.

Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

IT-Nutzerinnen und -Nutzer ohne spezifische Fachkenntnisse, von denen erwartet wird, dass sie Sicherheitsbewusstsein aufbauen und sicherheitskonformes Verhalten entwickeln.

Erklärung der Symbole auf den Seminarseiten

- Abschluss
- Voraussetzungen
- Zielgruppe
- Dauer
- Kosten
- Örtlichkeit

Energie- und Wasserversorgung

Infrastrukturen werden immer komplexer

Angriffe auf kritische Infrastrukturen wie bei der Energie- und Wasserversorgung können verheerende Schäden anrichten. Doch Cyberattacken in diesem Bereich wachsen zunehmend an: Hacking-Angriffe, Manipulationen oder Eingriffe und Missbrauch der Konfiguration. Cybersicherheit in diesem KRITIS-Bereich gehört deshalb zu den wichtigsten, zukünftigen Herausforderungen.

Unternehmen auf dem Energie- und Wasserversorgungsmarkt entwickeln immer smartere Methoden zur Prozessoptimierung. Neue Technologien ermöglichen Kostensenkung und Effizienzsteigerungen. Da auch in Versorgungsunternehmen für Energie und Wasser die Vernetzung gestiegen ist, entstehen neue potenzielle Schwachstellen. Insbesondere Verteilnetze, Komponenten und spezifische Netzwerkprotokolle sind aufgrund ihres Einsatzes prädestiniert für Angriffe.

Doch aufgrund der steigenden Digitalisierung entsteht Abhängigkeit von automatisierten Prozessen und IT-Systemen. So steigt die Anfälligkeit für Cyberattacken. Unbemerkter Diebstahl, Ausfall einzelner Systeme bis hin zum Versorgungsblackout sind denkbar. In unserem Lernlabor können komplette IT- und Hardwareinfrastrukturen flexibel nachgebildet werden. Das Kernstück bildet dabei ein OPAL-RT-Teststand für Hardware-in-the-Loop-Tests im Verbund mit variabel konfigurierbarer IT-Umgebung. Vom einfachen Bürorechner über VLAN-Separation unter Verwendung von Industriefirewalls bis hin zum Einsatz von teilvirtualisierten IT-OT-Umgebungen können damit die meisten heterogenen und vielfältigen IT-Systemlandschaften nachgebildet werden.

Die einzigartige Laborumgebung mit der Vereinigung von Automatisierungsprozessen der Energietechnik und IT-Netzwerkumgebung bietet ideale Voraussetzungen für anwendungsnahe Forschung. Vielfältige Szenarien lassen sich umsetzen zur grundlegenden Untersuchung von Sicherheitsaspekten in Kommunikationsnetzen bis hin zur individuellen Nachbildung realer Infrastrukturen und Bewertung des vorliegenden Sicherheitsniveaus. Eine Reihe von realen Prozessen mit Ankopplung zu virtuellen Umgebungen und der Integration in ein Stations- und Netzleitsystem bilden hierfür die Basis.

Sie lernen von unseren Expertinnen und Experten, wie Sie Bedrohungssituationen analysieren und Schwachstellen erkennen können, dabei ist das Lernlabor nicht nur Bestandteil unseres Schulungsportfolios, sondern dient auch der angewandten Forschung im Bereich Cybersicherheit, von der Sie schon heute in unseren Angeboten profitieren können

»Das Seminar ›IT-Sicherheit für Kritische Infrastrukturen‹ hat mich durch die sehr kompetenten Vorträge und erfrischenden Diskussionen überzeugt.«

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

IT-Sicherheit für die Energie- und Wasserversorgung

Gefahrenlage & Awareness für Versorgungsunternehmen

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.

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

Inhalte des Seminars

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?

Ihr Nutzen

- Nach dem Seminar können Sie viele verschiedene Angriffsbeispiele und deren Risiko aufs 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.

Energie- und Wasserversorgung | **Präsenz**

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

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

IT-Sicherheit für Energie- und Wasserversorgung

Angriffe abwehren bei kritischen Infrastrukturen

Informationen im Überblick

- Keine Voraussetzungen
- Führungskräfte, Fachkräfte und Spezialisten*innen
- 2,5 Tage
- 540,–
- online

Veranstaltet durch

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Hochschule Zittau/Görlitz

Referenten:

M.Sc. Dennis Rösch, wiss. Mitarbeiter Fraunhofer IOSB-AST

M.Sc. Marcel Kühne, wiss. Mitarbeiter Fraunhofer IOSB-AST

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/it-sicherheit-energie-wasser-online

Die Herausforderung: Für die Bedrohungslage gewappnet sein. Cyber-Angreifer entwickeln immer größere Fähigkeiten. Gerade automatisierte Prozesse und IT-Systeme bieten Angriffsfläche. Schützen Sie ihre Strukturen durch gezielte IT-Sicherheitsvorkehrungen. Informieren Sie sich, und bleiben Sie auf dem neusten Stand. In diesem Seminar erfahren Sie, welche gesetzlichen Anforderungen auf Sie zukommen, und wie Sie mit vorhandenen Richtlinien Ihr System schützen.

Inhalte des Seminars

Welche Angriffe auf Versorgungsunternehmen 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?

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

Welche Gesetze gelten für Kritische Infrastrukturen?

Welche Standards und Normen der IT-Sicherheit und technischen Umsetzung existieren?

Wie kann ich mich selbst vor Cyberangriffen schützen?

Wie sensibilisiere ich meine Mitarbeitenden nachhaltig?

Virtuelle Vorführung und Demonstration von Angriffen auf eine Mobile Schulungsplattform der Cyber-Kill-Chain.

Ihr Nutzen

- Nach dem Seminar kennen Sie die gesetzlichen Anforderungen zur IT-Sicherheit in der Energie und Wasserversorgung.
- Sie wissen, wie Sie ihre eigenen Infrastrukturen absichern.
- Sie lernen verschiedene Angriffsszenarien kennen.
- Sie wissen, wie Sie Gefahren konkret begegnen können.

Energie- und Wasserversorgung | **Präsenz**

Informationssicherheitsmanagement für Anlagenbetreiber

Cybersicherheit umfassend und prozessorientiert herstellen

Die Herausforderung: Richtige und prozessorientierte Einführung eines IT-Sicherheitsmanagements als Anlagenbetreiber. Ab März 2021 verpflichtet der IT-Sicherheitskatalog (EnWG) Anlagenbetreiber im KRITIS-Umfeld zur Umsetzung eines Informationsmanagementsystems und dessen Zertifizierung. Was kommt damit auf Führungsverantwortliche zu? Dieses Seminar liefert eine Einführung in den neuen Standard und befähigt zur Realisierung prozessorientierter Lösungskonzepte für die Cybersicherheit ihres Unternehmens.

Inhalte des Seminars

Hintergründe und Notwendigkeiten

Gesetzlicher Rahmen für die Umsetzung eines Informationsmanagementsystems
- Was schreibt der Gesetzgeber vor?
- Was ist zusätzlich sinnvoll?

Tools im IT-Sicherheitsmanagement
- Welche Werkzeuge unterstützen mich bei der Etablierung eines IT-Sicherheitsmanagementsystems?

Auf dem Weg zur Zertifizierung
- Was muss ich für zertifizierte IT-Sicherheit alles umsetzen?

Umsetzung von IT-Sicherheit im Unternehmen
- Wie etabliere ich Prozesse, wie ändere ich meine Prozesse möglichst kostenschonend?

Faktor Mensch
- Welche Rolle spielen die Mitarbeitenden, welche die Geschäftsführung?

Ihr Nutzen

- Nach dem Seminar können Sie Prozesse in Ihrem Unternehmen untersuchen sowie Risiken und Schwachstellen identifizieren und bewerten.
- Sie lernen, den gesetzlichen Rahmen für die Umsetzung eines Informationssicherheitsmanagementsystems zu beurteilen.
- Sie können die verschiedenen Standards und Standardvorgehensweisen voneinander abgrenzen und hinsichtlich ihres Aufwands bewerten.
- Ihr Unternehmen ist auf eine Zertifizierung vorbereitet.

Informationen im Überblick

Verständnis für Managementprozesse & rechtliche Aspekte zur Implementierung von Informationssicherheitsmanagementsystemen

Führungskräfte, Mitarbeitende aus dem Management, IT-Sicherheitsbeauftragte

2 Tage Präsenz

1200,–

Ilmenau, Görlitz, inhouse

Veranstaltet durch

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Hochschule Zittau/Görlitz

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/informationssicherheitsmanagement-anlagenbetreiber

Informationen im Überblick

Grundkenntnisse Elektrotechnik & Netzwerksicherheit sowie deren Konfiguration bei Automatisierungstechnik, gute Kenntnisse Netzwerktechnik

IT-Sicherheitsbeauftragte, Mitarbeitende der Feld- und Leittechnik, techn. Mitarbeitende in der Energie- und Wasserversorgung

2 Tage Präsenz

1200,–

Ilmenau, Görlitz, inhouse

Veranstaltet durch

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Hochschule Zittau/Görlitz

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/sichere-konfig-und-absicherung-e-und-w

»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

Sichere Konfiguration und Absicherung der Energieversorgungsinfrastruktur

Technisches Intensivtraining

Die Herausforderung: Absicherung der heterogenen Systemlandschaft in der Energietechnik. Die gestiegene Vernetzung in der Energieversorgung macht IT-Sicherheit nicht allein zur Aufgabe bei einzelnen Automatisierungssystemen, sondern betrifft das gesamte Netzwerk. Nur mit der richtigen Awareness für die Kommunikationsformen, und wie sie genutzt werden, können geeignete Sicherheitskonzepte implementiert werden. In diesem Seminar erhalten Sie Einblick in die Perspektive des Angreifers und können so geeignete Absicherungsmaßnahmen umsetzen.

Inhalte des Seminars

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

Ziele
- 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.

Ihr Nutzen

- Nach dem Seminar verstehen Sie das Vorgehen von Angreifern auf die Energieautomatisierung.
- Sie können Gefahrenpotenzial von verschiedenen Konfigurationen einschätzen.
- Sie verstehen, welche Methoden Sie zur Angriffsabwehr einsetzen müssen.
- Sie können Automatisierungskomponenten sicher konfigurieren und vernetzen.
- Sie sind in der Lage, Netzwerksicherung und -monitoring vorzunehmen.

Cyber security for the Energy Sector

Der passende Einstieg

Die Herausforderung: Gestiegene Komplexität bei kritischen Infrastrukturen durch Digitalisierung. Digitalisierung ermöglicht Flexibilität und Effizienz. Doch mit der zunehmenden Verknüpfung zwischen den Prozess- und Leitsystemen entstehen potenzielle Einfallstore für Eingriffe. Lernen Sie in diesem Seminar anhand echter Beispiele, wie Angriffe auf kritische Infrastrukturen ablaufen. Welche Besonderheiten gibt es bei der Anwendung und Implementierung von ISMS im Energiesektor? Dieses Online Skill bietet einen umfangreichen Einstieg.

Inhalte des Seminars

Introduction Cyber Attacks

ISMS – Legal Backgrounds

ISMS in the Energy Sector

Authentication and Authorization Techniques

IT Network Zoning and Segmentation

Securing Remote Access

Intrusion Detection Systems and Network Monitoring

Human Factor in IT Security: Social Engineering

Social Engineering: How to Protect Yourself

Ihr Nutzen

- Nach dem Seminar wissen Sie, welche aktuellen und potenziellen Angriffsvektoren existieren.
- Sie haben ein Verständnis von den rechtlichen Rahmen für ISMS, GDPR und ISO 27001.
- Sie wissen, wie man IT Security im Energiesektor managen kann, insb. mit ISMS-Implementierung.
- Sie wissen, wie Sie ein Security-Awareness-Programm in ihrem Unternehmen umsetzen.

Informationen im Überblick

Keine Voraussetzungen

IT-Sicherheitsbeauftragte, Mitarbeitende der Feld- und Leittechnik, techn. Mitarbeitende in der Energie- und Wasserversorgung

6,5 Stunden

400,–

online

Veranstaltet durch

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

University4Industry

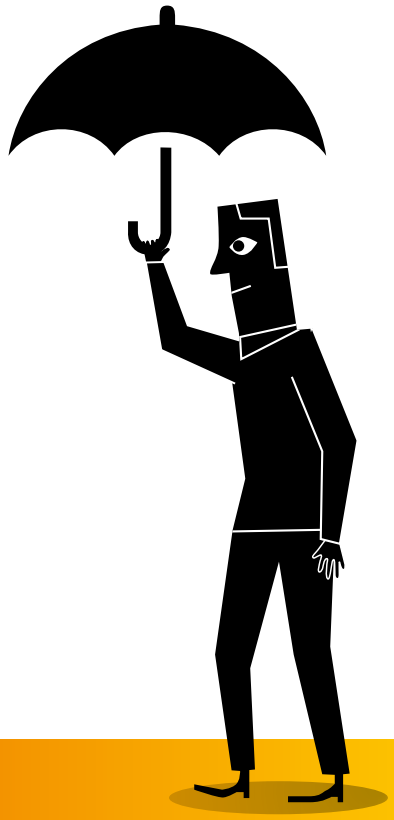
Hochschule Zittau/Görlitz

Weitere Infos und aktuelle Termine buchen unter:

www.university4industry.com/skills/cybersecurity-for-the-energy-sector

Public Safety

Öffentliche Sicherheit braucht starke Strukturen



Bestimmte Branchen, wie z.B. Finanzen, Ernährung oder Strom- und Wasserversorgung, stehen unter erhöhtem öffentlichen Interesse. Beeinträchtigungen oder gar Ausfälle in diesem Bereich würden massive Schäden auf wirtschaftlicher und gesellschaftlicher Ebene bedeuten. Aber auch hier spielt die digitale Infrastruktur und Vernetzung eine wichtige Rolle. So wird Cybersicherheit bei Public Safety zu einer besonders sensiblen Herausforderung.

Die Gewährleistung der Funktionstüchtigkeit der IT-Systeme steht hier an besonderer Stelle: Bedrohungen müssen rechtzeitig erkannt und sichtbar gemacht werden. Auch weil in diesem Feld oft ein reger Austausch zwischen Wirtschaft, Politik und Gesellschaft besteht. Dabei spielen nicht nur technische Eingriffe wie Cyberattacken eine Rolle, sondern auch organisatorisches Versagen. Hinzu kommen Bundesverordnungen wie das IT-Sicherheitsgesetz und EU-Datenschutzverordnungen, die umgesetzt werden müssen. In diesem speziellen Geflecht ist die Orientierung und Priorisierung unterschiedlicher Problemfelder nicht ganz einfach.

Cybersicherheit wird bei Public Safety zu einer besonders sensiblen Herausforderung.

Cyberkriminalität muss vorgebeugt werden, und man muss sie unter gezieltem, sachgerechten Einsatz entsprechender Maßnahmen abwehren. Strategische wie organisatorische Aspekte sind hierbei nicht zu unterschätzen. Zudem gibt es nach dem IT-Sicherheitsgesetz regelmäßige Sicherheitsaudits, die dafür sorgen, dass Unternehmen ständig auf dem Prüfstand stehen.

Im Lernlabor Cybersicherheit lernen Sie aktuelle Bedrohungen für den öffentlichen Sektor kennen. Auf Basis wissenschaftlicher Erkenntnisse werden Sie mit den aktuellen Trends vertraut gemacht. Durch die verschiedenen Kurse erfahren Sie, wie Sie strategisch sinnvoll im Bedrohungsfall agieren können. Sie profitieren direkt von der wissenschaftlicher Expertise und unternehmensgerechten Ansätzen.

Grundlagen der IT-Sicherheit für Public-Safety-Infrastrukturen

Grundlegende Anforderungen

IT-Systeme für die öffentliche Sicherheit und von kritischen Infrastrukturen benötigen besondere Aufmerksamkeit in der IT-Sicherheit. Das Seminar unterstützt Sie dabei, den Stand der IT-Sicherheit in Ihrem Unternehmen mittels einfachen Checklisten zu erfassen. Dadurch erstellen Sie die Grundlage, um den spezifischen Schutzbedarf zu ermitteln, spezifische Sicherheitsmaßnahmen umzusetzen und sich für den Notfall zu wappnen.

Inhalte des Seminars

Besondere Bedrohungen für IT-Systeme der öffentlichen Sicherheit und kritischer Infrastrukturen
- Bedrohungs- und Angriffsszenarien
- Analysen zum Stand der Sicherheit
- Bring your own device
- IT-Notfallmanagement
- IT-Risikomanagement
- Sicherheitskonzepte

Anforderungen des IT-Sicherheitsgesetzes
- Entwicklung und Grundlagen des IT-Sicherheitsgesetzes
- Ableitung der Anforderungen an die relevanten Sektoren
- Nachweispflichten und Durchführung von Sicherheitsaudits
- Verfahren zur Detektion, Analyse und Meldung von IT-Sicherheitsvorfällen
- Anforderungen an IT-Systeme in Entwicklung, Einführung und Betrieb

Anforderungen der EU-Datenschutzgrundverordnung
- Definition von personenbezogenen Daten
- Pseudonymisierung und Anonymisierung
- Datenschutzkonzept und Umsetzung
- Ausnahmeregelungen im Sicherheitskontext
- Anwendung von Security by Design

Ihr Nutzen

- Nach dem Seminar können Sie Risiken identifizieren (Risk Identification), analysieren (Risk Analysis), evaluieren und bewerten (Risk Evaluation).
- Sie sind in der Lage, Bedrohungen zu erkennen und Maßnahmen zu entwickeln.
- Sie können analysieren, was zu den kritischen Prozessen Ihres Unternehmens gehört, eine Schadensanalyse in Ihrem Unternehmen durchführen und ein zugeschnittenes Notfallmanagement nach dem BSI-Standard 100-4 entwickeln.

Informationen im Überblick

Keine Voraussetzungen

IT-Sicherheitsbeauftragte, IT-Risikomanager, Business Continuity Manager, CISOs, Krisenmanager, Risikomanager, Verantwortliche aus den Bereichen Compliance, Corporate Governance und interne/externe Revision, Qualitätsmanager, Projektleiter*innen für IT-Systeme, Projektleiter*innen in der Produktentwicklung im Bereich kritische Infrastrukturen (KRITIS) und Behörden/Organisationen mit Sicherheitsaufgaben (BOS)

12 Stunden
on Demand-Kurs

800,–

Online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu,
wiss. Mitarbeiter
Fraunhofer FOKUS

Michael Holzhüter,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/grundl-public-safety-infrastrukturen

Inhouse- oder Firmen- und Behördenschulungen

Inhouse-Schulungen individuell auf Sie zugeschnitten

Wollen Sie Inhalte aus unserem Kursangebot individuell zusammenstellen, oder finden Sie in unserem Angebot keinen passenden Termin oder Ort? Kein Problem: Stellen Sie Ihre ganz persönlichen Bedürfnisse in den Vordergrund.

Sie haben die Wahl, so geht's:

- Wählen Sie ein Wunschseminar aus unseren vielfältigen Themen aus und bestimmen Sie den Zeitraum und Schulungsort.
- Nennen Sie uns Inhalte aus unseren Kursangeboten, die geschult werden sollen, und wir konzipieren ein passendes Seminar.
- Sie sagen uns, welches spezielle Wissen geschult werden soll, und wir entwickeln eine individuelle Schulung für Sie.

Bei einem individuellen Inhouse-Seminar erhalten Sie genau auf Ihre Bedürfnisse abgestimmtes Wissen – für Ihr Unternehmen, Abteilungen Ihres Unternehmens, für Ihre Behörde, Fachreferate oder einzelne Mitarbeiterinnen und Mitarbeiter. Dabei stehen wir Ihnen sehr gerne beratend zur Verfügung, wenn es um für Sie maßgeschneiderte, inhaltliche Zusammenstellung der vielfältigen Kombinationsmöglichkeiten unserer Themen geht.

Wir als Lernlabor Cybersicherheit bieten Ihnen alle relevanten Elemente aus einer Hand: Die didaktische, mediale sowie technische Umsetzung der Inhalte, aber auch Konzept und Umsetzung.

Fragen Sie uns an!

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne

telefonisch unter +49 89 1205-1555

e-mail: cybersicherheit@fraunhofer.de

www.cybersicherheit.fraunhofer.de

Hier erhalten Sie aktuelles Wissen!

Aktuelle Informationen zu unseren Seminarangeboten, Veranstaltungen und Themen im Bereich Cybersicherheit finden Sie hier:

www.cybersicherheit.fraunhofer.de

Stöbern Sie in unserem Blog und erfahren Sie, was unsere Fachexpertinnen und -experten über aktuelle Themen im Bereich Cybersicherheit berichten:

www.cybersicherheit.fraunhofer.de/de/blog

Abonnieren Sie unseren Newsletter und bleiben Sie so auf dem Laufenden:

www.cybersicherheit.fraunhofer.de/newsletter

Weitere Informationen rund um das Thema Weiterbildung bei der Fraunhofer Academy erhalten Sie hier:

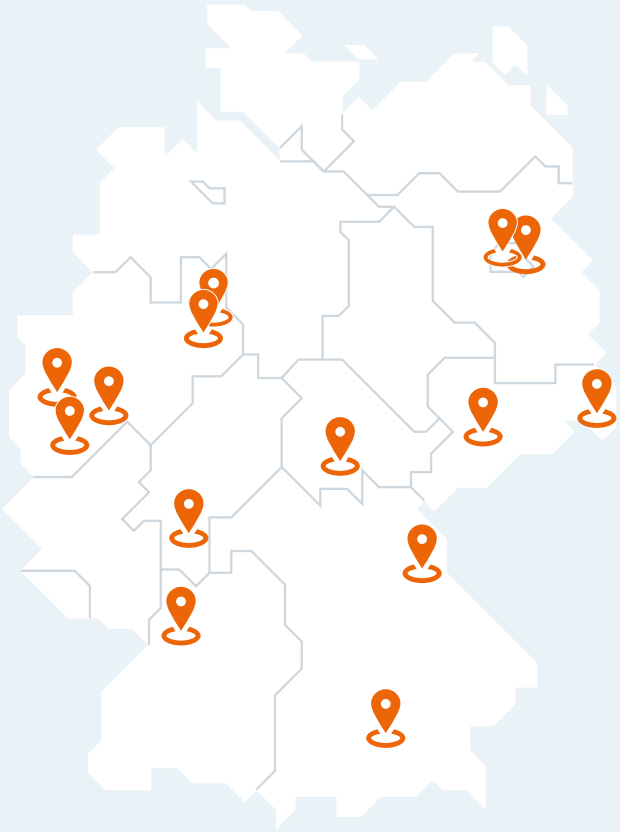
Aktuelle Qualifizierung aus der angewandten Forschung

Das Lernlabor Cybersicherheit ist ein Weiterbildungsprogramm, in dem Expertinnen und Experten von Fraunhofer und ausgewählten Fachhochschulen aktuellste Erkenntnisse auf dem Gebiet der Cybersicherheit vermitteln. Die Lehrmodule werden von den beteiligten Fraunhofer-Instituten und Fachhochschulen entwickelt und weitergegeben. Die Fraunhofer Academy ist die Geschäftsstelle und Plattform der Initiative, die Entwicklung, Vermarktung, Teilnehmermanagement und Qualitätssicherung koordiniert. Das Programm wird durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Die beteiligten Partnerhochschulen

- Ostbayerische Technische Hochschule Amberg-Weiden
- Hochschule für Technik und Wirtschaft Berlin
- Hochschule Bonn-Rhein-Sieg
- Hochschule Mittweida
- Hochschule Niederrhein
- Technische Hochschule Ostwestfalen-Lippe
- Hochschule Zittau/Görlitz

Standorte der Lern- und Forschungslabore der beteiligten Fraunhofer-Institute und Fachhochschulen



Die beteiligten Fraunhofer-Institute

- Fraunhofer AISEC
- Fraunhofer FKIE
- Fraunhofer FOKUS
- Fraunhofer IEM
- Fraunhofer IOSB
- Fraunhofer IOSB-AST
- Fraunhofer IOSB-INA
- Fraunhofer SIT

Know-how schafft Sicherheit! Seit 5 Jahren unterstützen wir deshalb Unternehmen auf dem Weg zu mehr IT-Sicherheit.«

Dr. Raphaela Schätz,
Qualitäts- und Programm Management
im Lernlabor Cybersicherheit

Herausgeber

Fraunhofer Academy
Hansastraße 27c
80686 München

Telefon +49 89 1205-1555
Fax +49 89 1205-77-1599

cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Redaktion: Elly Leimenstoll

Layout und Satz, Illustrationen:
Vierthaler & Braun

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne
- telefonisch unter + 49 89 1205-1555
- per E-Mail: cybersicherheit@fraunhofer.de
- auf unserer Website unter

www.cybersicherheit.fraunhofer.de

Wir beraten Sie gerne, welche Weiterbildungen und Inhalte für Sie hilfreich sind.

Sie suchen nach Angeboten für Ihr Team?

Für Unternehmen bieten wir Inhouse-Schulungen und unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung. Wir erheben gemeinsam mit Ihnen den Kompetenzbedarf in Ihrer Abteilung oder Firma und beraten Sie, die richtigen Fähigkeiten in Ihrer Organisation aufzubauen.

Adem Salgin

Ihr Ansprechpartner im Lernlabor Cybersicherheit

Seminarberatung
und Anmeldung

Möchten Sie Informationen zu einem anderen Themengebiet?

Hier finden Sie alle Broschüren rund um die Weiterbildungen im Lernlabor Cybersicherheit: **www.cybersicherheit.fraunhofer.de/downloads**

Stand Mai 2022

Sie erreichen uns

– telefonisch unter +49 89 1205-1555
– per E-Mail: cybersicherheit@fraunhofer.de
– auf unserer Website unter

www.cybersicherheit.fraunhofer.de