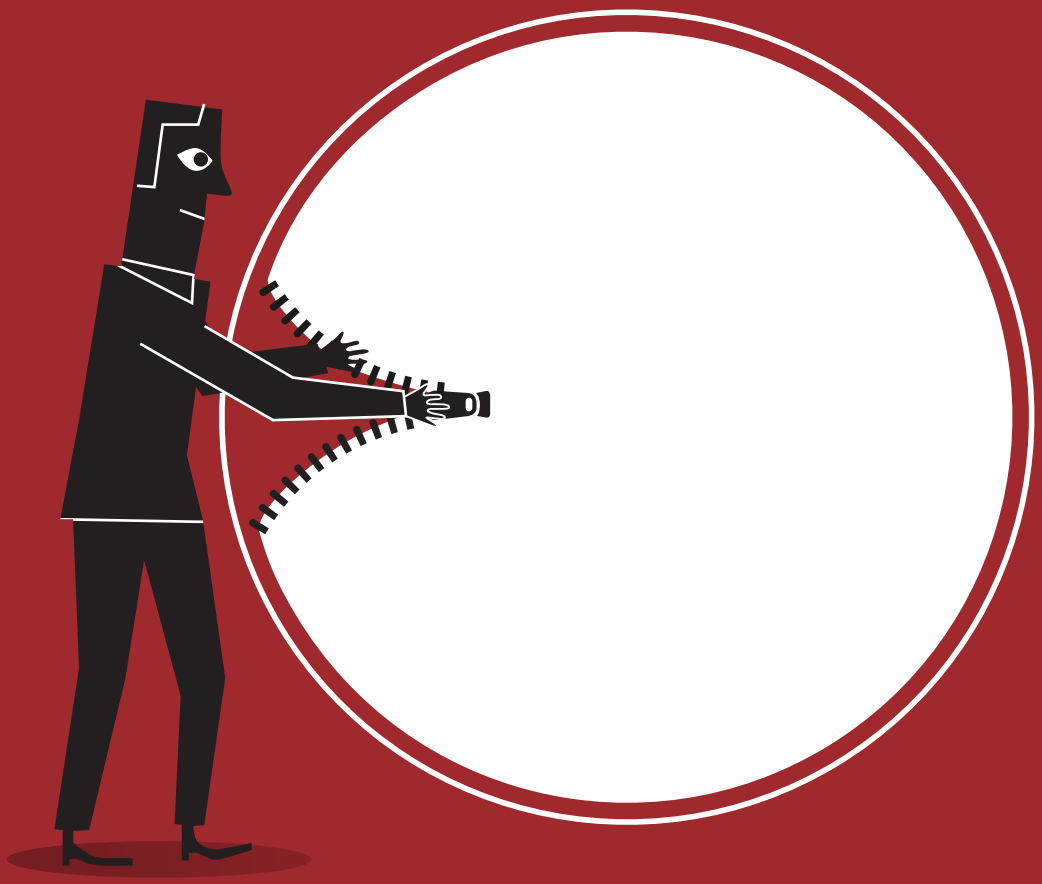
Lernlabor
Cybersicherheit

SEMINARKATALOG

1. Halbjahr 2019

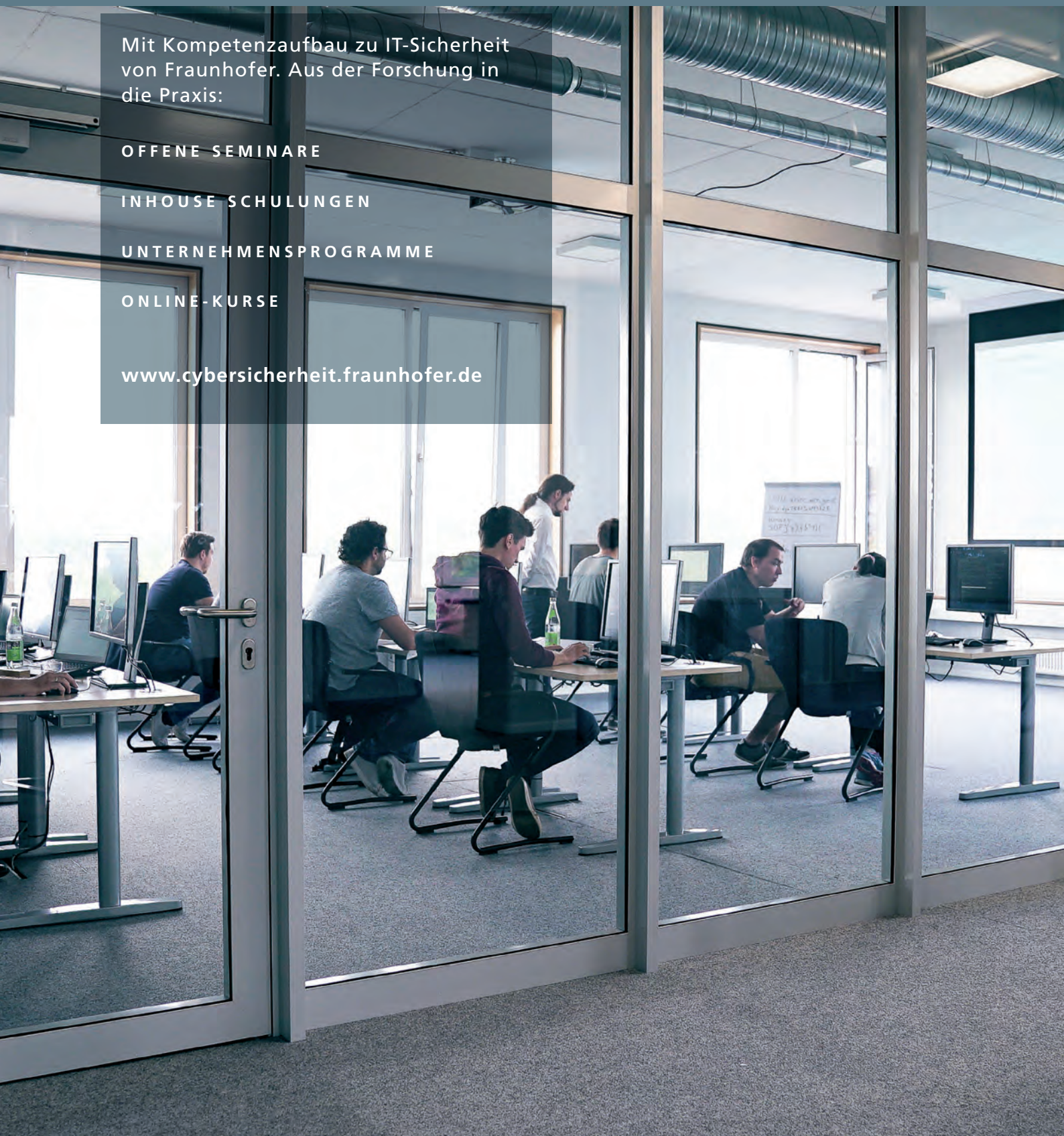


LÜCKEN SCHLIESSEN

MIT WEITERBILDUNG ZU IT-SICHERHEIT

Fraunhofer
ACADEMY

SICHERHEITSLÜCKEN UND WISSENSLÜCKEN SCHLIESSEN



Mit Kompetenzaufbau zu IT-Sicherheit von Fraunhofer. Aus der Forschung in die Praxis:

OFFENE SEMINARE

INHOUSE SCHULUNGEN

UNTERNEHMENSPROGRAMME

ONLINE-KURSE

www.cybersicherheit.fraunhofer.de

»Die berufsbegleitende Weiterbildung zur IT-Sicherheit ist für die Deutsche Telekom AG sehr wichtig. Insbesondere ein Angebot kleinerer Weiterbildungsmodule, in denen Personen sehr transferorientiert und kompakt in aktuellen Themen und insbesondere in der Anwendung aktueller Werkzeuge geschult werden, begrüßen wir sehr.«
Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense bei der Deutschen Telekom AG

INHALT

Hacking-Workshop des Fraunhofer AISEC im e-House Weiden

KNOW-HOW FÜR EINE SICHERE DIGITALE WIRTSCHAFT

Lücken in ihrer IT-Sicherheit sind Unternehmen oft gar nicht bekannt – den Hackern aber schon. Denn Angriffstechniken werden ausgefeilter, und mit der steigenden digitalen Vernetzung nehmen auch Möglichkeit sowie Wahrscheinlichkeit für Cyberattacken weiter zu. Mit Weiterbildungen zu IT-Sicherheit können Sie diese Wissenslücken schließen und damit Cyberangriffe verhindern.

In der Weiterbildungsinitiative Lernlabor Cybersicherheit schulen die Experten von Fraunhofer und Fachhochschulen praxisnah zu den aktuellsten Themen der IT-Sicherheit. Mitarbeiterinnen und Mitarbeiter aus Unternehmen können so ihre Kompetenzen zu IT-Sicherheit auf den neuesten Stand bringen und weiter spezialisieren.

Besonderes Merkmal dieses Weiterbildungsprogramms ist die Anwendungsorientierung: In den Lernlaboren stehen den Teilnehmenden sowohl die passende technische Infrastruktur als auch die Fachexperten zur Verfügung, um reale Bedrohungsszenarien nachzustellen und geeignete Lösungskonzepte zu ergründen.

Die Schulungen sind für unterschiedliche Wissens-Levels und Rollen im Unternehmen ausgerichtet: Auf Entscheiderinnen und Entscheider der Management-Ebenen, Spezialisten und Sicherheitsexperten sowie Fachkräfte und Anwender. An zahlreichen Standorten in Deutschland erhalten sie eine kompakte Qualifizierung in modular aufgebauten Seminaren.

Da IT-Sicherheit in jedem Betrieb relevant ist, richtet sich das Angebot an Unternehmen und Behörden aller Branchen und Domänen: Für spezialisierte Bereiche wie Energie- und Wasserversorgung, industrielle Produktion oder Domänen wie Mobile Security und Embedded Systems bietet das Lernlabor Cybersicherheit darauf ausgerichtete Kurse und Lernpfade an.

Weiterbildung im Lernlabor Cybersicherheit – Ihr Nutzen auf einen Blick

Aktuellstes Forschungswissen
praxisnah aufbereitet

Erprobung passgenauer Lösungsstrategien
in hochwertigen Laboren

Kompakte und transferorientierte Formate
ermöglichen berufsintegriertes Lernen

Flexibel kombinierbare Bausteine,
die auf den jeweiligen Bedarf der Unternehmen und Behörden zugeschnitten sind

KOMPETENZAUFBAU FÜR WIRTSCHAFT UND BEHÖRDEN

Um IT-Sicherheitskonzepte wirksam und ganzheitlich umzusetzen, sind sowohl Entscheider als auch Fachkräfte gefragt. Deshalb hat das Lernlabor Cybersicherheit genau für diese Zielgruppen spezielle Seminare im Angebot.

Unsere Zielgruppen: Management, Fachkräfte und Anwender

Der Fokus beim mittleren und gehobenen **Management** liegt in der Sensibilisierung zu aktuellen Bedrohungslagen und Schwachstellen. Die eigene Lage reflektieren und in Verbindung mit aktuellen Problemen des Unternehmens setzen, um Bewusstsein und Verständnis für Cybersicherheit zu erzeugen, stellt einen Teil der Weiterbildung dar. Darüber hinaus findet auch Beratung statt, etwa zu Produktzertifizierung, Organisationsaufbau, Notfallmanagement oder durch Information über aktuelle Standards, Normen und Gesetzeslagen.

Fachkräfte und Spezialisten im Bereich Security und Safety wiederum können ihr bereits profundes Wissen weiter vertiefen und sich spezialisieren. Durch Best Practices, Informationen zu State-of-the-Art und Qualifikation anhand von Fallbeispielen werden die Fachkräfte für aktuelle Bedrohungen und neue Aufgaben fit gemacht.

Anwender und Einsteiger in das Thema IT-Sicherheit werden hinsichtlich eines sicherheitskonformen Verhaltens sensibilisiert. Generelle Informationen zu IT-Bedrohungslage und Umgang mit Daten unterstützen die firmeneigene Informationspolitik.

IT-Sicherheit für Unternehmen und Behörden

Die Module sind nicht nur funktionsspezifisch ausgerichtet, sondern auch branchen- und themenspezifisch auf den Bedarf der Industrie und der öffentlichen Verwaltung abgestimmt. Denn die rasanten Veränderungen in der Informationstechnologie betreffen heute nicht nur Unternehmen in allen Bereichen und Geschäftsfeldern. Auch Behörden benötigen eine große Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und Konsequenzen von IT-Sicherheitsproblemen. Um die digitale Souveränität für alle Wirtschaftszweige und Behörden sicher zu gestalten, bildet das Lernlabor Cybersicherheit Fach- und Führungskräfte aus diesen verschiedenen Bereichen weiter.

Schulung in offenen Seminaren oder Inhouse

In unseren offenen Seminaren können sich einzelne Mitarbeiter weiterbilden und kommen so in den Austausch mit Beschäftigten anderer Unternehmen.

Für mehrere Mitarbeiter oder Abteilungen führen wir die Kurse aber auch beim Unternehmen inhouse durch und passen die Inhalte individuell an.

BRANCHEN

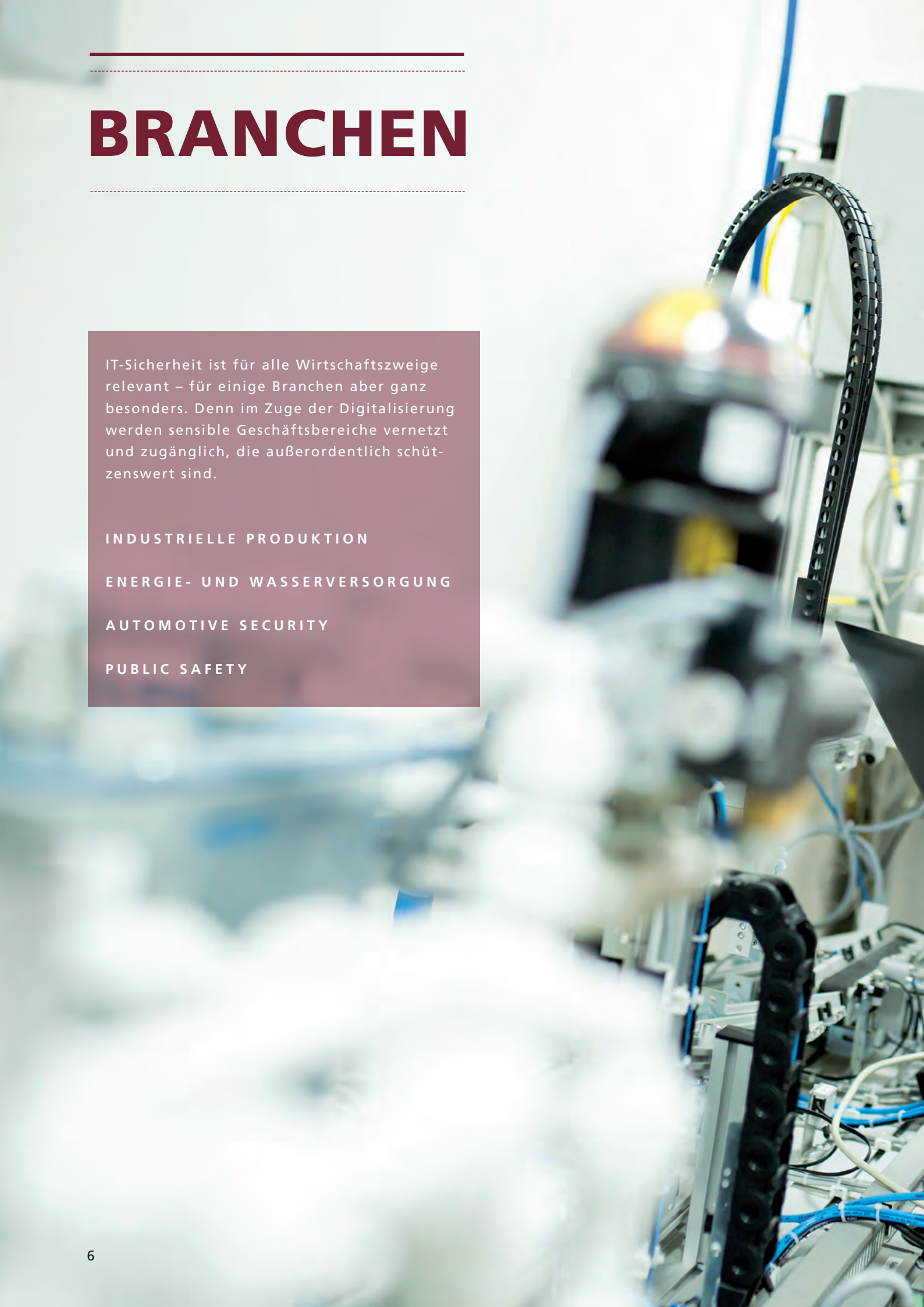
IT-Sicherheit ist für alle Wirtschaftszweige relevant – für einige Branchen aber ganz besonders. Denn im Zuge der Digitalisierung werden sensible Geschäftsbereiche vernetzt und zugänglich, die außerordentlich schützenswert sind.

INDUSTRIELLE PRODUKTION

ENERGIE- UND WASSERVERSORGUNG

AUTOMOTIVE SECURITY

PUBLIC SAFETY

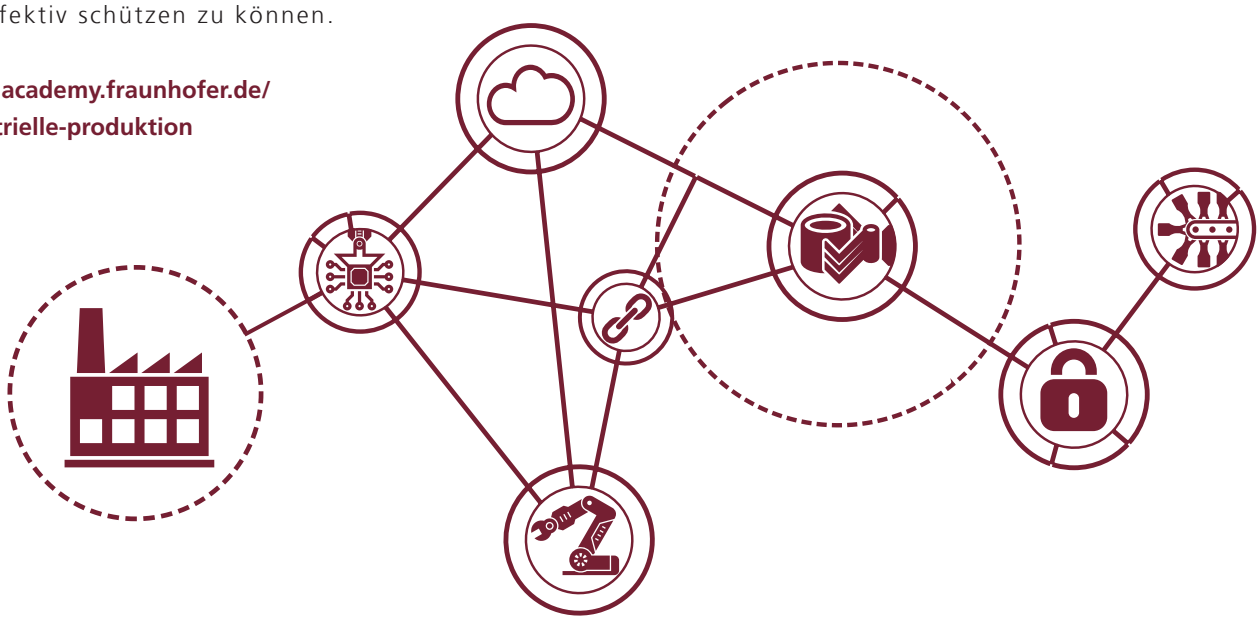


INDUSTRIELLE PRODUKTION

Die Anlagen in einer modernen Produktion sind hochgradig vernetzt: Automatisierungsaufgaben werden über Systeme aus der Cloud gelöst, Anlagen und Systeme kommunizieren selbstständig miteinander, von der Ferne aus werden Wartungen durchgeführt. Damit diese Netzwerk-Verbindungen nicht von Hackern ausgenutzt und Produktionsanlagen lahmgelegt werden, ist IT-Sicherheit in der Produktion essenziell.

Unternehmen müssen im Zuge der digitalen Transformation ihre kritischen Systeme, Anlagen und Werte kennen, um geeignete Schutzmaßnahmen zu ergreifen. Dazu gehört, typische Schwachstellen in Design und Implementierung in eingebetteten Systemen und industriellen Komponenten zu kennen und zu erkennen. Auch neueste Entwicklungen im Bereich von Kommunikations-Protokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software müssen in den Produktionsanlagen umgesetzt werden, um sie effektiv schützen zu können.

www.academy.fraunhofer.de/industrielle-produktion



IT-Sicherheit in der Automatisierungstechnik

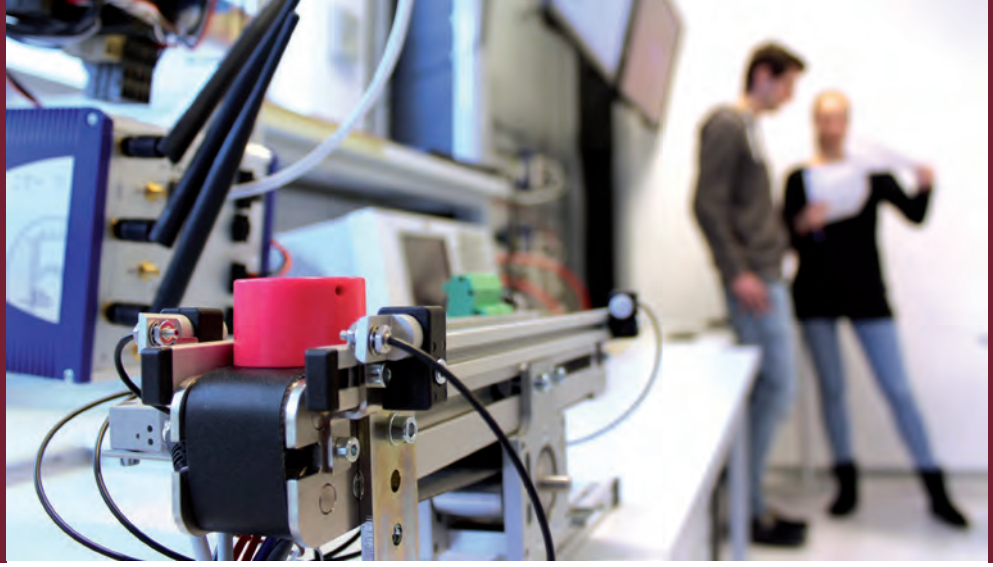
Die sicherheitskritischen Aspekte von Industrie 4.0 analysieren: Industrie 4.0-Anwendungsfälle kennenlernen, sichere Industrie 4.0-Kommunikation mit OPC UA umsetzen, Public Key Infrastrukturen verstehen, Angriffstechniken und Absicherung von Netzwerkinfrastruktur nach IEC 62443 anwenden.

für Mitarbeiter der industriellen Automatisierungstechnik
3 Tage Präsenz | Lemgo | 1.800 €

Sichere Hardware- und Softwareplattformen für Industrie 4.0-Produkte

Sichere Industrie 4.0-Produkte entwickeln: Hardware- und Softwareplattformen bewerten, Sicherheitsanforderungen an die Geräte und Server nach IEC 62443 und Kommunikation mit OPC UA verstehen, Richtlinien für den sicheren Betrieb von Industrie 4.0-Produkten umsetzen.

für Komponentenhersteller, Softwareentwickler
3 Tage Präsenz | Lemgo | 1.800 €



Grundlagen-Know-how Cybersicherheit – Teil I

IT- und Informationssicherheit in der digitalen und vernetzten Produktion verstehen: Grundbegriffe der Informations- und IT-Sicherheit beherrschen, geeignete Schutzmaßnahmen und relevante IT-Sicherheitsstandards kennen, Best-Practice-Beispiele erfahren.

für Informations- und IT-Sicherheitsinteressierte
1 Tag Präsenz | Karlsruhe | 600 €
in Kooperation mit Deutscher Gesellschaft für Qualität (DGQ)

Cybersicherheit in der vernetzten Produktion – Teil II

Das Know-how eines Spezialisten für Cybersicherheit in der vernetzten Produktion erwerben: realistische Angriffsszenarien auf Produktionssysteme identifizieren, mit geeigneten Gegenmaßnahmen reagieren, die Produktion sichern, den rechtlichen Rahmen kennen.

für Fachkräfte und Mitarbeiter in vernetzten Produktionen
4 Tage Präsenz | Karlsruhe | 2.400 €
in Kooperation mit Deutscher Gesellschaft für Qualität (DGQ)

Management-Know-how Cybersicherheit

Grundlagen der Cybersicherheit im Industrie 4.0-Umfeld verstehen: Bewusstsein für Bedrohungslagen und Lösungsstrategien schaffen, rechtlichen Rahmen kennen, Angriffe auf Produktionssysteme und deren Auswirkungen abschätzen, Mitarbeiter sensibilisieren.

für Fach- und Führungskräfte
2 Tage Präsenz | Karlsruhe | 1.200 €
in Kooperation mit Deutscher Gesellschaft für Qualität (DGQ)

Advanced Industrial Cyber Security in Practice

Building cyber security expertise amongst IT/OT managers and engineers: recognizing the relevance of ICS vulnerabilities, identifying incidents and initiating an appropriate response, using selected tools for incident handling, analyze control network traffic.

for IT / OT / IS specialists
2 days live training in English | Ingolstadt | 1.500 €
in cooperation with Kaspersky Lab

IEC 62443-Standards zum Sichern Ihrer Steuerungssysteme (IC32)

Kritische Steuerungssysteme mit IEC 62443-Standards schützen: Sicherheitsprogramm erstellen, Richtlinien für industrielle Sicherheit interpretieren und auf das Unternehmens-System anwenden, Trends bei industriellen Sicherheitsvorfällen und Hackermethoden analysieren.

für Fachkräfte und Mitarbeiter in vernetzten Produktionen
2 Tage Präsenz | Karlsruhe | 1.790 €, Rabatt für ISA-Mitglieder
in Kooperation mit International Society of Automation (ISA)

INDUSTRIELLE PRODUKTION – LERNPFAD

SICHERE INDUSTRIELLE VERNETZUNG

IT-Sicherheit für Industrie 4.0 – Bedrohungslage und Handlungsbedarf

Bewusstsein für die Bedrohungslage industrieller Produktionssysteme schaffen: Grundlagen der IT-Sicherheit für Industrie 4.0 verstehen, Handlungsbedarf abschätzen, Grundzüge der benötigten IT-Sicherheitsprozesse erarbeiten, rechtlichen Rahmen kennen.

für Führungs- und Fachkräfte in vernetzten Produktionen
2 Tage Präsenz | Karlsruhe, Lemgo oder inhouse | 1.200 €

Betrieb sicherer industrieller Netzwerke

Technologien und Mechanismen für einen sicheren Betrieb von industriellen Netzen: Sicherheitsrisiken in der Automatisierungstechnik erkennen, Netzwerke analysieren und Netzwerkinfrastrukturen absichern, mit Sicherheitsvorfällen richtig umgehen.

für Fachkräfte und Mitarbeiter in vernetzten Produktionen
3 Tage Präsenz | Karlsruhe, Lemgo oder inhouse nach Absprache | 1.800 €

Aufbau sicherer industrieller Netzwerke

Industrielle Netzwerke sicher entwerfen und umsetzen: Grundlegende Vernetzungskonzepte und Sicherheitskonzepte kennenlernen, Grundlagen der Netzwerktechnik verstehen, mögliche Angriffsziele in der industriellen Produktion kennen und Gegenmaßnahmen umsetzen.

für Fachkräfte und Mitarbeiter in vernetzten Produktionen
3 Tage Präsenz | Karlsruhe, Lemgo oder inhouse nach Absprache | 1.800 €

Sichere Umsetzung von Industrie 4.0-Anwendungsfällen

Condition Monitoring oder Cloud-Anbindung sicher implementieren: Sicherheitsrisiken in typischen Industrie 4.0-Anwendungen erkennen, Schutzmaßnahmen richtig planen und umsetzen, Industrie 4.0-Kommunikation mit OPC UA verstehen, VPN im Produktionsumfeld einsetzen.

für Fachkräfte und Mitarbeiter in vernetzten Produktionen
3 Tage Präsenz | Karlsruhe, Lemgo oder inhouse nach Absprache | 1.800 €

Demonstrationsanlagen zur standortübergreifenden Produktion im Lernlabor SmartFactoryOWL in Lemgo


ABB
EPSON

ENERGIE- UND WASSERVERSORGUNG

Die Verteilnetze, Komponenten und spezifischen Netzwerkprotokolle von Energie- und Wasserversorgung sind aufgrund ihres Einsatzes besonders für Angriffe exponiert. Die Abhängigkeit von automatisierten Prozessen und IT-Systemen steigt immer weiter an und erhöht die Anfälligkeit von Energie- und Wasserversorgung gegenüber Cyberattacken. Dabei sind verschiedene Vorfälle möglich: Unbemerkter Datendiebstahl, Ausfall einzelner Systeme bis zur nachhaltigen Störung von Unternehmensprozessen und einem Versorgungs-Blackout.

Die Absicherung gegen diese Bedrohungssituationen umfasst die Analyse von Schwachstellen bei der Planung und dem Betrieb der Energie- und Wasserversorgung, insbesondere auch die Risikobewertung und Strategien vorbeugender Maßnahmen für Cyberangriffe. Neben den technischen Komponenten müssen auch die Führungskräfte und Mitarbeiter sensibilisiert werden, um entsprechende Sicherheitskonzepte organisatorisch zu entwickeln und umzusetzen.

www.academy.fraunhofer.de/energie-wasserversorgung

IT-Sicherheit für Energie- und Wasserversorgung

Angriffe auf Versorgungsstrukturen beurteilen und deren Ablauf nachvollziehen: Typische Schwachstellen in Unternehmen benennen, den gesetzlichen Rahmen für das eigene Unternehmen beurteilen, Maßnahmen für aktuelle Gesetze und Standards einleiten.

für Mitarbeiter aus dem Management
1 Tag Präsenz | Berlin, München oder inhouse | 600 €

Robustheit elektrischer Energienetze gegen Cyberangriffe

Bewertung der Robustheit von elektrischen Energienetzen bezüglich Gefahren von Cyberangriffen: Elektrische Energienetze modellieren und eigene Strukturen abbilden, Ausfälle simulieren und potentielle Schäden abschätzen.

für Fernwirktechniker und Netzplaner
2 Tage Präsenz | Ilmenau oder inhouse | 1.200 €

Sichere Konfiguration von Automatisierungssystemen in der Energietechnik

Automatisierungssysteme sicher konfigurieren für den Einsatz in der Energietechnik: SCADA und ICS-Systeme sicher konfigurieren, Netzwerkverkehr visualisieren, analysieren und Netzwerke absichern, bestehende Leit- und Steuerungssysteme absichern.

für Fernwirktechniker
2 Tage Präsenz | Ilmenau | 1.200 €

IT-Sicherheitsmanagement für die Energie- und Wasserversorgung

Initiierung eines IT-Sicherheitsmanagementsystems (ISMS) für Versorgungsunternehmen: Anforderung aus Standards zur Informationssicherheit, Fallstudie zur Implementierung eines ISMS, Relevante Standards und Grundlagen rechtlicher Anforderung.

für Informationssicherheitsbeauftragte, CISO
2 Tage Präsenz | Ilmenau, Görlitz oder inhouse | 1.200 €

Der IT-Sicherheitsbeauftragte in der Energie- und Wasserversorgung

Die Aufgaben des Informationssicherheitsbeauftragen in Versorgungsunternehmen: Beschreibung der Aufgabenbereiche und vorgesehenen Kompetenzen, Methoden zur Implementierung von geregelter Informationssicherheit in verschiedenen Unternehmensstrukturen.

für Informationssicherheitsbeauftragte, Manager, CISO
1 Tag Präsenz | Ilmenau, Görlitz oder inhouse | 600 €

Sichere Datenkommunikation im Energiemarkt

Datenkommunikation in den Handelsgeschäften im Energiemarkt sicher vollziehen: Überblick über die Prozesse der Energiemarktkommunikation, sichere Kommunikationswege und Nachrichtenaustausch im Energiemarkt, Identifikation von Sicherheitslücken.

für Energiedaten-Manager
1 Tag Präsenz | Ilmenau, München oder inhouse | 600 €

AUTOMOTIVE SECURITY

Das Automobil der Zukunft beinhaltet vernetzte technische Systeme und Komponenten, bei denen Sicherheitsfragestellungen von zentraler Bedeutung sind. Diese Vernetzung und Komplexität von Systemen im Fahrzeug stellen allerdings neue Angriffsmöglichkeiten auf die Sicherheit der Verkehrsteilnehmer, deren Privatsphäre oder Geschäftsmodelle der Fahrzeughersteller dar. Deshalb müssen IT-Sicherheitsaspekte in der Fahrzeugentwicklung zielgerichtet eingebunden werden.

Hierfür ist ein Verständnis für die Schutzbedarfe, Angriffswege und Abwehrmöglichkeiten im Fahrzeugumfeld erforderlich, um frühzeitig geeignete Maßnahmen ergreifen zu können. Und auch die Überprüfung und Einbindung von Software nach Sicherheitsaspekten ist im automobilen Entwicklungsprozess notwendig.

www.academy.fraunhofer.de/automotive-security

Secure Software Engineering im automobilen Entwicklungsprozess

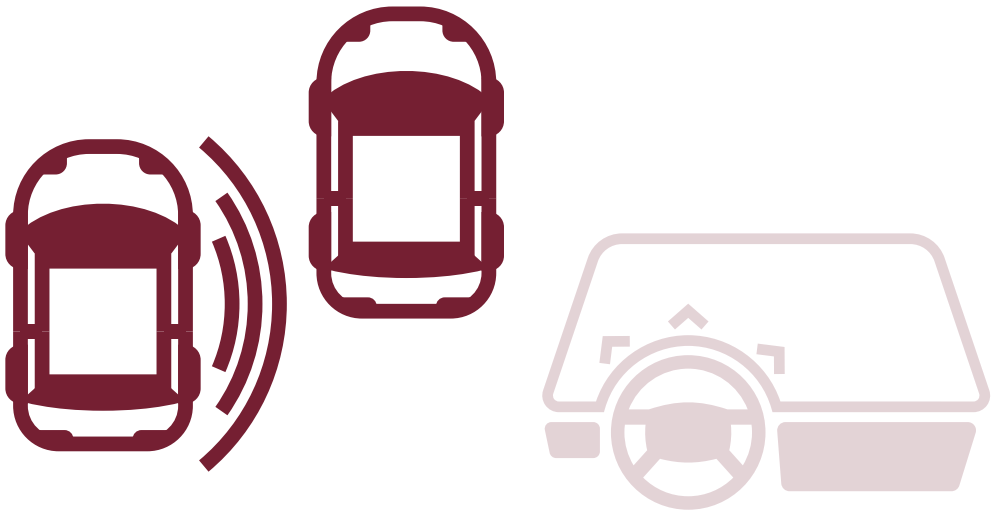
Sichere Software im gesamten Lebenszyklus systematisch entwickeln: Sicherheitsbelange in allen Stadien der Softwareentwicklung berücksichtigen, aktuelle Vorgehensmodelle und Methoden zur Softwareentwicklung anwenden, wichtige Implementierungsfehler vermeiden.

für Software-Architekten, -Ingenieure und -Entwickler
2 Tage Präsenz | 1.200 € | Garching bei München oder inhouse

IT-Sicherheit in der Fahrzeugkommunikation

Vernetzung im Fahrzeug absichern: Risiken und Lösungswege in der Fahrzeugkommunikation kennenlernen, kryptographische Verfahren verstehen, Security-Format der V2X-Kommunikation nachvollziehen, IT-Sicherheit von Bussystemen und Betriebssystemen im Fahrzeug kennen.

für Mitarbeiter im Automotive-Bereich
1 Tag Präsenz | 600 € | Garching bei München oder inhouse



PUBLIC SAFETY

IT-Systeme im öffentlichen Sektor und bei kritischen Infrastrukturen bedürfen besonderer Aufmerksamkeit hinsichtlich ihrer Sicherheit. Um einen effizienten Schutz der öffentlichen IT-Systeme zu gewährleisten, müssen zunächst der Schutzbedarf vor Bedrohungen sowie mögliche Angriffsszenarien bekannt sein.

Anhand dieser Kenntnisse können dann Strategien für die IT-Sicherheit in der Organisation entwickelt und Maßnahmen zur Sicherung der öffentlichen IT ergriffen werden. Dazu gehören auch die Gewährleistung konventioneller Informationssicherheits- und Datenschutzziele, ebenso wie Verfügbarkeit, Integrität und Vertraulichkeit hinsichtlich der IT-Systeme.

www.academy.fraunhofer.de/public-safety

Grundlagen der IT-Sicherheit für Public-Safety-Infrastrukturen

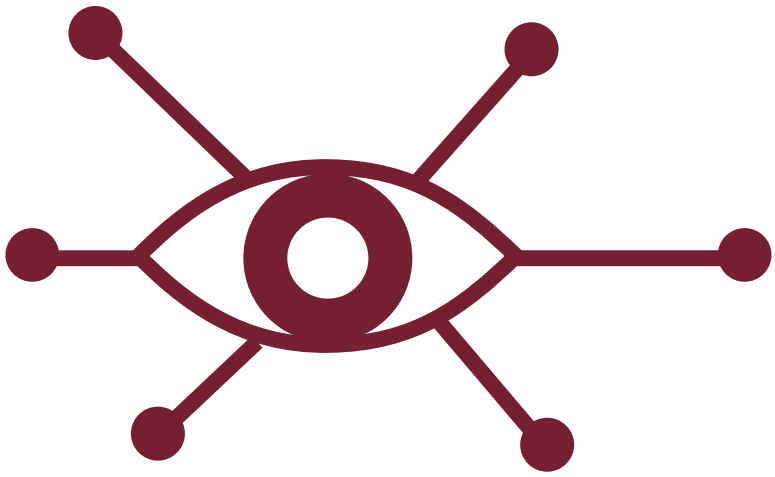
Bedrohungen für IT-Systeme öffentlicher und kritischer Infrastrukturen identifizieren: Schutzbedarf kennenlernen und Notfallplanung erstellen, Analysen zum Stand der Sicherheit durchführen, Maßnahmen nach den Anforderungen rechtlicher Grundlagen anwenden.

für Sicherheitsverantwortliche und Projektleiter IT-Systeme
2 Tage Präsenz | 1.200 € | Berlin oder inhouse

Strategische Fragen der IT-Sicherheit und ihre Auswirkungen auf Public-Safety-Lösungen

Öffentliche und kritische IT-Systeme strategisch entwickeln, betreiben und managen: Bedrohungen analysieren und kategorisieren, Auswirkungen der rechtlichen Verordnungen verstehen, Strategien für die IT-Sicherheit in der Organisation entwickeln.

für Management im Bereich KRITIS/BOS
1 Tag Präsenz | 600 € | Berlin oder inhouse



DOMÄNEN

IT-Sicherheit wird in den verschiedensten Wissensgebieten umgesetzt: Vom Entwicklungsprozess von Software über mobile Anwendungen bis hin zum sicheren Umgang mit Daten.

EMBEDDED SECURITY

IoT-SICHERHEIT

MOBILE APPLICATION SECURITY

BLOCKCHAIN

SOFTWAREENTWICKLUNG UND TESTING

PRODUKTZERTIFIZIERUNG

IT-FORENSIK

SCHADSOFTWAREANALYSE

DATENSCHUTZ

IDENTITÄT UND IDENTITÄTSNACHWEIS

EMBEDDED SECURITY

Eingebettete Systeme (Embedded Systems), Sensoren und Aktoren sind in einer Vielzahl sicherheitskritischer Szenarien im Einsatz. Etwa für den sicheren Betrieb von Produktionsanlagen oder für andere sicherheitssensible Systeme sind besondere Anforderungen relevant: eine hohe Verfügbarkeit der Komponenten, die Sicherstellung der Manipulationssicherheit, der Schutz vor unerlaubtem Informationsabfluss sowie Reaktionszeiten mit Echtzeitanforderungen.

Es ist deshalb essenziell, dass die verantwortlichen Fachkräfte ein Verständnis für die Kritikalität dieser Komponenten entwickeln. Außerdem müssen sie in der Lage sein die Qualität einzelner Komponenten sowie deren Zusammenwirken zu bewerten, erforderliche, individuell auf die Unternehmensbedürfnisse angepasste, eingebettete Software sicher zu entwickeln oder entsprechend Lastenhefte für Dienstleister zu erstellen.

www.academy.fraunhofer.de/embedded-security

IT-Sicherheitsanalysen und -tests für Embedded Systems

Cybersicherheit eingebetteter Systeme umfassend und effizient prüfen: Anhand von Praxisbeispielen für Automotive und IoT IT-Sicherheitsanalysen planen, Bedrohungsanalysen durchführen, Sicherheitskonzepte und -protokolle analysieren, Ergebnisse sinnvoll bewerten.

für Embedded-Entwickler und -Sicherheitsexperten
2 Tage Präsenz | Darmstadt oder inhouse | 1.200 €

Embedded Security Engineering

IT-Sicherheit für eingebettete Systeme entwickeln und umsetzen: Anhand von Praxisbeispielen für Automotive und IoT Bedrohungs- und Risikoanalysen durchführen, Sicherheitskonzepte und -protokolle systematisch entwickeln, Sicherheitslösungen umsetzen und bewerten.

für Embedded-Entwickler und -Sicherheitsexperten
2 Tage Präsenz | Darmstadt oder inhouse | 1.200 €

Sichere hardwaregebundene Identitäten – Von der Fertigungsschwankung zum einzigartigen Gerät

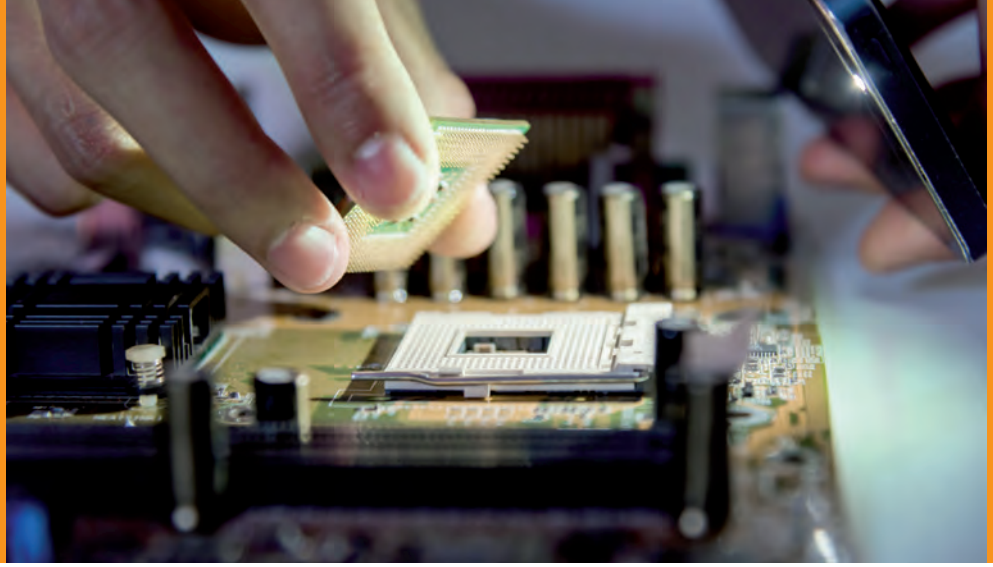
IoT-Systeme effizient schützen: Szenarien für den Einsatz von Physical Unclonable Functions (PUF) erstellen, PUF-Schaltungen verstehen, Protokolle für Lightweight-Authentifizierung nachvollziehen, Fehlerkorrekturverfahren und Angriffe auf PUFs erkennen.

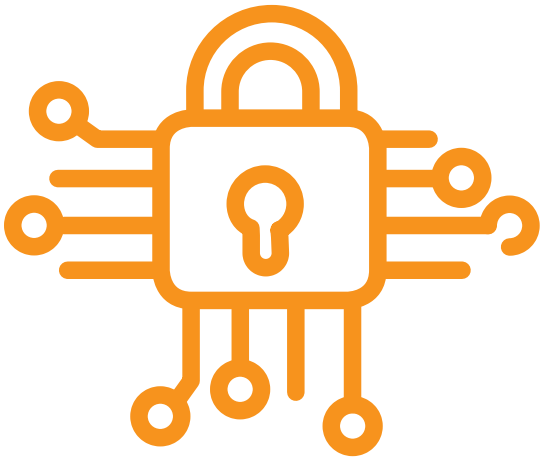
für IT-Security-Experten, Hardware-Architekten, Manager
1 Tag Präsenz | Garching bei München oder inhouse | 600 €

Sichere eingebettete Systeme mit FPGAs

Rekonfigurierbare Hardwarebausteine sicher in eingebetteten Systemen nutzen: Aktuelle Angriffsarten auf FPGAs kennenlernen, Sicherheitsmaßnahmen mit aktuellen Chips implementieren, geeignete FPGAs für das eigene System richtig auswählen und umsetzen.

für IT-Security-Experten, Hardware-Architekten, Manager
1 Tag Präsenz | München oder inhouse | 600 €





Virtualisierung für mehr Sicherheit

Eigenschaften und Möglichkeiten von Virtualisierung: Technische Details zu Systemvirtualisierung mit Fokus auf Intel- und ARM-Plattformen verstehen, alternative Isolationstechnologien wie ARM TrustZone und Intel SGX nachvollziehen und praktisch anwenden.

für Entwickler und interessierte Administratoren
2 Tage Präsenz | Garching bei München oder inhouse | 1.200 €

Advanced Linux Security

Zielgerechte und grundlegende Härtung von Linux-Systemen verstehen: Virtualisierungstechniken gezielt anwenden, Sicherheitsmechanismen des Linux-Kernels und der Hardware-Infrastruktur kennen, Angriffs- und Verteidigungstechniken nachvollziehen.

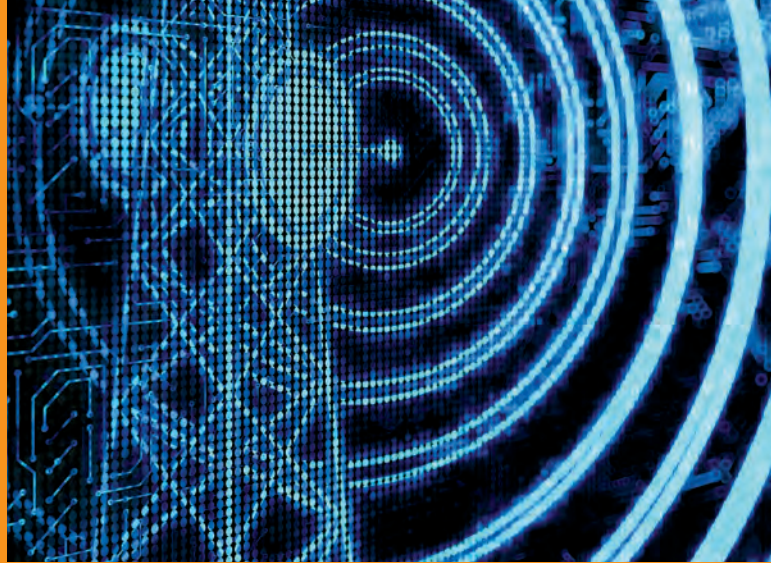
für System- und Software-Entwickler
3 Tage Präsenz | Garching bei München oder inhouse | 1.800 €

Security in Embedded Systems (Online)

Sicherheitsaspekte beim Einsatz und der Entwicklung von Embedded Systems verstehen: Mögliche Gefahren und Schwachstellen erkennen, Schutz von Hardware und Software nachvollziehen, sichere Entwicklungsprozessen für Embedded Systems richtig umsetzen.

zum Einstieg oder zur Vertiefung in eingebettete Systeme
4,5 Stunden | Online-Kurs | 250 €
in Kooperation mit University4Industry

IOT-SICHERHEIT



Internet of Things-Geräte werden immer häufiger Einfallstor und Ziele von Cyberangriffen: Sie sind allgegenwärtig, eröffnen Zugang zu vertraulichen Bereichen des Privatlebens oder schützenswerten Unternehmensbereichen – und sie besitzen eine Internet-Anbindung und sind oft unzureichend abgesichert.

Für eine funktionierende Wirtschaft und eng vernetzte Gesellschaft sind aber zuverlässige Kommunikationssysteme essenziell. Um Sicherheit von IoT-Geräten und drahtlosen Kommunikationssystemen zu gewährleisten, gilt es, potenzielle Sicherheitsrisiken und denkbare Bedrohungsszenarien kennenzulernen. Anhand dessen können Schutzziele entwickelt und Schutzmaßnahmen ergriffen werden, damit im Spannungsfeld zwischen absoluter Sicherheit und praktikabler Anwendung im Alltag effektive und sichere Lösungen umgesetzt werden.

www.academy.fraunhofer.de/iot-sicherheit

Sicherheit im Internet der Dinge

Sichere Datenübertragung und Softwareaktualisierung für IoT: Angriffsflächen und -vektoren von IoT, Elemente für sichere IoT-Kommunikation, Entwicklung sicherer IoT-Anwendungen, Sicherheitsprobleme und Anforderungen von Firmware-Updates, sicheres OTA-Update.

für IoT-Anwendungsentwickler und Sicherheitsbeauftragte
2 Tage Präsenz | Sankt Augustin oder inhouse | 1.200 €

IT-Sicherheit in drahtlosen Kommunikationssystemen

Überblick über gängige Technologien, Risiken und Schutzmaßnahmen am Beispiel von WLAN: Typische Bedrohungsszenarien und deren Risiken kennen, Gefährdungen durch drahtlose Kommunikationstechnologien einschätzen, Kommunikationstechnologien erfolgreich absichern.

für Administratoren, Tester, Betreiber oder Anwender
1,5 Tage Präsenz | Nürnberg oder inhouse | 900 €

Absicherung von IoT-Systemen

Wichtige Sicherheitslücken in IoT-Geräten auffinden und absichern: Aufbau einer IoT-Kommunikationsarchitektur kennen, Bedrohungen für IoT richtig einschätzen und abwehren, Sicherheitslücken gezielt aufspüren und beseitigen.

für Software-Architekten und -Entwickler
1 Tag Präsenz | Garching oder inhouse | 600 €

Netzwerksicherheit: Radius, NAC, VPN

Sichere Netzwerkinfrastruktur zur Nutzung von NAC (Network Access Control), Radius und VPN (Virtual Private Network) bereitstellen: Geräte im Netzwerk erkennen und deren Zugriff verwalten, Konfigurationsfehler vermeiden und Risiken richtig einschätzen.

für Administratoren und Betreiber im Open Source-Umfeld
1 Tag Präsenz | Aalen oder inhouse | 600 €

MOBILE APPLICATION SECURITY

Mobile Endgeräte sind im beruflichen und privaten Umfeld kaum noch wegzudenken. Diese vielfältigen Einsatzmöglichkeiten bedeuten aber auch eine Vielzahl an neuen Angriffsmöglichkeiten. Und weil die Geräte auch immer mehr in kritischen Umgebungen eingesetzt werden, muss sich das IT-Sicherheitswissen nicht nur auf Entwicklung und Administration, sondern auch sicheren Einsatz derartiger Geräte, z.B. beim Auslesen von Maschinendaten, erstrecken.

Um die Angriffsmöglichkeiten einzuschränken, müssen je nach Gefährdung die richtigen Sicherheitslösungen ausgewählt und korrekt eingesetzt werden. Auch bei der Entwicklung von Apps, die häufig für kritische Aufgaben wie geschäftliche Emails eingesetzt werden, ist es wichtig, die Gefahren und Risikopotenziale richtig einzuschätzen.

www.academy.fraunhofer.de/mobile-security

Mobile Application Security

Sicherheit von Apps und Plattformen in Android und iOS analysieren: Sicherheitsmodell von Android und iOS kennenlernen, typische Angriffe und aktuelle Gefahren nachvollziehen, Verfahren und Tools zur Hands-on-Sicherheitsanalyse von Apps praktisch anwenden.

für Entwickler, Tester und Entscheider von Apps
2 Tage Präsenz | Garching bei München oder inhouse | 1.200 €

Mobile Endgeräte: Android

Sicheren Umgang mit Android im Unternehmen umsetzen: Typische Schwachstellen und Angriffsmöglichkeiten von Android kennenlernen, Sicherheitsmechanismen und -konzept von Android verstehen, Mobile-Device-Management-Lösungen richtig administrieren.

für Administratoren und Entwickler für Android
1 Tag Präsenz | Aalen oder inhouse | 600 €

Sicherheit von mobilen Endgeräten: iOS

Unternehmensnetzwerke mit iOS-Geräten durch Mobile Device Management absichern: Sicherheitskonzepte zur Verwaltung von iOS-Endgeräten erstellen und verbleibende Restrisiken abschätzen, geeignete MDM-Lösungen auswählen und mit Fokus auf iOS konfigurieren.

für Administratoren, IT-Dienstleister und IT-Verantwortliche
1 Tag Präsenz | Aalen oder inhouse | 600 €

BLOCKCHAIN

Ausgelöst durch die revolutionären technischen Ideen von Bitcoin gab es nach der Veröffentlichung dieser Kryptowährung einen Boom in der Blockchain-Entwicklung. In der Menge an neuen Start-ups, Forschungen und Schlagzeilen ist es schwer, sich einen Überblick über den tatsächlichen Fortschritt und die Sicherheit im Bereich Blockchain zu verschaffen.

Und gerade die (vermeintliche) Sicherheit bei der Blockchain-Lösung darf nicht vernachlässigt werden, da auch diese Technologien – unter bestimmten Umständen – angreifbar und manipulierbar sind. Eine Reihe von Hackerattacken auf Blockchain-Anwendungen und -Dienste hat bereits gezeigt, dass diese Technologien ein ausnehmend attraktives Ziel für Angreifer darstellen. Deshalb ist es notwendig abzuwägen, welche Anwendungsfelder und Potenziale es für Blockchain gibt, wann der Einsatz im Unternehmen lohnenswert ist, und welche Skills dafür nötig sind.

www.academy.fraunhofer.de/blockchain

Blockchain

Funktionsweise von Blockchain verstehen und nutzen: Einsatzmöglichkeiten der existierenden Blockchain-Implementierungen und -Konzepte einschätzen, sicherheitsrelevante Aspekte kennenlernen, selbst erste Erfahrungen im Programmieren von Smart Contracts sammeln.

für Administratoren, Entwickler, Tester oder Betreiber
3 Tage Präsenz | Weiden i. d. Oberpfalz, Garching bei München oder inhouse | 1.800 €

Blockchain: Das Wichtigste in Kürze (Online)

Die Blockchain knapp und informativ: Grundlagen und Eigenschaften der Blockchain kennenlernen, Anwendungsfelder und Beispiele der Technologie nachvollziehen, mit Use Cases Potenziale erschließen.

zum Einstieg oder zur Vertiefung in das Thema Blockchain
ca. 1,5 Stunden | Online-Kurs | 120 €
in Kooperation mit University4Industry

Potenziale der Blockchain-Technologie identifizieren (Online)

Anwendungsmöglichkeiten und Risiken der Blockchain: Die Technologie der Blockchain verstehen, zukünftige Anwendungen und neue Geschäftsmodelle kennenlernen, Potenziale der Blockchain richtig erschließen.

zum Einstieg oder zur Vertiefung in das Thema Blockchain
ca. 2 Stunden | Online-Kurs | 150 €
in Kooperation mit University4Industry

Technische Grundlagen und Sicherheitsaspekte der Blockchain (Online)

Technische Grundlagen und Sicherheitsaspekte der Blockchain: Funktionsweisen und Kryptografie verstehen, technische Herausforderungen und Weiterentwicklungen kennenlernen, Manipulationssicherheit und Angriffe nachvollziehen.

zum Einstieg oder zur Vertiefung in das Thema Blockchain
3 Stunden | Online-Kurs | 350 €
in Kooperation mit University4Industry

Wie kann ich die Blockchain-Technologie anwenden? (Online)

Technische Grundlagen und Anwendungsfelder von Transaktionen mit Blockchain verstehen, Validierungen und kryptografische Verfahren nachvollziehen, Beispiele von Industrieanwendungen erfahren.

zum Einstieg oder zur Vertiefung in das Thema Blockchain
ca. 4,5 Stunden | Online-Kurs | 340 €
in Kooperation mit University4Industry

Die Blockchain: Potenziale, technische Grundlagen, Anwendungen und Sicherheitsaspekte (Online)

Blockchain aus unterschiedlichsten Perspektiven kennenlernen: Technische Funktionsweisen und Sicherheitsaspekte der Blockchain erforschen, Potenziale erfahren und mit Use Cases Anwendungsmöglichkeiten richtig erschließen.

zum Einstieg oder zur Vertiefung in das Thema Blockchain
7 Stunden | Online-Kurs | 550 €
in Kooperation mit University4Industry

SOFTWAREENTWICKLUNG UND TESTING

Gegenüber funktionalen Anforderungen werden Sicherheitsanforderungen oft vernachlässigt. Dabei fehlt eine systematische Herangehensweise, um auch Sicherheit effektiv und effizient zu implementieren. Sicherheit beginnt schon mit den ersten Entwicklungsschritten: Mit Security by Design wird die Sicherheit von Software, Systemen und Produkten schon zu einem integralen Aspekt zu Beginn der Entwicklung – nicht zu einem nachgelagerten Schritt.

Dazu gehören auch regelmäßige Sicherheitstests von Software und Systemen. Denn fast alle Software-Sicherheitsvorfälle werden durch Angreifer verursacht, die bekannte Sicherheitslücken ausnutzen – und sind somit vermeidbar. Die Einführung eines Sicherheitstestprozesses, strukturierter Risikoanalysen, Penetrationstests und Hacking erlauben es, sicherheitsrelevante Schwachstellen aufzudecken und zu bewerten.

www.academy.fraunhofer.de/softwareentwicklung-testing

Sichere Softwareplanung: Softwareentwicklung von Beginn an sicher

Aus der Bedrohungsanalyse Sicherheitsanforderungen für die Software ableiten: Schutzbedarf und Sicherheitsanforderungen ermitteln, Angreifer klassifizieren, Sicherheit der modellierten Software beurteilen, valide Sicherheitsmetriken entwickeln und einschätzen.

für Software-Architekten, Entwicklungs- und Projektleiter
2 Tage Präsenz | Brandenburg an der Havel oder inhouse | 1.200 €

Software-Härtung: Software gegen Schwachstellen sichern

Software-Härtung an den gefährdeten Stellen einfügen: Schwachstellen in einer bestehenden Software-Architektur bestimmen, geeignete Sicherheitsmaßnahmen auswählen, Sicherheitsanforderungen im Code integrieren, Secure Design Pattern anwenden.

für Software-Entwickler
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

Hacking: Pentesting

IT-Sicherheit aus der Perspektive des Angreifers prüfen: Perspektive eines Hackers einnehmen, Penetrationstest professionell durchführen, sicherheitsrelevante Schwachstellen von Software aufdecken und analysieren, Risiken abwägen und richtig einschätzen.

für Netzwerkadministratoren, Sicherheitsbeauftragte, Softwareentwickler
3 Tage Präsenz | Weiden i.d. Oberpfalz oder inhouse | 1.800 €

Hacking: Binary Exploitation

Vorgehensweise von Hackern verstehen und ihnen zuvorkommen: Typische Programmierfehler in C-Code identifizieren, Grenzen der Schutzmechanismen verstehen und damit richtig umgehen, Exploits praktisch üben und zum Aufzeigen der Schwachstelle selbst entwickeln.

für Programmierer, Entwickler, Tester, Betreiber
3 Tage Präsenz | Garching bei München oder inhouse | 1.800 €

Security Tester – Basic

Systematische Einführung in die Grundlagen des Sicherheitstestens: Auswahlkriterien für Sicherheitstesttechniken beurteilen, Rolle des Testens im Entwicklungszyklus verstehen, risikobasiertes Sicherheitstesten und spezielle Testtechniken anwenden.

für Produktmanager und -entwickler, Testentwickler, Abnahmetester, Qualitätsmanager
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

Maschinelles Lernen für mehr Sicherheit

Maschinelles Lernen und Data Mining für die Modellierung von Anomalieerkennungen in der IT-Sicherheit nutzen: Grundlagen des maschinellen Lernens und des Data Mining kennen, Grundlagen der Modellierungsmethoden zur Anomalieerkennung vertiefen.

für Sicherheitsingenieure, IT-Analysten, System-/Software-Entwickler
1 Tag Präsenz | Garching bei München | 600 €

Security Tester – Advanced

Schwachstellen in Software systematisch aufdecken und bewerten: Fortgeschrittene Techniken und Methoden des Sicherheitstestens anwenden, komplexe Sicherheitsmechanismen testen, risikobasierte Sicherheitstestprozesse systematisch bewerten und verbessern.

für Produktmanager und -entwickler, Testentwickler, Abnahmetester, Qualitätsmanager
3 Tage Präsenz | Berlin oder inhouse | 1.800 €

PRODUKT-ZERTIFIZIERUNG

Zertifizierungen können das Vertrauen potenzieller Kunden in die Sicherheit von IT-Produkten steigern und den Zugang zu regulierten Märkten eröffnen. Denn durch eine Sicherheitszertifizierung wird unabhängig bestätigt, dass diese Produkte über angemessene Sicherheitseigenschaften verfügen.

Dafür gilt es zunächst, die geeignete Sicherheitszertifizierung für das eigene Produkt auszuwählen und den Aufwand, den Nutzen und die Risiken bis hin zu einer erfolgreichen Zertifizierung richtig abzuschätzen.

www.academy.fraunhofer.de/produktzertifzierung

Vertrauen durch Produktzertifizierung

Zertifizierungen im IT-Sektor richtig bewerten und umsetzen: Vorteile sowie Risiken und Aufwand einer Zertifizierung für das eigene Produkt abschätzen, Common-Criteria-Zertifizierungen verstehen, Zertifizierungsprozesse mit Ressourcenaufwand planen können.

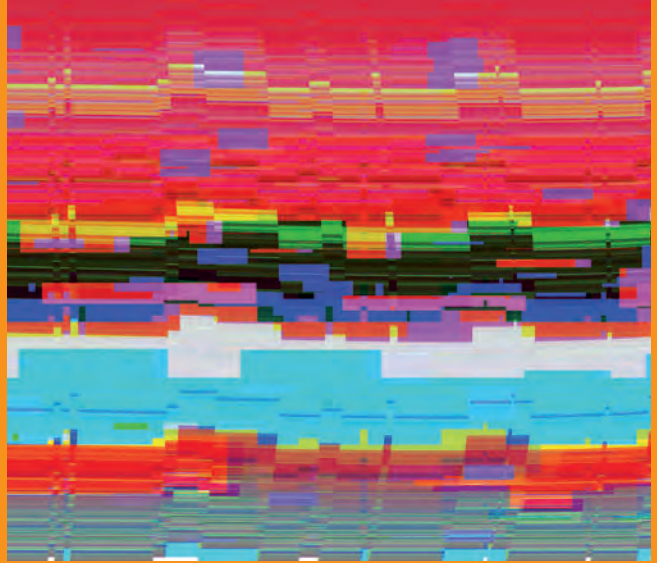
für Entscheider und Produktmanager
1 Tag Präsenz | Berlin oder inhouse | 600 €

Sicherheitszertifizierung von Produkten

Eine Common-Criteria-Zertifizierung als das Mittel der Wahl einschätzen: Überblick über das deutsche Zertifizierungsschema bekommen, zentrale Konzepte des CC-Standards und den Ablauf einer Zertifizierung verstehen, Anwendbarkeit auf das eigene Produktportfolio bewerten.

für Produktmanager/-entwickler und technische Einkäufer
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

IT-FORENSIK



Da viele Sicherheitsschwachstellen in Unternehmen und Behörden ausgenutzt werden für Angriffe, Spionage und Manipulation, besteht ein erheblicher Bedarf zur Aufklärung solcher Vorfälle. In den Seminaren zum Themenfeld IT-Forensik werden Vorgehensweisen und Werkzeugen zur sicheren Identifikation und beweissicheren Extraktion von Spuren behandelt, wobei durch das IT-forensische Vorgehen keine Spuren verändert werden dürfen.

Das Spektrum IT-forensischer Werkzeuge ist dabei sehr groß. Es reicht von der effizienten Identifikation bestimmter Inhalte in riesigen Festplattenspeichern oder Online-Speicherdiensten über die Live-Forensik bis hin zur IT-forensischen Analyse von Mobilgeräten wie etwa Smartphones oder auch die trickreiche Umgehung von Sicherungsmechanismen, mittels derer Angreifer versuchen ihre Beute oder Aktivitäten gegen Aufklärung zu schützen.

www.academy.fraunhofer.de/it-forensik

Multimedia-Forensik für Ermittlungsverfahren

Spuren in digitalen Bildern, Video- und Audiodaten forensisch auswerten: Grundlagen von Multimedia-Datenformate verstehen, Verfahren zur Rekonstruktion gelöschter oder fragmentierter Mediendaten anwenden, verdächtige Dateien auf versteckte Botschaften untersuchen.

für IT-Forensiker in Unternehmen und Behörden
2 Tage Präsenz | Darmstadt oder inhouse | 1.200 €

Textanalyse mit NLP und maschinellem Lernen

Textdaten forensisch auf relevante Inhalte »zwischen den Zeilen« untersuchen: Textdateien maschinenlesbar bereinigen und strukturieren, automatisierte Verfahren des maschinellen Lernens anwenden, Problemstellungen zur Verarbeitung von Textdaten selbstständig lösen.

für Ermittler, Prüfer, Versicherer
3 Tage Präsenz | Darmstadt oder inhouse | 1.800 €

IT-Forensik für die Erkennung von Bild-Manipulationen

Gefälschte Bilder und Videos erkennen: Wichtigste Dateiformate und spezielle Multimediaforensik-Verfahren kennenlernen und praxisnah üben, Echtheitsprüfungen von digitalen Bild- und Videodaten durchführen, Echtheit multimedialer Beweisstücke richtig beurteilen.

für IT-Forensiker, Schadensregulierer, Ermittler
1 Tag Präsenz | Darmstadt oder inhouse | 600 €

Grundlagen der Datenträger-Forensik

Möglichkeiten der IT-Forensik verstehen und anwenden: IT-forensische Methoden kennen und zur Prüfung von Sicherheitsvorfällen auswählen, IT-forensische Untersuchung planen, Analysen von Datenträgern auf relevante Informationen durchführen und richtig dokumentieren.

für Prüfende von IT-Sicherheitsvorfällen
1 Tag Präsenz | Darmstadt oder inhouse | 600 €

IT-FORENSIK

Open Source Intelligence – Digitale Informationsgewinnung

Informationen im Rahmen digitaler Investigationen gewinnen: Prozessketten des Informations-Gathering verstehen, Kali-Linux und Open-Source-Werkzeuge einsetzen, fallspezifische Untersuchungen (Maltego, Recon-ng, Tor-Browser) erfolgreich durchführen.

für Personen aus journalistischen, juristischen und medialen Bereichen
2 Tage Präsenz | Mittweida oder inhouse | 1.200 €

Open Source Intelligence für Behörden

Informationsgewinnung für Behörden und kriminalistische Institutionen: Prozessketten des Informations-Gathering verstehen, Kali-Linux und Open-Source-Werkzeuge einsetzen, fallspezifische Untersuchungen (Maltego, Recon-ng, Tor-Browser) erfolgreich durchführen

für Mitarbeiter kriminologischer Institutionen und Behörden
2 Tage Präsenz | Mittweida oder inhouse | 1.200 €

Der Datenanalyst 1 – Datenvorverarbeitung und Visualisierung

Mit Open-Source-Werkzeugen Daten analysieren und visualisieren: Daten verschiedener Formate importieren und bereinigen, Kennzahlen der deskriptiven Statistik ermitteln, unterschiedliche Datentabellen miteinander verbinden, Visualisierungen von Daten erstellen.

für Anwender und Fachkräfte der Datenauswertung
3 Tage Präsenz | Mittweida oder inhouse | 1.800 €

Vielen Dank für Ihre Daten – Cybercrime vs. offenes Unternehmen

Wirksamer Schutz vor Social Engineering: Vorgehensweisen von Human Hacking in Unternehmen verstehen, digitale Investigationen mithilfe von Open-Source-Werkzeugen durchführen, Schwachstellen finden und beseitigen sowie souverän in IT-Krisensituationen reagieren.

für Management und Anwender aus dem Office-Bereich
1 Tag Präsenz | Leipzig, München, Berlin oder inhouse | 690 €
in Kooperation mit PAN-Seminare

Einführung in die Datenträger- und Netzwerkforensik

Methoden und Werkzeuge zur Datenträger- und Netzwerkverkehrsanalyse richtig anwenden: Datenträger und Dateisysteme analysieren, digitale Spuren extrahieren, einfache Aufgaben der Datenträger- und Netzwerkforensik automatisieren, gelöschte Dateien wiederherstellen.

für Incident-Responder, Security-Analysten, IT-Forensiker
2 Tage Präsenz | Bonn oder inhouse | 1.200 €

Ermittlungen im Darknet

Tor, Hidden Services, Blockchain, Bitcoin besser verstehen: Selbstsicher und unauffällig im Darknet surfen, Kommunikationsverläufe im Darknet einschätzen, Kryptowährungen unterscheiden können, Chancen und Risiken der Anonymität im Darknet besser beurteilen.

für Ermittler, Strafverfolger, Fachjournalisten
1 Tag Präsenz | Darmstadt oder inhouse | 600 €

Car Forensik

Digitale forensische Auswertung vernetzter IT-Systeme im Kfz: Steuergeräte über den CAN-Bus und Transponderschlüssel auslesen, Daten in Fahrzeugen für die eigene forensische Arbeit nutzen, verschiedenen Modi Operandi bei Kfz-Diebstählen nachvollziehen.

für Strafverfolgungsbehörden, Justiz, Versicherungsgutachter
2,5 Tage Präsenz | Mittweida oder inhouse | 1.500 €

SCHADSOFTWAREANALYSE

Im Zuge der Digitalisierung ist auch die Schadsoftware heutzutage allgegenwärtig geworden. Insbesondere das Internet der Dinge vergrößert die Angriffsfläche für Schädlinge exponentiell: Neben Computern und Smartphones sind auch Fernseher, Glühbirnen, Autos und Medizintechnik zu möglichen Zielen von Cyberangriffen durch Schadsoftware geworden.

Mit dem Bewusstsein für diese Art der Schwachstellen und dem Erkennen von Angriffsmustern ist es möglich, Schaden frühzeitig abzuwenden. Nur zu wissen, dass sich ein Programm möglicherweise bösartig verhält oder nicht, reicht nicht aus. Um Vorfälle umfassender zu bewerten und Schadenspotenziale abwägen zu können, ist eine aufwendige, detaillierte Analyse der Schadsoftware nötig.

www.academy.fraunhofer.de/schadsoftwareanalyse

Netzwerkgrundlagen für Analysten

Network Basics in a Nutshell: Schichten des OSI-Modells und ihre jeweilige Funktion kennenlernen, komplexe Zusammenhänge zwischen den einzelnen Bausteinen im Netzwerk erkennen, aufgezeichneten Netzwerkverkehr analysieren und deuten, Gegenmaßnahmen ergreifen.

für angehende Netzwerkadministratoren, Incident-Responder oder Analysten
4 Tage Präsenz | Bonn oder inhouse | 2.400 €

Grundlagen der Python-Programmierung für Analysten

Mit Python bestehende IT-Sicherheits-Software automatisieren und erweitern: Grundlagen von Python verstehen, selbstständig Programme zur Lösung alltäglicher Probleme entwickeln, auf wichtige Komponenten für Analysten aus dem Python-Universum zurückgreifen können.

für angehende Entwickler und IT-Sicherheitsanalysten
2 Tage Präsenz | Bonn oder inhouse | 1.200 €

Einführung Windows für Analysten

Windows-Architektur und die zugrundeliegenden Konzepte erfassen: Schichtenmodel der Windows-Architektur nachvollziehen, Komplexität und beteiligte Komponenten bei Vorhaben des Betriebssystems richtig abschätzen, Systemspezifika für Softwareanalyse nutzen.

für angehende Softwareanalysten
1 Tag Präsenz | Bonn oder inhouse | 600 €

Einführung in die Firmwareanalyse

Aufbau von Firmware und Betriebssystemen in eingebetteten Systemen sowie Angriffsvektoren auf diese Systeme kennen, Firmware durch Soft- oder Hardware aus Systemen extrahieren und entpacken, Firmware statisch und dynamisch auf Schwachstellen analysieren.

für IT-Sicherheitsfachkräfte und Analysten
2 Tage Präsenz | Bonn oder inhouse | 1.200 €

Einführung Schadsoftware

Bedrohungen von Schadsoftware richtig einschätzen: Aktuelle Fallbeispiele großer Sicherheitsvorfälle kennenlernen, Merkmale und Angriffsvektoren von Schadsoftware verstehen und einordnen können, Schwachstellen und Angriffe erfolgreich erkennen.

für angehende Analysten
1 Tag Präsenz | Bonn oder inhouse | 600 €

Grundlagen Schadsoftwareanalyse Windows – Malware untersuchen und verstehen lernen

Malware mit Analysetechniken untersuchen: Angriffsvektoren und Verbreitungswege von Software verstehen, Systemaufrufe und Netzwerkprogrammierung in Assembler analysieren, Methoden zur statischen und dynamischen Analyse von Windows-Schadsoftware anwenden.

für IT-Administratoren, Analysten und CERTs
3 Tage Präsenz | Bonn oder inhouse | 1.800 €

Fortgeschrittene Schadsoftwareanalyse Windows

Schadsoftware entschleiern und analysieren: Gängige Verschleierungsmethoden wie Code-Injektionen, String-Verschlüsselung und API-Verschleierung erkennen, Verschleierungsmethoden selbst programmatisch auflösen, IDA Pro automatisieren, Code-Injektionen verfolgen.

für Schadsoftwareanalysten mit ersten Erfahrungen
2 Tage Präsenz | Bonn oder inhouse | 1.200 €

DATENSCHUTZ

Auch nach dem 25.05.2018 ist Datenschutz immer noch ein drängendes Thema: Die Schutzziele aus der EU-Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz müssen richtig in den Organisationen umgesetzt und bei neuen Entwicklungen berücksichtig werden. Gerade in spezifizierten Bereichen, in denen Daten verarbeitet werden, wie der IT-Forensik oder der Energiebranche, drängen sich ganz neue Fragestellungen zum Datenschutz auf.

Deshalb müssen Mitarbeiter befähigt werden, ihre Arbeit in Bezug auf Datenschutzkonformität zu bewerten und die richtigen Maßnahmen zur Umsetzung des Datenschutzes zu ergreifen.

www.academy.fraunhofer.de/datenschutz

Zertifizierte/r EU-Datenschutz Spezialist/in (DSGVO/GDPR)

Praktische Anleitung für die Umsetzung des Bundesdatenschutzgesetzes und der EU-Datenschutzgrundverordnung: Relevanz des Datenschutzes nachvollziehen, aktuelle Rechtsbegriffe verstehen, Realisierung der Vorschriften planen und durchführen.

für Datenschutzbeauftragte, Projektleiter, Product Owner
1 Tag Präsenz | Berlin | 499 € + 119 €
mit Zertifizierung durch International Software Quality Institute (iSQI)

Zertifizierte/r EU-Datenschutz Spezialist/in (DSGVO/GDPR) (Online)

Anleitung für die praktische Umsetzung der EU-Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes: Aktuelle Rechtsbegriffe besser verstehen, Anwendung der rechtlichen Richtlinien planen und durchführen, technische Konzepte und Lösungsansätze kennenlernen.

für Mitarbeiter im Umgang mit Daten
ca. 6 Stunden | Online-Kurs | 420 €
aufbauend dazu weitere Online-Vertiefungskurse
– für Personaler
– für Mitarbeiter in Marketing und Sales

Datenschutz für Energiedaten-Manager

Einhaltung von Datenschutzanforderungen im Energiedatenmanagement: Überblick über benötigte Daten in Prozessen am Energiemarkt, rechtlich korrekt mit Kunden- und Stammdaten umgehen, Anforderungen der Datenschutzgrundverordnung korrekt in Prozessen umsetzen.

für Energiedaten-Manager
1 Tag Präsenz | in Ilmenau, Görlitz, München oder inhouse | 600 €

Datenschutz für IT-Forensiker

Effektiv und datenschutzkonform ermitteln: Grundprinzipien der Datenverarbeitung nach Datenschutzgrundverordnung und Bundesdatenschutzgesetz verstehen, datenschutzkonformes Arbeit in der IT-Forensik richtig bewerben und mögliche Maßnahmen ergreifen.

für IT-Forensiker in Unternehmen und Behörden
0,5 Tage Präsenz | Darmstadt oder inhouse | 300 €

IDENTITÄT UND IDENTITÄTSNACHWEIS

Im Zuge der Digitalisierung ergeben sich für das Identitätsmanagement vielfältige Herausforderungen, aber auch neue Lösungen: Mit biometrischen Verfahren können Authentifizierungen von Personen umgesetzt werden, firmenübergreifende Systemzugriffe werden mit digitalem Identitätsmanagement sicher gestaltet, ein vertrauenswürdiges Identitätsmanagement kann mit dem Know-how zu rechtlich-organisatorischen Rahmenbedingungen und den fachlichen-technischen Anforderungen aufgebaut werden.

www.academy.fraunhofer.de/identitaeten

Digitale Identitäten

Systemzugriffe im Unternehmenskontext absichern: Identitätsmanagement anhand relevanter Protokolle anwenden, Authentifizierung mit offenen und lizenzfreien Standards der FIDO-Allianz durchführen, Entscheidungen zum Identitätsmanagement treffen können.

für Webentwickler, Betreiber und Anwender
2 Tage Präsenz | Garching bei München oder inhouse | 1.200 €

Biometrische Sicherheit I

Biometrie ermöglicht alternative Methoden zur Authentifizierung und Autorisierung: biometrische Verfahren verstehen, Vor- und Nachteile biometrischer Verfahren nachvollziehen, Sicherheit eines biometrischen Systems einschätzen und geeignete Lösungen entwerfen.

für Systementwickler und Sicherheitsbeauftragte
2 Tage Präsenz | Sankt Augustin oder inhouse | 1.200 €

Vertrauenswürdiges Informationsmanagement in Behörden und Unternehmen

Rechtlich-organisatorische Rahmenbedingungen und fachlich-technische Anforderungen an ein sicheres Informationsmanagement verstehen: Eigene Bedarfe analysieren, Projekte und Lösungen planen und durchführen, Produkte grundsätzlich bewerten und einschätzen.

für Mitarbeiter in Information Governance und E-Akte
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

Digitale Geschäftsprozesse – sicher, effizient, vertrauenswürdig

Nutzung elektronischer Vertrauensdienste und digitaler Identitäten für ein sicheres E-Government: Anforderungen und Lösungsbeispiele verstehen und einordnen, nachhaltige Digitalisierungsstrategie aufbauen, E-Government in Unternehmen gezielt weiterentwickeln.

für Manager in E-Government/E-Business und IT
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

Vertrauenswürdige digitale Transaktionen durch eIDAS

Sichere digitale Identitäten und elektronische Vertrauensdienste: Strategie zur Umsetzung sicherer digitaler Transaktionen auf Basis von eIDAS definieren, Anforderungen in der Organisation richtig analysieren und dokumentieren, mögliche Geschäftsmodelle bewerten.

für Mitarbeiter in IT-Strategie, E-Business, PKI, E-Akte, ECM
2 Tage Präsenz | Berlin oder inhouse | 1.200 €

BASICS DER IT-SICHERHEIT

Der Schutz von Unternehmen vor Cyberangriffen beginnt nicht bei den technischen Lösungen, sondern bei den Menschen: Oft fehlt es an der notwendigen Sensibilität aller Mitarbeiter in Bezug auf IT-Sicherheit, einer funktionierenden IT-Sicherheitsorganisation oder dem Wissen über aktuellen IT-Sicherheitsanforderungen.

Schulungen zur Strategie und Organisation von IT-Sicherheit, Bewusstseins- und Handlungstraining zum Krisenmanagement sowie Kompetenznachweise zu allen wichtigen Gebieten der Informationssicherheit helfen dabei, das IT-Sicherheitsniveau im Unternehmen zu steigern.

www.academy.fraunhofer.de/basics-it-sicherheit

IT-Sicherheitsorganisation im Unternehmen

IT-Sicherheitsorganisation aufbauen: Bedrohungen für Unternehmensdaten einschätzen, Mitarbeiter-Awareness fördern, IT-Sicherheitsmaßnahmen treffen, Aufbau eines IT-Sicherheitsmanagements, rechtliche Rahmenbedingungen umsetzen.

für Manager aus dem Nicht-IT-Bereich
1 Tag Präsenz | Aalen oder inhouse | 600 €

Grundlagen der IT-Sicherheit für Fachkräfte

IT-Sicherheitsmechanismen verstehen und anwenden: Die wichtigsten IT-Sicherheitskonzepte aus Sicht eines Systementwicklers nachvollziehen und in Übungen erproben, potenzielle Sicherheitsrisiken identifizieren, Sicherheitsanforderungen analysieren und festlegen.

für Anwendungsentwickler und Sicherheitsbeauftragte
3 Tage Präsenz | Sankt Augustin oder inhouse | 1.800 €

IT-Sicherheitsstrategie im Unternehmen

Ganzheitliche IT-Sicherheitsstrategie etablieren: Die wichtigsten Sicherheitsfragen der digitalen Transformation verstehen, Schwachstellen identifizieren, prozessorientierte Maßnahmen ermöglichen, Mitarbeiter sensibilisieren und Angriffe aktiv verhindern.

für Geschäftsführer und Mitarbeiter des Managements
1 Tag Präsenz | Bonn oder inhouse | 600 €

IT-Sicherheit für KMU

Angriffe auf verschiedene Unternehmensstrukturen von kleineren und mittleren Unternehmen nachvollziehen, typische Schwachstellen in Unternehmen benennen, den gesetzlichen Rahmen für das eigene Unternehmen beurteilen, Maßnahmen für aktuelle Gesetze und Standards einleiten.

für Manager
1 Tag Präsenz | in München, Görlitz oder inhouse | 600 €

Cybercrime Management

Bewusstseins- und Handlungstraining für strukturiertes Krisenmanagement in Organisationen: Entscheidungsmodelle selbst in einer Krisensimulation erproben, in Krisenfällen souverän reagieren und kommunizieren, Bewusstsein für Gefahren von Cyberangriffen schärfen.

für Management, Anwender und Fachkräfte
1 Tag Präsenz | Mittweida oder inhouse | 600 €

Schutz vor Social Engineering

Social-Engineering-Angriffe und Datendiebstahl von Personen sowie ganzen Unternehmen verhindern: Gefahren des Human Hackings kennen, mit sensiblen Informationen sicher umgehen, Methoden von Human-Hacking-Attacken verstehen, passende Schutzmaßnahmen ergreifen.

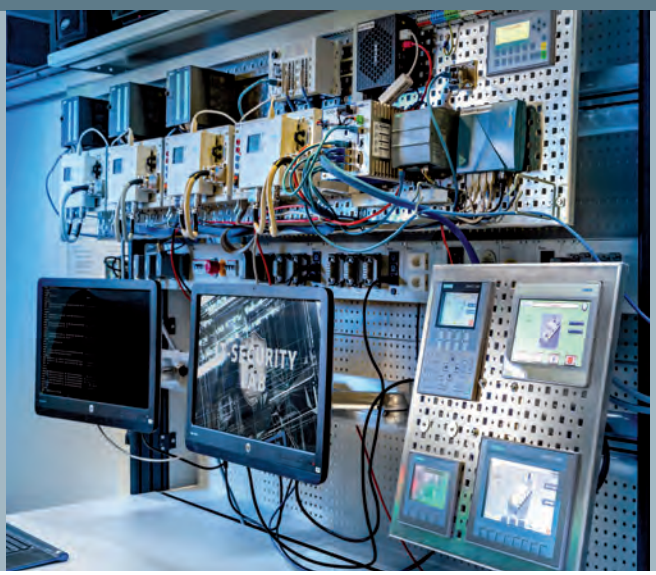
für öffentlich wirksame Personen, Führungskräfte, Selbstständige
1 Tag Präsenz | Mittweida oder inhouse | 600 €

Zertifikat zum TeleTrusT Information Security Professional (T.I.S.P.)

Expertenzertifikat zur Informationssicherheit nach höchsten Qualitätsstandards: Kenntnisse der Informationssicherheit vertiefen mit Grundlagen zur Netzwerksicherheit, Kryptografie, Sicherheitsmanagement, rechtliche Grundlagen und Systemsicherheit.

für Information Security Officers und IT-Auditoren
5 Tage Präsenz | Darmstadt | 2.940 € + 360 €
mit Zertifizierung durch TÜV Rheinland

HANDS-ON SCHULUNGEN IN LABOREN UND ONLINE



»Besonders habe ich die technische Umgebung im Seminar geschätzt, die Ausstattung und die Räumlichkeiten waren optimal. Man bekommt einen breiten Blick auf unterschiedliche Branchen und deren Problemstellungen sowie Impulse zur Umsetzung im eigenen Unternehmen. Zusammengefasst: hochprofessionell.«
Tatjana Fell, Pilz GmbH & Co. KG

Im IT-Security Lab des Fraunhofer IOSB in Karlsruhe werden Sicherheitsangriffe auf Industrie-Anlagen simuliert.

Der Name »Lernlabor« ist Programm: Durch eine hochwertige technische Infrastruktur und anhand konkreter Anwendungsfälle machen wir in unseren Seminaren das Know-how erfahrbar. Und unsere Experten vermitteln die Inhalte zu IT-Sicherheit so, dass der Wissenstransfer im eigenen Unternehmen auch einfach funktioniert. Dafür setzen wir einen idealen Mix aus anwendungsorientierten Praxisphasen im Lernlabor und online verfügbaren Lernangeboten ein.

Im eigenen Tempo auf die Laborphase vorbereiten

Basisinhalte der IT-Sicherheit können sich die Teilnehmenden im Vorfeld der Präsenzphase zeit- und ortsunabhängig in ihrem eigenen Lerntempo selbstgesteuert aneignen. Dafür werden professionell produzierte Inhalte eingesetzt. In kurzen Videos kommen die Wissenschaftlerinnen und Wissenschaftler der Fraunhofer-Institute und Partnerhochschulen zu Wort und erklären Zusammenhänge und Anwendungsbeispiele. Zusätzlich werden Angriffs- und entsprechende Sicherheitsmaßnahmen videobasiert demonstriert und bereits die ersten Einblicke ins Lernlabor gegeben. In individuellen Aufgaben können die Lernenden ihr neu erworbenes Wissen gleich anwenden und überprüfen. Sie erhalten dazu Rückmeldung und können so ihren Wissensstand entsprechend einschätzen.

Mit kurzen Online-Kursen können die Teilnehmer sich ideal auf das Präsenz-Seminar vorbereiten und danach ihren Wissenstransfer unterstützen.

Wissen im Lernlabor zur Anwendung bringen

Mit den wichtigsten Vorkenntnissen ausgestattet, wird die Zeit in der Präsenzphase effektiv genutzt, um das Wissen zu vertiefen und direkt anzuwenden. In den Lernlaboren simulieren die Fraunhofer-Expertinnen und -Experten die Arbeitsumgebungen der jeweiligen Themenfelder authentisch durch entsprechende Hard- und Software sowie passende Virtualisierungen. So können sich die Teilnehmenden in einem geschützten Rahmen Fähigkeiten aneignen, ihr neues Wissen ausprobieren, Methoden und Vorgehensweisen üben und auch mal in die Rolle des Angreifers schlüpfen. Unsere Fachexpertinnen und -experten begleiten diesen Prozess, leiten an, vertiefen Inhalte und veranschaulichen mit Praxisbeispielen. Zusätzlich gibt es in den Präsenzphasen die Gelegenheit, sich intensiv auszutauschen, um sowohl von den Erfahrungen der anderen Teilnehmen als auch der Expertise der Fachreferentinnen und -referenten der Fraunhofer-Institute und Fachhochschulen zu profitieren.

Den Transfer in den Berufsalltag meistern

Nach der Präsenzphase im Lernlabor stehen optional weitere Lerninhalte und Übungsaufgaben online zur Verfügung, die die Anwendung des neuen Wissens im eigenen Arbeitsalltag gezielt unterstützen. Durch diesen Blended-Learning-Ansatz kann sichergestellt werden, dass der Transfer der neu erworbenen Fähigkeiten in den Berufsalltag gelingt.

Das aktuelle Angebot an Online-Kursen im Lernlabor Cybersicherheit finden Sie unter
www.academy.fraunhofer.de/onlinekurse-cybersicherheit

QUALIFIZIERUNG AUF DEM AKTUELLSTEN STAND

Im Lernlabor Cybersicherheit arbeiten Fraunhofer und ausgewählte Partnerhochschulen zusammen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Dieser Kooperationsverbund wird vom Bundesministerium für Bildung und Forschung gefördert.

Fraunhofer-Gesellschaft

Die Fraunhofer-Gesellschaft hat in ihrem Strategie- und Positionspapier zur Cybersicherheit 2020 eine nationale Forschungsagenda beschrieben. Ihre Institute kennen die Bedarfe der Industrie und sind in bedeutenden Initiativen zur Cybersicherheit eingebunden, etwa Industrial Data Space, Center for Research in Security and Privacy, Kompetenzzentrum für angewandte Sicherheitstechnologie etc.

Fraunhofer Academy

Die Fraunhofer Academy ist die Plattform der Fraunhofer-Institute, auf der sie gemeinsam mit ausgewählten Partnern ihre Kompetenzen für den Wissenstransfer aus der Fraunhofer-Forschung in die Praxis einbringen. Die Angebotsentwicklung, Vermarktung und Qualitätssicherung koordiniert die gemeinsame Geschäftsstelle in München.

Fachhochschulen

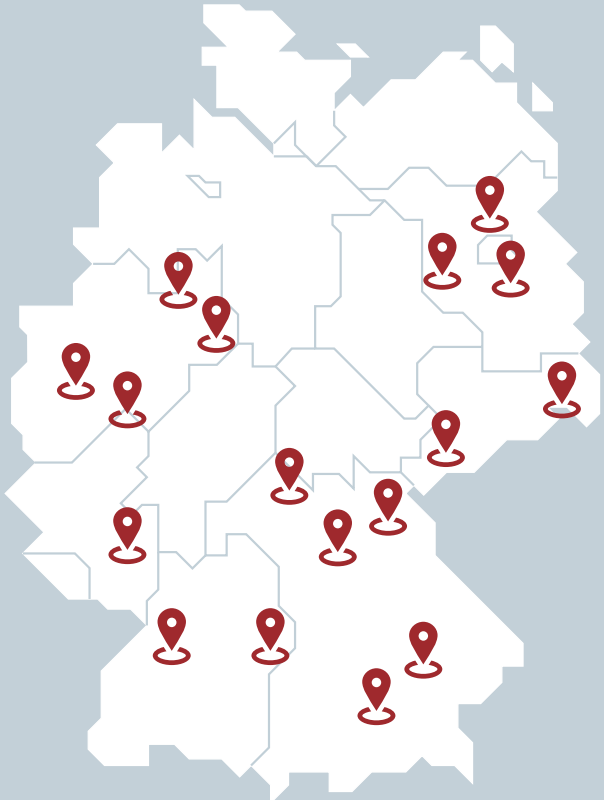
Die beteiligten Fachhochschulen haben durch ihre Kooperation mit der Wirtschaft, insbesondere mit den ansässigen KMU, eine starke regionale Verankerung. Zudem spielen sie eine tragende Rolle in der Ausbildung von Fach-und Führungskräften in Deutschland. Sie bilden für die regional ansässige Industrie einen wichtigen Talentpool für die Einstellung neuen Personals.

Beteiligte Fraunhofer-Institute

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

Beteiligte Partnerhochschulen

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



IHR ANSPRECHPARTNER IM LERNLABOR CYBERSICHERHEIT

Adem Salgin
Organisation und Anmeldung
im Lernlabor Cybersicherheit

Für Fragen zu den aktuellen und geplanten Angeboten im Bereich Cybersicherheit steht Ihnen das Team der Fraunhofer Academy gerne zur Verfügung. Wir beraten Sie, welche unserer Weiterbildungsmodule für Sie zielführend sind. Für Firmenkunden bieten wir zudem Inhouse-Schulungen und unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung.

Herausgeber
Fraunhofer Academy
Hansastraße 27c
80686 München

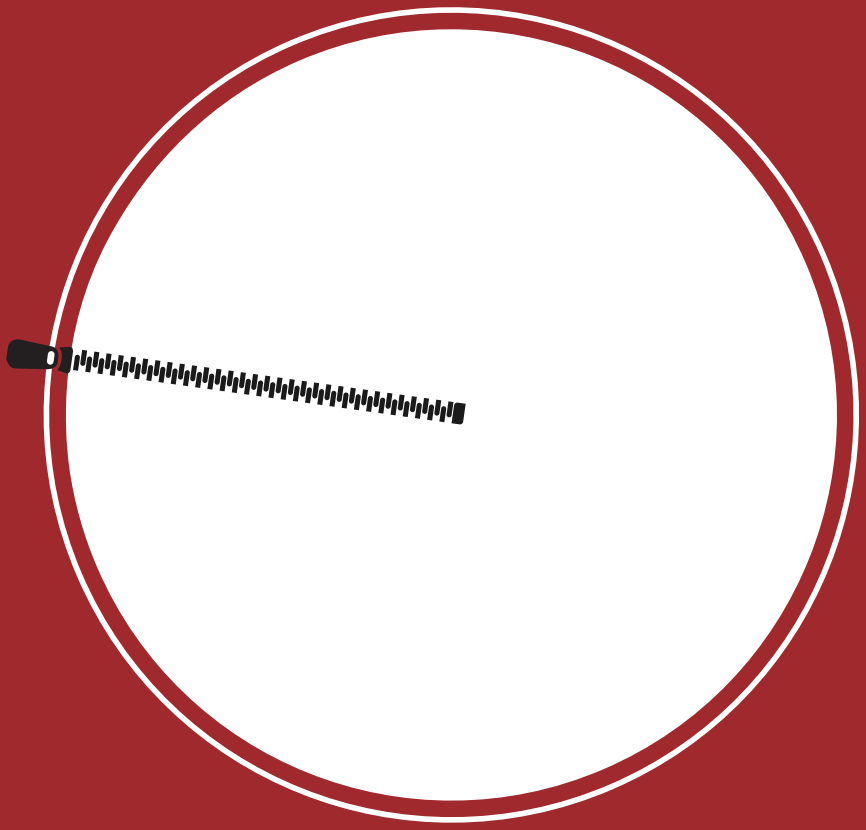
Telefon +49 89 1205-1555
Fax +49 89 1205-77-1599
cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Redaktion: Theresia Gierull

Layout und Satz:
Vierthaler & Braun,
Visuelle Kommunikation

Abbildungen: © Fraunhofer, istock, shutterstock, Hochschule Mittweida, Andreas Heddergott/TU Muenchen, Myrzik und Jarisch, Adrian Zimmermann/Fraunhofer AISEC, Fraunhofer IOSB, Fraunhofer IOSB-INA; Stand Oktober 2018

Lernlabor
Cybersicherheit



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

www.cybersicherheit.fraunhofer.de