Fraunhofer
ACADEMY

SEMINARKATALOG 2. HALBJAHR 2019

FIT IN IT-SICHERHEIT

WEITERBILDUNG IM LERNLABOR CYBERSICHERHEIT

70 JAHRE
FRAUNHOFER
70 JAHRE
ZUKUNFT
#WHATSNEXT

MIT DEM RICHTIGEN TRAINING FIT IN IT-SICHERHEIT BLEIBEN

In der Weiterbildungsinitiative Lernlabor Cybersicherheit schulen Experten und Expertinnen aus der Forschung praxisnah zu den aktuellsten Themen der IT-Sicherheit. Das Programm ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um neue Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Wirtschaft und Behörden erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen und modernen IT-Laboren.

AUS DER FORSCHUNG IN DIE PRAXIS:

OFFENE SEMINARE

INHOUSE-SCHULUNGEN

UNTERNEHMENSPROGRAMME

ONLINEKURSE

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 speziell in der Anwendung aktueller Werkzeuge geschult werden, begrüßen wir sehr.« *Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense bei der Deutschen Telekom AG*

SEMINARE ZUR IT-SICHERHEIT

IT-Sicherheitslabor an der Hochschule für Technik und Wirtschaft Berlin

ERFOLGREICH IM UNTERNEHMEN DURCH IT-FITNESS

Mehrwert für das Unternehmen durch IT-Sicherheit

IT-Infrastrukturen und digitale Systeme bilden das Herz im Unternehmen, das alle Prozesse am Laufen hält. Der Einsatz von Informations- und Kommunikationstechnologien ist in praktisch allen Wirtschaftsbranchen ein entscheidender Faktor für die Wettbewerbsfähigkeit der Unternehmen. Diese Technologien durchdringen branchenübergreifend Wertschöpfungsketten und sind inzwischen einer der wichtigsten Treiber von Innovationen.

Dadurch sind IT- und Kommunikationsinfrastrukturen einerseits von zentraler Bedeutung für Wirtschaft und Wohlstand in Deutschland, andererseits entstehen durch den breiten Einsatz von digitalen Systemen erhebliche Risiken für Wirtschaft und Gesellschaft. Das gilt insbesondere dann, wenn informationstechnische Systeme, Anwendungssoftware oder Infrastrukturen nicht hinreichend sicher sind. Lücken in der IT-Sicherheit können zu Fehlern oder gar Stillstand im Arbeitsprozess führen und große finanzielle sowie Imageschäden versuchen.

Aufgrund dieser großen Abhängigkeit von Informationstechnologie ist deren Schutz besonders wichtig. IT-Sicherheit ist somit eine Querschnitts- und Schlüsseltechnologie für eine funktionierende moderne Gesellschaft und Industrie und steht für die Erlangung digitaler Souveränität an erster Stelle. Die richtigen Fähigkeiten und Kompetenzen in der IT-Sicherheit verringern im Unternehmen das Risiko durch Schadsoftware und Hackerangriffe, sie schützen das Know-how im Betrieb, tragen zum Wettbewerbsvorteil, zur Kundenzufriedenheit und schlussendlich zum wirtschaftlichen Erfolg bei.

Fit bleiben durch IT-Security-Trainings

IT-Sicherheit ist eine Querschnittsaufgabe, die sich über alle Bereiche und Prozesse des Unternehmens erstreckt. Um diese Aufgabe erfolgreich zu meistern, sind nicht nur technische Abwehrsysteme notwendig, sondern vor allem die richtigen Fähigkeiten und stets aktuelles Wissen.

Im Trainingsangebot des Lernlabor Cybersicherheit können Sie und Ihr Unternehmen bei dem IT-Fitness-Level einsteigen, das für Sie das richtige ist. Unsere Kurse haben wir in kleinen, modularen Einheiten von ein bis drei Tagen angelegt, damit sich die Weiterbildung kompakt in den Berufsalltag integrieren lässt und Ressourcen nicht über längere Zeiträume gebunden sind.

Die Kurse orientieren sich passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Die Module sind außerdem branchen-, themen- und funktionsspezifisch auf die Bedarfe der Wirtschaft und Behörden abgestimmt – so trainieren Sie also auch in den Bereichen, die für Sie tatsächlich relevant sind.

KOMPETENZAUFBAU AUF ALLEN EBENEN

IT-Sicherheitswissen für alle Anforderungsprofile

Um IT-Sicherheitskonzepte wirksam und ganzheitlich umzusetzen, sind nicht nur IT-Sicherheitsfachkräfte gefragt, sondern auch Entscheider, Fachkräfte und Anwender. Sie alle benötigen eine große Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und Konsequenzen von IT-Sicherheitsproblemen – insbesondere in kleineren und mittelständischen Unternehmen sowie Behörden. Ziel ist es, mögliche Risiken für das unternehmerische Handeln zu reduzieren und sicher zu beherrschen. Deshalb adressiert das Lernlabor Cybersicherheit genau diese Zielgruppen mit jeweils spezifischen Seminaren:

- **Führungskräfte,** die IT-Sicherheit auf der Entscheidungs- und Prozessebene verantworten, benötigen einen verständlichen Überblick über aktuelle Gefahren und Sicherheitsstrategien.

- **Sicherheitsexperten,** die eine IT-Sicherheitsausbildung oder die entsprechende Berufserfahrung vorweisen und beispielsweise für die IT-Sicherheit in Unternehmen oder von Produkten und Dienstleistungen zuständig sind, bringen dafür ihr Wissen auf den neuesten Stand.

- **Fachkräfte und Spezialisten,** die in ihrem speziellen Anwendungsfeld IT-Sicherheit mit berücksichtigen sollen, müssen Sicherheitsexpertise aufbauen.

- **IT-Nutzer und Anwender** ohne spezifische IT-Ausbildung müssen Sicherheitsbewusstsein und sicherheitskonformes Verhalten entwickeln.

Trainings im richtigen Format

Das Universalkonzept bei IT-Sicherheitsschulungen, das immer für alle passt, gibt es nicht. Deshalb entwickeln wir kompakte, transferorientierte Formate, die sich den tatsächlichen Bedarfen und Problemen von Einzelpersonen oder Unternehmen anpassen.

- In unseren **offenen Seminaren** können sich einzelne Mitarbeitende weiterbilden und kommen so in Austausch mit Beschäftigten anderer Unternehmen.

- Für mehrere Mitarbeitende oder Abteilungen führen wir die Kurse aber auch als geschlossene, firmenspezifische Kurse durch. Wir passen die Inhalte individuell auf die jeweiligen Bedarfe an und führen die Seminare nach Möglichkeiten auch **inhouse** durch.

- Wenn einzelne Inhouseschulungen den Qualifizierungsbedarf nicht decken, entwickeln wir mit Ihnen ein spezifisches **Unternehmensprogramm** mit flexiblen und kombinierbaren Modulen in kompakten Event-Formaten.

- Unsere **Onlinekurse** können Sie als Einzelangebot wahrnehmen, um in ein Thema einzusteigen, Grundlagen aufzufrischen oder erste Anwendungsfälle kennenzulernen. Die Onlinekurse lassen sich aber auch mit den Präsenzseminaren im Lernlabor Cybersicherheit zu Blended-Learning-Formaten kombinieren.

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 Netzwerkverbindungen 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 identifizieren. Auch neueste Entwicklungen im Bereich von Kommunikationsprotokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software müssen in den Produktionsanlagen umgesetzt werden, um sie effektiv schützen zu können.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 und 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, analyzing 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 Unternehmenssystem 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)

CURRICULUM:
SICHERE INDUSTRIELLE VERNETZUNG

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 und 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 und inhouse | 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 und inhouse | 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 und inhouse | 1.800 €

Designen Sie das Curriculum zur sicheren industriellen Vernetzung für Ihr Unternehmen.

Mit den Bausteinen dieses Curriculums schaffen Sie in Ihrem Unternehmen eine sichere Vernetzung. Ganz bedarfsgerecht können die jeweils verantwortlichen Mitarbeitenden in dem Level und Modul einsteigen, das für die Unternehmenssituation, Vorkenntnisse und Kompetenzbedarfe geeignet ist.

Geeignete Problemlöse-strategien entwickeln

Sichere Umsetzung von Industrie 4.0-Anwendungen

Problemlöse-kompetenz und Methodenspektrum erweitern

Betrieb sicherer industrieller Netzwerke

Aufbau sicherer industrieller Netzwerke

Grundlegende Konzepte verstehen

IT-Sicherheit für Industrie 4.0 – Bedrohungslage und Handlungs-bedarf

www.academy.fraunhofer.de/sichere-industrielle-vernetzung

IT-SICHERHEIT IN DER AUTOMATISIERUNGSTECHNIK

Auf dem Weg zur Industrie 4.0 – aber sicher!

Die Herausforderung: Sicherheitsaspekte bei der Transformation zu Industrie 4.0

Bei dem Thema Industrie 4.0 stehen vor allem der Bezug zum eigenen Unternehmen und die möglichen Risiken und Chancen im Mittelpunkt. Für produzierende Unternehmen im Mittelstand ist es eine wichtige Voraussetzung, den aktuellen Zustand ihrer bestehenden Anlagen und Produktionsstätte zu verstehen, bevor sie den Weg zur Industrie 4.0 beschreiten. Dies ist für die Umsetzung geeigneter Schutzmaßnahmen für ihre Systeme im Zuge der digitalen Transformation notwendig.

Die Lösung: Digitale Assets kennen und schützen

Zunächst gilt es, die aktuelle Technik abzusichern, bevor neue Lösungen der Industrie 4.0 zum Einsatz kommen. Das 3-tägige Seminar »IT-Sicherheit in der Automatisierungstechnik« bietet eine praxisnahe Einführung in die Kommunikations- und Automatisierungstechnik. Sie erhalten einen ganzheitlichen Ausblick auf das Thema Industrie 4.0 und seine sicherheitskritischen Aspekte – in praktischen Übungen und in der Theorie. Dazu stellt das Fraunhofer IOSB-INA in Kooperation mit dem Institut für Industrielle Informationstechnik der Hochschule OWL eine hochmoderne Laborinfrastruktur zur Verfügung. Diese Schulung vermittelt die Grundlagen, um darauf aufbauende Weiterbildungen zu spezifischen Themen rund um IT-Sicherheit im Produktionsumfeld zu belegen.

Inhalte

Einführung in die Automatisierungstechnik
- Automatisierungstechnik
- Industrie 4.0
- Kommunikation mit OPC UA

Praktische Übung: Netzwerkkonfiguration, Steuerungsprogrammierung und OPC UA

Netzwerke und Analyse
- Public Key Infrastructure (PKI)
- Grundlagen Netzwerkanalyse

Praktische Übungen, Public Key Infrastructure (PKI) und Netzwerkanalyse OPC UA sowie Profinet

Angriff und Absicherung
- Angriffsszenarien auf Automatisierungstechnik
- Absicherung von Netzwerkinfrastruktur

Praktische Übung: Angriffsszenarien, Firewall, Virtual Private Network (VPN)

Zielgruppe

Mitarbeiterinnen und Mitarbeiter im Bereich Entwicklung, Betrieb sowie Planung von industrieller Automatisierungstechnik; Personal mit IT-Hintergrund, das sich mit industrieller Automatisierungstechnik vertraut machen möchte

»Das Seminar war sehr interessant und fachlich breit aufgestellt. Die Grundlagen und das Thema Verschlüsselung wurden interessant aufgearbeitet – diese sind in einem guten Überblick in den Leitfäden zusammengefasst. Unser wichtigstes Fazit, insbesondere für die Anwendungsebene: Security muss funktionieren, ohne restriktiv zu sein!« *Ralf Meier, Jowat SE*

»Besonders habe ich die technische Umgebung des Seminars geschätzt, die Ausstattung und die Räumlichkeiten waren optimal. Die Ausführungen waren sehr praxisorientiert, die Vortragenden haben sich detailliertes Feedback und Vorstellungen der Teilnehmenden eingeholt. 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*

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… direkt am nächsten Arbeitstag die neu erlernten Sicherheitskonzepte in Ihrem Betrieb anwenden.

Dieses Seminar bietet Ihnen …
… praktische Anwendung der Seminarinhalte in einzigartiger hochmoderner Laborinfrastruktur.
… Know-how von morgen aus Forschung und Entwicklung in einer der stärksten Regionen im Bereich Kommunikations- und Automatisierungstechnik.
… kleine, geschlossene Seminargruppen mit großem Fokus auf praktischer Anwendung und direktem Austausch mit den Experten.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/it-sicherheit-automatisierungstechnik

INFORMATIONEN IM ÜBERBLICK

Kurs: IT-Sicherheit in der Automatisierungstechnik
Voraussetzungen: Keine, technischer Hintergrund wird empfohlen
Dauer: 3 Tage in Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: SmartFactoryOWL, Lemgo
Kosten: 1.800 €

Veranstaltet durch

Fraunhofer IOSB-INA

TH OWL Technische Hochschule Ostwestfalen-Lippe University of Applied Sciences and Arts

Lernziele

- Aktuelle Automatisierungssysteme kennenlernen: vom klassischen System bis zum cyber-physischen Produktionssystem im Sinne der Industrie 4.0
- Etablierte Methoden zur sicheren Industrie 4.0-Kommunikation mit OPC UA anwenden, um Industrie 4.0-Anwendungsfälle wie Condition Monitoring, Plug & Work und Optimierung zu realisieren
- Sicherheitskonzepte erlernen und so gestärkt und sensibilisiert sein für sicherheitskritische Vorgänge

UNSERE REFERENTEN

**Prof. Dr. Stefan Heiss | Jens Otto, M.Sc. | Felix Specht, M.Sc.
Andreas Schmelter, M.Sc. | Abdul Sami Nassery, M.Sc.
Simon Stöhr, M.Sc.**

ANSPRECHPARTNER

Jens Otto, M.Sc.
Gruppenleiter Cybersicherheit
Fraunhofer IOSB-INA
Telefon +49 5261 94290-44
jens.otto@iosb-ina.fraunhofer.de

ENERGIE- UND WASSERVERSORUNG

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 zu einer 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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 Manager*

1 Tag Präsenz | Berlin, München und inhouse | 600 €

Informationssicherheitsbeauftragte in der Energie- und Wasserversorgung

Die Aufgaben der Informationssicherheitsbeauftragten 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 und inhouse | 600 €

»Das Seminar ›IT-Sicherheit für Energie- und Wasserversorgung‹ hat mich durch die sehr kompetenten Vorträge und erfrischenden Diskussionen überzeugt. Für meine strategische Arbeit konnte ich aus dem Tag viel mitnehmen und kann deshalb das Seminar sehr weiterempfehlen.«

Susanne Kufeld, Leiterin DB-Lagezentrum und globales Krisenmanagement, zivile Verteidigung der Deutschen Bahn AG, zum Seminar »IT-Sicherheit für Energie- und Wasserversorgung«

CURRICULUM:
SICHERE ENERGIEAUTOMATISIERUNG

SICHERE ENERGIEAUTOMATISIERUNG

Praktische Cyberabwehr in der Energieautomatisierung

Sicherheitslücken einer realen Beispielkonfiguration aus dem Energiesektor aufdecken und untersuchen: Netzwerkkomponenten analysieren, Netzwerkstrukturen absichern, Sicherheitsaspekte in unterschiedlichen Netzkonfigurationen und -strukturen untersuchen.

» *für Fernwirktechniker, Informationssicherheitsbeauftragte*
3 Tage Präsenz | Ilmenau und inhouse | 1.800 €

Robustheit elektrischer Energienetze gegen Cyberangriffe

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

» *für Fernwirktechniker und Netzplaner*
2 Tage Präsenz | Ilmenau | 1.200 €

Datenschutz für Energiedatenmanager

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 Energiedatenmanager*
1 Tag Präsenz | in Ilmenau, Görlitz, München und 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 Energiedatenmanager*
1 Tag Präsenz | Ilmenau, München und inhouse | 600 €

Sichere Konfiguration von Automatisierungssystemen in der Energietechnik

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

» *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 und CISO*
2 Tage Präsenz | Ilmenau, Görlitz und inhouse | 1.200 €

Designen Sie das Curriculum zur sicheren Energieautomatisierung für Ihr Unternehmen.

Mit den Bausteinen dieses Curriculums schaffen Sie in Ihrem Unternehmen eine sichere Energieautomatisierung. Ganz bedarfsgerecht können die jeweils verantwortlichen Mitarbeitenden in dem Level und Modul einsteigen, das für die Unternehmenssituation, Vorkenntnisse und Kompetenzbedarfe geeignet ist.

www.academy.fraunhofer.de/sichere-energieautomatisierung

AUTOMOTIVE SECURITY

Automobile ohne vernetzte technische Systeme und Komponenten sind heute schon nicht mehr vorstellbar. Daher sind Sicherheitsfragestellungen mehr denn je von zentraler Bedeutung: Die Vernetzung und Komplexität von Systemen im Fahrzeug stellen 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. Die Sicherheit der eingebetteten Systeme müssen in diesem Themenfeld natürlich auch mit berücksichtigt werden. Die Kurse zu Embedded Systems finden Sie auf S. 22, die bei Bedarf auch speziell für den Automotive-Bereich angepasst werden können.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 Softwarearchitekten, -ingenieure und -entwickler*
2 Tage Präsenz | 1.200 € | Garching bei München, Weiden i. d. Oberpfalz und inhouse

IT-Sicherheit in der Fahrzeugkommunikation

Vernetzung im Fahrzeug absichern: Risiken und Lösungswege in der Fahrzeugkommunikation kennenlernen, kryptografische 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 und 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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 und inhouse

Strategische Fragen der IT-Sicherheit und ihre Auswirkung 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 Manager im Bereich KRITIS/BOS*
1 Tag Präsenz | 600 € | Berlin und inhouse

IT-Sicherheit für Public-Safety-Anwendungen

Kritische IT-Systeme mit spezifischen Software-Engineering-Methoden entwickeln: Anforderungen und Lösungsmöglichkeiten für IT-Infrastrukturen, Betriebssysteme und Datenbanken auf Anwendungsebene und mobile Anwendungen umsetzen, Angriffsdetektion und -analyse sowie Schutzmaßnahmen durchführen.

» *für Entwickler von kritischen IT Systemen, Sicherheitsverantwortliche, Projektleiter für IT-Systeme, KRITIS und BOS*
3 Tage Präsenz | 1.800 € | Berlin und 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

IT-SICHERHEITSTECHNOLOGIEN

ENTWICKLUNG UND TESTING SICHERER SOFTWARE

PRODUKTZERTIFIZIERUNG

IT-FORENSIK

SCHADSOFTWARE- UND FIRMWAREANALYSE

NETZWERKSICHERHEIT

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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/embedded-security**

IT-Sicherheitsanalysen und -tests für Embedded Systems

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

» *für Embedded-Entwickler und -Sicherheitsexperten*
2 Tage Präsenz | Darmstadt und 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 und 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, Hardwarearchitekten, Manager*
1 Tag Präsenz | Garching bei München und 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, Hardwarearchitekten, Manager*
1 Tag Präsenz | Garching bei München und 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 und inhouse | 1.200 €

Advanced Linux Security

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

» *für System- und Softwareentwickler*
3 Tage Präsenz | Garching bei München, auf Nachfrage in Weiden i. d. Oberpfalz und inhouse | 1.800 €

Security in Embedded Systems (online)

Sicherheitsaspekte bei dem Einsatz und der Entwicklung von Embedded Systems verstehen: mögliche Gefahren und Schwachstellen erkennen, Schutz von Hardware und Software nachvollziehen, sichere Entwicklungsprozesse für Embedded Systems richtig umsetzen.

» *zum Einstieg oder zur Vertiefung in Sicherheitsaspekte eingebetteter Systeme*
4,5 Stunden | Onlinekurs | 250 €

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 Internetanbindung 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. Kurse zum Thema Netzwerksicherheit finden Sie auf S. 37.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/iot-sicherheit**

IoT-Sicherheit – Sicherheit in drahtlosen Netzen

Vermittlung von Sicherheitsmechanismen und Angriffsflächen verschiedener drahtloser Technologien. Entwicklung und praktisches Erproben sicherer IoT-Anwendungen für eine sichere IoT-Kommunikation.

» *für Administratoren, Anwender, Entwickler*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

IoT-Sicherheit – Sichere und zuverlässige Protokolle

Aufbau, Sicherheit und Zuverlässigkeit von MQTT- und CoAP-Protokollen. Identifikation von Sicherheitslücken und deren Vermeidung. Herausforderungen und Risiken zum Thema Firmware-Updates und Energieverbrauch.

» *für Anwender, Berater, Entwickler*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

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 Softwarearchitekten und -entwickler*
1 Tag Präsenz | Aalen und inhouse | 600 €

Device Identity Management

Aufzeigen von Lösungen aus Praxis und Forschung für eine zuverlässige und eindeutige Identifizierbarkeit von Geräten, um einen vertrauensvollen und sicheren Informationsaustausch im IoT gewährleisten zu können.

» *für Fachkräfte und Entscheider*
1 Tag Präsenz | Nürnberg und 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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/mobile-security**

5G Security

Vorstellung des Mobilfunk-Standards der Zukunft 5G als Enabler für neue Applikationen und Geschäftsmodelle: aufzeigen von Sicherheitsmechanismen und Konzepten der 5G-Technologien, Erläuterung anhand praktischer Anwendungsbeispiele.

» *für Fachkräfte, Entscheider*

1 Tag Präsenz | Nürnberg und inhouse | 600 €

Pentesting Mobile Applications

Übersicht über aktuell verbreitete Gefahren in Android Apps, selbstständiges Erkennen der von Android Apps ausgehenden Gefahren und praxisorientiertes Kennenlernen verschiedener statischer und dynamischer Verfahren und Werkzeuge zur Analyse von Android Apps.

» *für Entwickler, Tester und Entscheider von Apps*

1 Tag Präsenz | Garching bei München und inhouse | 600 €

IT-SICHERHEITSTECHNOLOGIEN

Ausgelöst durch revolutionäre technische 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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/it-sicherheitstechnologien**

Blockchain: Einsatzmöglichkeiten und Anwendungen

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, Anwender oder Betreiber*
3 Tage Präsenz | Weiden i. d. Oberpfalz und inhouse | 1.800 €

Blockchain-Technologie: Schnelleinstieg in die Funktionsweise und Bausteine

Vermittlung von Funktionen, Prinzipien und Herausforderungen der Blockchain-Technologie: Möglichkeiten zur Anwendung der Technologie und damit einhergehende Sicherheitsaspekte einschätzen und kritisch bewerten; praktische Vermittlung wichtiger Blockchain-Bausteine.

» *für Entwickler, Berater und Tester*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

Post-Quanten Sicherheit

Funktionsweise eines Quantencomputers sowie dessen Auswirkungen auf die moderne Kryptografie verstehen. Einführung in quantensichere Mechanismen und die heute schon laufenden Bemühungen einer rechtzeitigen Standardisierung zur Absicherung vorstellen.

» *für Entwickler*
2 Tage Präsenz | Weiden i. d. Oberpfalz und inhouse | 1.200 €

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 | Onlinekurs | 150 €
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 | Onlinekurs | 550 €
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 | Onlinekurs | 350 €
in Kooperation mit University4Industry

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 | Onlinekurs | 120 €
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 | Onlinekurs | 340 €
in Kooperation mit University4Industry

ENTWICKLUNG UND TESTING SICHERER SOFTWARE

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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 Softwarearchitekten, Entwicklungs- und Projektleiter*
2 Tage Präsenz | Brandenburg an der Havel und inhouse | 1.200 €

Softwarehärtung: Software gegen Schwachstellen sichern – Advanced

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

» *für Softwareentwickler*
2 Tage Präsenz | Berlin und 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 und 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 | Weiden i. d. Oberpfalz und 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 und inhouse | 1.200 €

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 und inhouse | 1.800 €

Maschinelles Lernen für mehr Sicherheit

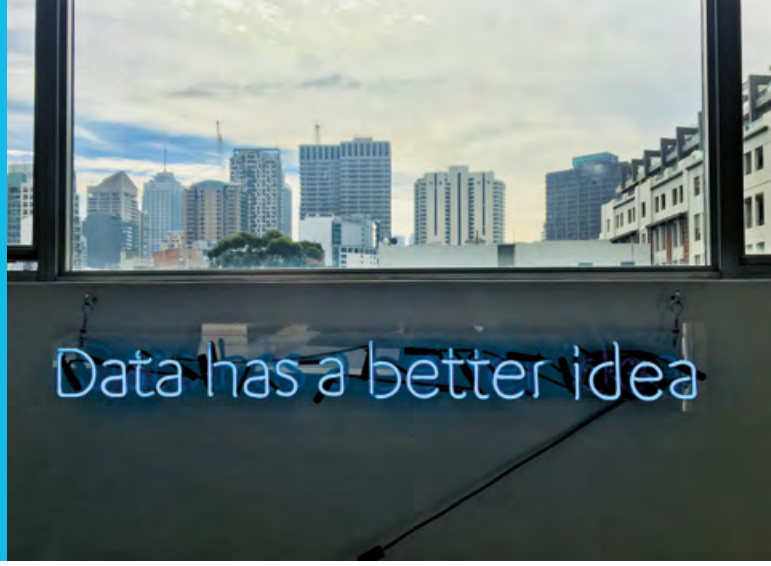
Maschinelles Lernen und Date Mining für die Modellierung von Anomalienerkennung in der IT-Sicherheit nutzen: Grundlagen des maschinellen Lernens und des Data Mining kennen, Grundlagen der Modellierungsmethoden zur Anomalienerkennung vertiefen.

» *für Sicherheitsingenieure, IT-Analysten, System-/Softwareentwickler*
1 Tag Präsenz | Garching bei München | 600 €

Sicheres Implementieren und Testen in C

Überblick über sicherheitsrelevante Komponenten in den einzelnen Softwareentwicklungsphasen. Ein besonderes Augenmerk liegt hierbei auf sicherheitskritischen Problemen beim Implementieren sowie dem Testen auf Sicherheitslücken.

» *für Entwickler*
1 Tag Präsenz | Weiden i. d. Oberpfalz und inhouse | 600 €



MASCHINELLES LERNEN FÜR MEHR SICHERHEIT

Methoden zur Anomalienerkennung modellieren

Die Herausforderung: Sicherheitslösungen skalieren bei zunehmenden Datenmengen nicht

Durch die Vielzahl an Daten ist es schwierig, einen Überblick zu bewahren. Maschinelles Lernen ist daher eine Trendtechnologie. Bei der Analyse großer Mengen an Daten ist maschinelles Lernen in der Lage, Vorhersagen zu machen und Entscheidungen automatisch zu treffen. Im Bereich der Cybersicherheit nimmt die Datenmenge so rasant zu, dass aktuelle Sicherheitslösungen kaum skalieren; darüber hinaus müssen Security-Experten im Wettlauf so schnell wie möglich Gegenmaßnahmen entwickeln und einsetzen, um neuartige Angriffe abzuwehren. Dies stellt uns vor große Herausforderungen, die wir mit statistischen Methoden wie maschinelles Lernen meistern können.

Die Lösung: Entscheidungsmodelle mithilfe maschinellen Lernens erstellen

Mit maschinellem Lernen kann man zahlreiche Daten aus Sicherheitskomponenten entnehmen und Modelle erzeugen. Diese beschreiben die Eingaben und erstellen Vorhersagen, wodurch auch Entscheidungen getroffen werden können. Mit zunehmender Datenmenge werden diese Modelle kontinuierlich präzisiert, weswegen möglicherweise auch unbekannte Bedrohungen erkannt werden können.

Inhalte

- Überblick über Themen der Cybersicherheit
- Was kann man mit maschinellem Lernen machen?
- Grundlagen des maschinellen Lernens
- Basisverfahren
- State-of-the-Art Wissen zu maschinellem Lernen
- Forschungsgebiete
- Use Case: Anomalienerkennung
- Definition
- Modellierungsmethoden
- Algorithmen/Tools
- Programmierungshinweise
- Take home message

Zielgruppe

Sicherheitsingenieure, Analysten der IT-Sicherheit, Entwickler sicherer Systeme/Software

Lernziele

- Überblick über die Themen der Cybersicherheit, bei denen maschinelles Lernen eine Rolle spielt
- Grundlagen des maschinellen Lernens und Daten Mining kennen und verstehen
- Modellierungsmethoden zur Anomalienerkennung kennen lernen

»Das Seminar ›Maschinelles Lernen für mehr Sicherheit‹ empfand ich als einen rundum großartig organisierten Schulungstag. Besonders das umfangreiche Themenspektrum sowie die sehr kompetenten Referenten mit offenkundiger Praxiserfahrung haben mich überzeugt. Die erlernten Methodiken habe ich auch bereits bei eigenen Problemstellungen im Unternehmen anwenden können.« *Kevin Beck, Specialist Data Analytics & Machine Learning bei Giesecke+Devrient Mobile Security GmbH*

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… einschätzen, in welchen Bereichen Sie maschinelles Lernen sinnvoll einsetzen können.
… Programmierungen und Modellierungen zur Anomalienerkennung vornehmen.

Dieses Seminar bietet Ihnen …
… einen Einstieg in die Themen der Cybersicherheit, bei welchen maschinelles Lernen relevant ist.
… praktische Übungen am Use Case Anomalienerkennung.
… State-of-the-Art-Wissen zu maschinellem Lernen und neuen Forschungen.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/maschinelles-lernen

INFORMATIONEN IM ÜBERBLICK

Kurs: Maschinelles Lernen für mehr Sicherheit
Voraussetzungen: Basiswissen zu Programmierung, IT-Sicherheit und maschinellem Lernen
Dauer: 1 Tag in Präsenz
Kurssprache: Englisch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: Garching bei München
Kosten: 600 €

Veranstaltet durch

Fraunhofer AISEC

UNSERE REFERENTEN

Nicolas Müller
Nicolas Müller ist wissenschaftlicher Mitarbeiter in der Abteilung Cognitive Security Technologies des Fraunhofer AISEC. Seine Forschungsschwerpunkte liegen im Bereich Machine Learning und Anomaly Detection für Cyber Security.

Pascal Debus
Pascal Debus ist wissenschaftlicher Mitarbeiter in der Abteilung Cognitive Security Technologies des Fraunhofer AISEC. Seine Forschungsschwerpunkte liegen im Bereich Machine Learning für Schwachstellensuche in Binaries sowie im Adversarial und Privacy-Preserving Machine Learning.

ANSPRECHPARTNER

Nicolas Müller
Cognitive Security Technologies
Fraunhofer AISEC
Telefon +49 89 3229986-197
nicolas.mueller@aisec.fraunhofer.de

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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/produktzertifzierung**

International Data Space Komponentenzertifizierung

International Data Space Komponentenzertifizierung: Vorteile und Risiken einer IDS-Zertifizierung bewerten, Komponentenzertifizierung auf technischer Ebene verstehen, Zertifizierbarkeit des eigenen Produkts einschätzen, Aufwand für das eigene Produkt realistisch einschätzen.

» *für Hersteller von IDS-Kernkomponenten sowie Techniker, Entwickler, Product Owner*
3 – 5 Tage Präsenz | Garching bei München, Berlin und inhouse | Preis nach Vereinbarung

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, Produktentwickler und technische Einkäufer*
2 Tage Präsenz | Berlin und 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.

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 Analyse von Mobilgeräten.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/it-forensik**

Grundlagen der Datenträger-Forensik

IT-Forensik verstehen und anwenden: IT-forensische Methoden kennen und zur Prüfung von Sicherheitsvorfällen auswählen, IT-forensische Untersuchung planen, selbst durchführen oder extern beauftragen können; Praxis-Übunng: einfache Analyse von Datenträgern.

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

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, IT-Forensiker, Security-Analysten*
2 Tage Präsenz | Bonn und inhouse | 1.200 €

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

Digitale Asservatsicherung

Handlungstraining zur Asservatsicherung digitaler Endgeräte: Grundlagen der digitalen Tatortarbeit und -fotografie, gerichtsfester Umgang mit digitalen Endgeräten, Kompetenzaufbau im Umgang mit forensischen Werkzeugen zur Datensicherung im Planspiel.

» *für Strafverfolger, Justiz und Gutachter*
1,5 Tage Präsenz | Mittweida und inhouse | 900 €

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 und inhouse | 1.200 €

Open Source Intelligence Advanced

Informationsgewinnung und fallspezifische Untersuchungen mit Maltego und Co.: Informations Gathering und OSINT-Recherchen automatisieren, gewonnene Informationen filtern und visualisieren, komplexe Zusammenhänge in den Ergebnissen identifizieren.

» *für Strafverfolger, Justiz, Gutachter, Ermittler*
1 Tag Präsenz | Mittweida und inhouse | 600 €

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 und 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 und inhouse | 1.800 €

Car Forensik – Auswertung vernetzter Systeme

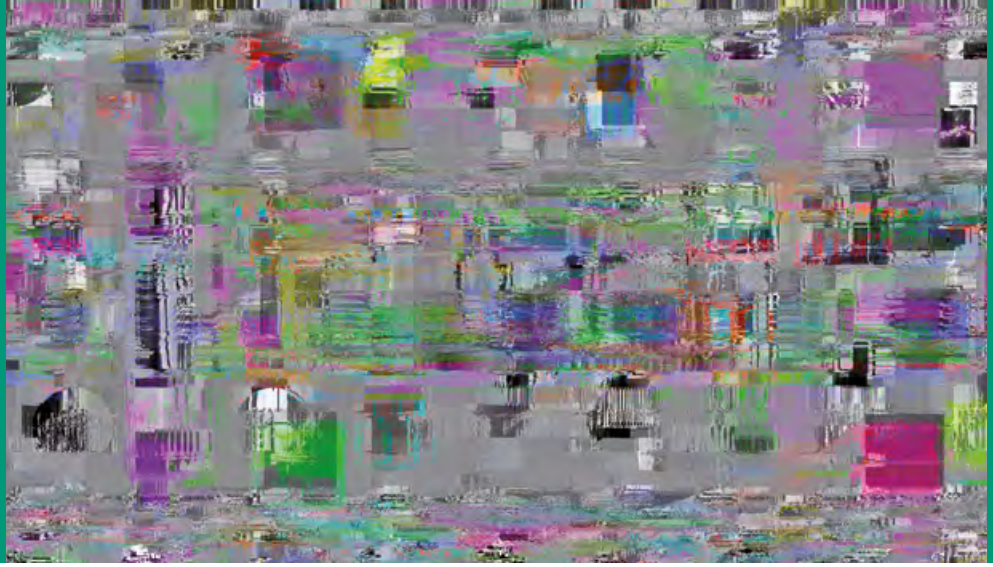
Digitale forensische Auswertung vernetzter IT-Systeme im Kfz: Steuergeräte über den CAN-Bus und Transponderschlüssel auslesen, Daten in Fahrzeugen für die eigene forensische Arbeit nutzen, verschiedenen Modi Operandi bei Kfz-Diebstählen nachvollziehen.

» *für Strafverfolger, Justiz und Versicherungsgutachter*
2,5 Tage Präsenz | Mittweida und inhouse | 1.500 €

Car Forensik – automobile Bussysteme

Angriffserkennung auf Kfz-Bussysteme: Funktionsweise und Kommunikation auf mobile Bussysteme kennenlernen, FlexRay- und CAN-Bussysteme konzipieren und simulieren sowie Angriffe und Manipulationen auf Kfz-Bussysteme erkennen und auswerten.

» *für Fachkräfte und Anwender*
3 Tage Präsenz | Mittweida und inhouse | 1.800 €



Datenschutz für IT-Forensiker

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

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

IT-Forensik für die Erkennung von Bildmanipulationen

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 €

Einführung in Darknet und Kryptowährung

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 und Fachjournalisten*
1 Tag Präsenz | Darmstadt und inhouse | 600 €

Forensische 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 €

Multimedia-Forensik für Ermittlungsverfahren

Spuren in digitalen Bildern, Video- und Audiodaten forensisch auswerten: Grundlagen von Multimedia-Datenformaten 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 und inhouse | 1.200 €

»Ich habe nicht nur viel Neues kennengelernt und konnte bisheriges Wissen ausbauen, sondern es hat vor allem auch sehr viel Spaß gemacht.« *Teilnehmender der Schulung ›Multimedia-Forensik für Ermittlungsverfahren‹*

SCHADSOFTWARE- UND FIRMWAREANALYSE

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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/schadsoftwareanalyse**

Einführung in die Firmwareanalyse

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

» *für Analysten, Entwickler, Reverser*
2 Tage Präsenz | Bonn und inhouse | 1.200 €

Grundlagen Schadsoftwareanalyse Windows

Aktuelle Schadsoftware und deren Verbreitungswege kennen, Systemaufrufe und Netzwerkprogrammierung in disassembliertem Code analysieren sowie allgemein Methoden und Werkzeuge zur statischen und dynamischen Analyse von Windows-Schadsoftware anwenden.

» *für Administratoren, Analysten, CERT-Mitarbeiter*
3 Tage Präsenz | Bonn und inhouse | 1.800 €

Fortgeschrittene Schadsoftwareanalyse Windows

Gängige Verschleierungsmethoden, wie String-Verschlüsselung, API-Verschleierung und Code-Injektionen, kennenlernen, diese umgehen und programmatisch auflösen sowie Analysen automatisieren.

» *für Schadsoftwareanalysten mit ersten Erfahrungen*
2 Tage Präsenz | Bonn und inhouse | 1.200 €

NETZWERK-SICHERHEIT

Netzwerksicherheit ist ein gleichermaßen facetten- wie detailreicher Themenkomplex und fasst alle Fragen zur Sicherheit des Internets als Infrastruktur. Um die Sicherheit in Netzwerkstrukturen ganzheitlich betrachten zu können, sind fundierte Fähigkeiten und Wissen zu den zugrundeliegenden Netzwerktechnologien entscheidend.

In den Schulungsmodulen zu Netzwerksicherheit stehen die sich stetig ändernde Bedrohungslage im Internet und die damit verbundenen Anforderungen der Unternehmen im Fokus. Daher werden neben aktuellen Bedürfnissen der Wirtschaft auch neueste Entwicklungen und Erkenntnisse in den Seminaren aufgegriffen. Kurse zum Thema IoT-Sicherheit finden Sie auf S. 24.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/netzwerksicherheit**

Hands-on Wireless LAN Security

Sicherheitsfunktionen und -risiken von WLANs verstehen: die Sicherheit von WLAN-Netzen richtig einschätzen, Angriffe gegen WLANs mit typischen Tools erproben, WLAN-Infrastrukturen sicher aufbauen, als Entwickler sicheres WLAN in eigene Produkte integrieren.

» *für IT-Administratoren, Produktentwickler und Pentester*
2 Tage Präsenz | Darmstadt und inhouse | 1.200 €

IT-Sicherheit drahtloser Kommunikationssysteme

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

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

IT-Sicherheitsanalyse in Unternehmensnetzen

Schwachstellen in Unternehmensnetzwerken identifizieren und beheben: Netzwerkstrukturen, -komponenten und -protokolle verstehen, bestehende IT-Netzwerke analysieren, Sicherheitsrisiken und Designfehler erkennen, einschätzen und Gegenmaßnahmen einleiten.

» *für IT-Administratoren und IT-Verantwortliche*
2 Tage Präsenz | Darmstadt und inhouse | 1.200 €

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 und inhouse | 600 €

DATENSCHUTZ

Datenschutz ist 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, drängen sich ganz neue Fragestellungen auf, wie datenschutzkonform gearbeitet und die richtigen Maßnahmen umgesetzt werden können.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 und Vertiefung: Personaler, PR- und Kommunikationsmanager, Web-Admins

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 | Onlinekurs | 420 €
aufbauend dazu weitere Onlinevertiefungskurse für
– *Personaler*
– *PR- und Kommunikationsmanager*
– *Web-Administratoren*

Datenschutz für Energiedatenmanager

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 Energiedatenmanager*
1 Tag Präsenz | in Ilmenau, Görlitz, München und 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 fachlich-technischen Anforderungen aufgebaut werden.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **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 | Berlin und 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 Sicherheitsbeauftragte, Sicherheitspersonal, Systementwickler*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

BASICS

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

BASICS DER IT-SICHERHEIT

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 aktuelle 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.

Für weitere Informationen zu den hier gelisteten Kursen, Seminar-Terminen und Inhouse-Anfragen besuchen Sie: **www.academy.fraunhofer.de/basics-it-sicherheit**

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 Manager, Anwender und Fachkräfte*
1 Tag Präsenz | Mittweida und inhouse | 600 €

IT-Sicherheit – Netzwerksicherheit

Schwachstellen in Netzwerken und Angriffsszenarien demonstrieren, um Risiken in Netzen identifizieren zu können und diesen entgegenzuwirken. Gängige Angriffswerkzeuge kennenlernen und eine effektive Abwehr erproben.

» *für Anwender und Einsteiger der Netzwerksicherheit*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

IT-Sicherheit – Kryptografie

Verschiedenene kryptografische Verfahren, deren Einsatzzwecke und Angriffsmöglichkeiten kennenlernen, um diese unter Sicherheitsaspekten zu bewerten. Die Verwendung von Kryptografie in alltäglichen Anwendungen innerhalb praktischer Übungen untersuchen.

» *für Anwender und Einsteiger der Kryptografie*
1 Tag Präsenz | Sankt Augustin und inhouse | 600 €

IT-Sicherheit – Von Prävention bis Reaktion

Aktueller Überblick über das Thema IT-Sicherheit. Verschiedene Aspekte und Grundbegriffe der IT-Sicherheit kennenlernen. Praktische Beispiele zu Angriffsmethoden und entsprechenden Schutzmechanismen sowie der Identifikation von Schutzzielen.

» *für Anwender und Einsteiger*
1 Tag Präsenz | Sankt Augustin, Weiden i. d. Oberpfalz und 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

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 und 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 und inhouse | 600 €

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, Manager*
1 Tag Präsenz | Bonn und inhouse | 600 €

IT-Sicherheit für KMU

Angriffe auf verschiedene Unternehmensstrukturen 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 Manager*
1 Tag Präsenz | München, Görlitz und inhouse | 600 €

Sicherheit webbasierter Systeme

Untersuchung der Sicherheit verschiedener Dienste und Technologien. Schutzmechanismen auf Netzwerk-, Protokoll- und Anwendungsebene kennenlernen sowie Werkzeuge und Vorgehensweisen für Gegenmaßnahmen erproben.

» *für Anwender und Einsteiger in Security webbasierter Systeme*
2 Tage Präsenz | Sankt Augustin und inhouse | 1.200 €

IT-SICHERHEIT FÜR KMU

Digitalisierung – mit Sicherheit!

Die Herausforderung: Zunehmendes Bedrohungspotenzial erfordert Bewusstsein im Management

Mit der zunehmenden Digitalisierung der Gesellschaft steigt das Bedrohungspotenzial durch Cyberattacken deutlich an: Das Risiko, Opfer eines Angriffs zu werden, erhöht sich ebenso kontinuierlich wie die durch Cyberangriffe verursachten Kosten.

Der erfolgreiche Umgang mit diesen Risiken erfordert ein Bewusstsein für Cybersicherheit, Kenntnisse im Management effektiver Schutzmaßnahmen sowie die Fähigkeit, das aktuelle und das notwendige Schutzniveau des eigenen Unternehmens realistisch einzuschätzen.

In den Unternehmen muss eine IT-Sicherheitskultur etabliert werden, da jeder Mitarbeiter Opfer eines Cyberangriffs werden oder einen Angriff identifizieren und so das Unternehmen schützen kann.

Die Lösung: Etablierung einer IT-Sicherheitskultur

Mit vielen anschaulichen Beispielen werden Ihnen Angriffsvektoren und häufige Schwachstellen in Unternehmen aufgezeigt. Welche Schritte für ein umfassendes Schutzkonzept notwendig sind, und wie diese am besten angegangen werden, wird Ihnen ebenfalls vermittelt. Sie lernen die derzeitigen und zukünftigen gesetzlichen Rahmen sowie die vielen vorhandenen IT-Sicherheitsstandards kennen.

Sie werden sensibilisiert für Gefahren beispielsweise am eigenen Arbeitsplatz oder auf Geschäftsreisen, und wie Sie sicher mit diesen umgehen. Ebenfalls werden Ihnen Möglichkeiten aufgezeigt, das Wissen an die eigenen Mitarbeiter weiterzugeben.

Inhalte

- Was sind die aktuellen und zukünftigen Gesetzeslagen zu IT-Sicherheit, die in Ihrem Unternehmen wichtig sind?
- Wie sehen Angriffe und deren Ablauf aus? Was können wir aus typischen Beispielen lernen?
- Wie stelle ich ein schlagkräftiges IT-Sicherheitsmanagement auf?
- Welche Standards existieren für einen umfassenden Schutz?
- Wo sind die Schwachstellen in meinem Unternehmen?
- Wie versuchen Angreifer, mich im Alltag oder in speziellen Situationen (Geschäftsreise) zu schädigen, und wie schütze ich mich persönlich davor?
- Wie gehe ich sicher mit mobilen Geräten um?
- Wie erreiche ich es, dass meine Mitarbeiter eine »Human Firewall« bilden?

Zielgruppe

Geschäftsführer, Führungskräfte, Mitarbeiter aus dem Management, IT-Sicherheitsbeauftragte

Lernziele

- Sich mit der eigenen Verantwortung für die IT-Sicherheit des Unternehmens identifizieren
- Verstehen, wie ein Angriff abläuft, und welche Angriffsvektoren existieren
- Standardvorgehensweisen im eigenen Unternehmen umsetzen und damit verbundenen Aufwand abschätzen
- Angriffe identifizieren und abwehren können
- Aktuelle Gesetzeslage kennen

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… Schwachstellen Ihres Unternehmens identifizieren und Angriffe aktiv verhindern.
… Ihre Mitarbeiter sensibilisieren und auf die Gefahren aufmerksam machen.
… begründete Entscheidungen treffen, um prozessorientierte Maßnahmen zu ermöglichen.
… Ihr Unternehmen in den gesetzlichen Rahmen einordnen und die vorgeschriebenen Maßnahmen einschätzen.

Dieses Seminar bietet Ihnen …
… einen Einblick in verschiedenste IT-Sicherheitsstandards.
… Beispiele für Angriffsvektoren und Schwachstellen in Ihrem Unternehmen.
… Möglichkeiten zur Weitergabe Ihres Wissens an Ihre Mitarbeiter.
… einen Überblick über die aktuelle und zukünftige Gesetzeslage.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/enterprise

INFORMATIONEN IM ÜBERBLICK

Kurs: IT-Sicherheit für KMU
Voraussetzungen: Verständnis für Managementprozesse
Dauer: 1 Tag in Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: 20 Personen
Veranstaltungsort: München, Görlitz und inhouse
Kosten: 600 €

Veranstaltet durch

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Hochschule Zittau/Görlitz

UNSERE REFERENTEN

Adam Bartusiak, M. Sc.
Adam Bartusiak ist wissenschaftlicher Mitarbeiter im Lernlabor Cybersicherheit am Fraunhofer IOSB-AST in Görlitz. Er hat Kommunikations- und Informationsmanagement, Informatik sowie Risikomanagement studiert und als Softwareentwickler wie Forschungsmitarbeiter im Bereich Datenanalyse gearbeitet.

Oliver Nitschke, Dipl.-Inf.
Oliver Nitschke arbeitet als wissenschaftlicher Mitarbeiter im Lernlabor Cybersicherheit am Fraunhofer IOSB-AST in Görlitz. Nach seinem Studium der Informatik war er als IT-Spezialist für einen Schienenfahrzeugfertiger tätig.

ANSPRECHPARTNER

Dennis Rösch, M.Sc.
Abteilung Energie
Fraunhofer IOSB-AST
Telefon +49 3677 461-188
dennis.roesch@iosb-ast.fraunhofer.de

NEUE IT-SICHERHEITSKOMPETENZEN PRAKTISCH IN LABOREN ERWERBEN

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 anwendungsorientierte Praxisphasen im Lernlabor und Onlinelernangeboten ein.

1

2 *IT-Sicherheitslabor in Karlsruhe: Sicher produzieren und automatisieren in der Industrie 4.0.*

Neue Fähigkeiten im Lernlabor direkt anwenden

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 Teilnehmenden als auch der Expertise der Fachreferentinnen und -referenten der Fraunhofer-Institute und Fachhochschulen zu profitieren.

1 *Lernlabor für Energie- und Wasserversorgung in Ilmenau: IT- und Hardwareinfrastrukturen der Energie- und Wasserversorger werden im Labor nachgebildet und in Simulationen angegriffen.*

Problemorientierung und multiple Kontexte fördern den Wissenstransfer

Ein zentrales Ziel der Lernlabore ist es, das erlernte Wissen in den Arbeitskontext zu übertragen. Deshalb gestalten wir unsere Weiterbildungsangebote nach dem Konzept der Problemorientierung: Gelernt wird in einem authentischen Kontext, dem Lernlabor als Lernfeld, das möglichst ähnlich zur tatsächlichen Arbeitssituation gestaltet ist. Dort können die Seminarteilnehmerinnen und -teilnehmer ihr Wissen in einer unkritischen Umgebung praktisch anwenden und ausprobieren. Weiterhin liegt das Prinzip der multiplen Kontexte zugrunde: Die Teilnehmenden schlüpfen im Kurs in verschiedene Rollen, beispielsweise die der Angreifer oder Verteidiger. Der Perspektivenwechsel hilft, das Wissen flexibel zu gestalten. Darüber hinaus interagieren sie mit den anderen Teilnehmenden, die, wie auch im tatsächlichen Arbeitskontext, aus verschiedenen Fachbereichen stammen. So treffen hier zum Beispiel Mitarbeitende aus der Produktion auf Kollegen und Kolleginnen aus der IT-Abteilung.

3 *SmartFactory OWL in Lemgo: mit Demonstrationsanlagen zur standortübergreifenden Produktion die Sicherheit in der Industrie 4.0 erleben und erlernen.*

Und das Konzept geht auf, wie anonyme Befragungen unserer Seminarteilnehmenden ergeben: Die Mehrheit nutzt demnach die in der Weiterbildung erworbenen Kenntnisse auch häufig in ihrer täglichen Arbeit. Zudem äußerte sich die überwiegende Mehrheit der Teilnehmenden sehr positiv zu unseren Veranstaltungen: Sie waren beispielsweise sehr zufrieden mit den Inhalten, den Trainern sowie der Lernumgebung im Lernlabor. Was den Wissenstransfer anbelangt, geht ein Großteil davon aus, das neu erworbene Wissen in der Praxis anwenden und von der Veranstaltung auch im Berufsalltag profitieren zu können.

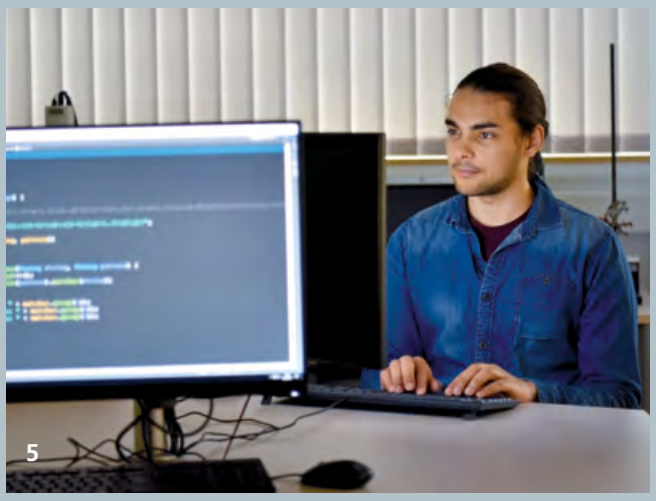
Den Transfer weiter begleiten mit selbstgesteuertem Onlinelernen

Vor und nach den Präsenzphasen können sich die Teilnehmenden zeit- und ortsunabhängig Basiswissen und Grundlagen aneignen oder mit Übungsaufgaben Gelerntes wiederholen. 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. Durch diesen Blended-Learning-Ansatz wird der Transfer der neu erworbenen Fähigkeiten in den Berufsalltag unterstützt.

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

4 *IT-Sicherheitslabor an der HTW Berlin: in Szenarien verschiedene Notfälle der öffentlichen Sicherheit erleben.*

6 *Lernlabor Cybersicherheit in Sankt Augustin: Techniken und Strategien für den Hochsicherheitsbereich kennenlernen, z.B. sichere biometrische Gesichtserkennung.*



5 *Forensiklabor an der Hochschule Mittweida: IT-Forensikkurse umfassen die Vorgehensweise und Werkzeuge zur Identifikation und Extraktion von Spuren.*

7 *Hacking-Labor in Weiden: aus der Sicht des Angreifers – Vorgehensweise von Hackern verstehen, um besser auf mögliche Angriffe vorbereitet zu sein.*

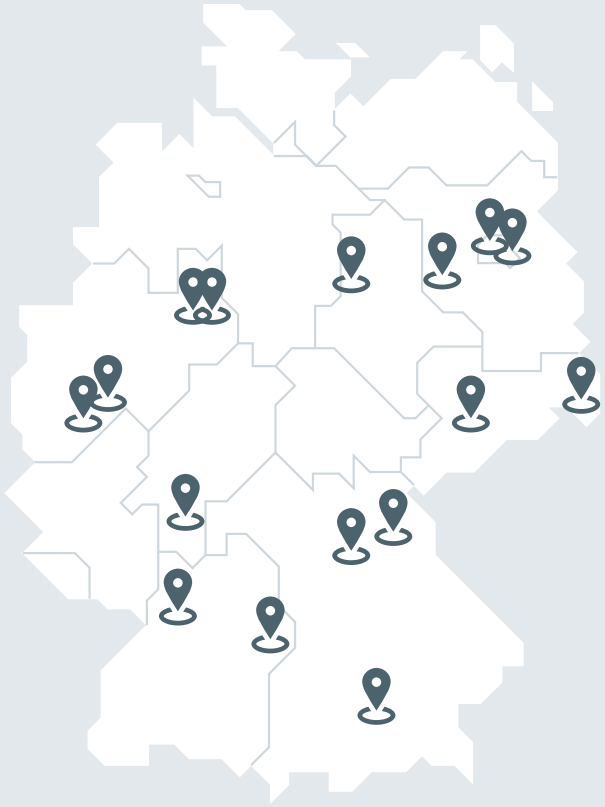
AKTUELLE QUALIFIZIERUNG AUS DER ANGEWANDTEN FORSCHUNG

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 vermittelt. Die Fraunhofer Academy ist die Geschäftsstelle und die 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

- 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

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



Die beteiligten Fraunhofer-Institute

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

Ihr Ansprechpartner im Lernlabor Cybersicherheit
Adem Salgin
Seminarberatung und Anmeldung

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 Ihrem Unternehmen aufzubauen.

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, Titelillustration: Vierthaler & Braun

Stand Mai 2019

Sie erreichen uns

– telefonisch unter **+49 89 1205-1555**

– per E-Mail: cybersicherheit@fraunhofer.de

– auf unserer Website unter

www.cybersicherheit.fraunhofer.de