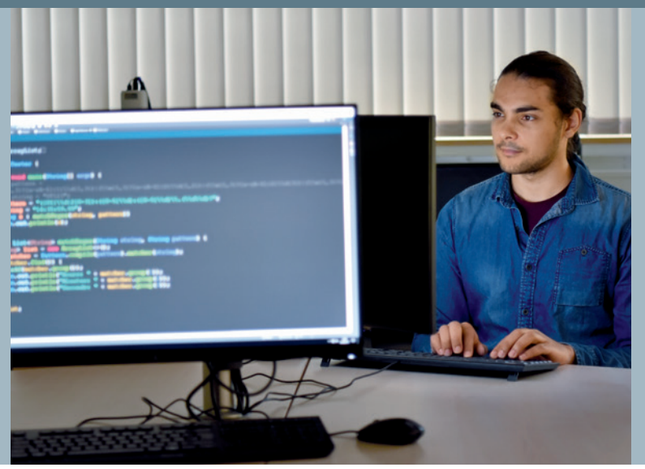
Fraunhofer
ACADEMY

WEITERBILDUNG IM LERNLABOR CYBERSICHERHEIT

DEN HACKERN EINEN SCHRITT VORAUS

WAS ZEICHNET DAS LERNEN IM LERNLABOR CYBERSICHERHEIT AUS?

PRAXISNAHES LERNEN IN LABOREN UND ONLINE

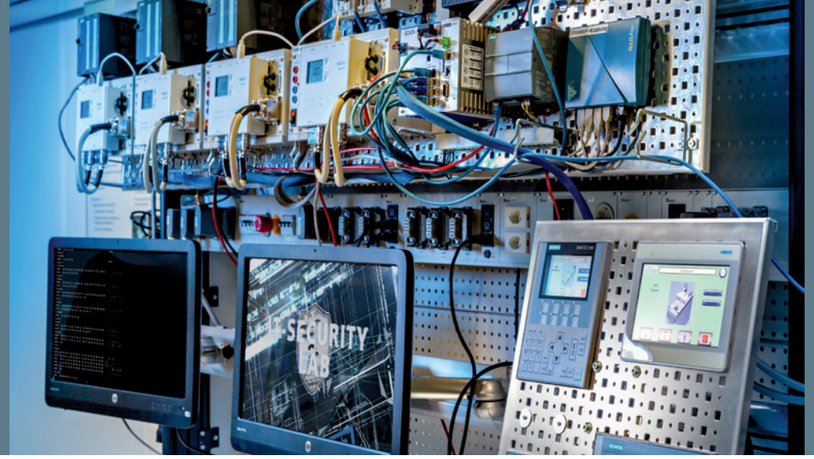


Neben aktuellem Forschungswissen und relevanten Praxisbezügen aus Fraunhofer-Instituten und Fachhochschulen zeichnen sich die Weiterbildungsmodule durch einen idealen Mix aus anwendungsorientierten Praxisphasen im Lernlabor und online verfügbaren Lernangeboten aus.

Grundlegende Inhalte können sich die Teilnehmenden im Vorfeld der Präsenzphase zeit- und ortsunabhängig in ihrem eigenen Lerntempo selbstgesteuert aneignen. Mit diesen Vorkenntnissen ausgestattet, wird die Zeit in der Präsenzphase genutzt, um das Wissen zu vertiefen und anzuwenden, sich neue Fähigkeiten anzueignen und zu üben sowie sich auszutauschen. In den Lernlaboren stehen dafür die passende technische Infrastruktur sowie die Fachexperten zur Verfügung, die anleiten, unterstützen und beraten sowie Inhalte vertiefen und mit Praxisbeispielen veranschaulichen.

Durch diesen Blended-Learning-Ansatz kann sichergestellt werden, dass der Transfer der neu erworbenen Fähigkeiten in den Berufsalltag gelingt.

INHALT



»Besonders das Angebot berufsbegleitender kleinerer Weiterbildungsmodule, in denen Personen sehr transferorientiert und kompakt in aktuellen Themen und der Anwendung aktueller Werkzeuge geschult werden, begrüßen wir sehr.«
Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense bei der Deutschen Telekom AG

WEITERBILDUNG ZU IT-SICHERHEIT FÜR DIGITALE SOUVERÄNITÄT

Die Herausforderung: Zunehmende Cybersicherheits-Risiken, nur wenige Spezialisten

Gut ausgebildete IT-Sicherheitsfachleute sind hierzulande rar gesät. Dabei ist Weiterbildung in der IT-Sicherheit eine Aufgabe von nationalem Interesse: Hohe finanzielle Verluste, Versorgungsengpässe oder Störungen der öffentlichen Sicherheit können die Folgen von Cyberattacken auf kritische Infrastrukturen und Industrieanlagen sein. Das Bedrohungspotenzial wächst mit zunehmender Vernetzung und Digitalisierung. Der Weiterbildungsbedarf ist enorm: Bereits 2014 sahen laut IHK-Unternehmensbarometer 61 Prozent der Betriebe in punkto Sicherheit der IT-Infrastruktur einen vordringlichen Qualifizierungsbedarf. Doch boten 2015 nur fünf von 64 großen Universitäten, in denen Informatik gelehrt wird, einen Studiengang für IT- und Cybersicherheit an. Damit nicht genug: Nach einer Studie von Frost & Sullivan werden bis 2020 weltweit 1,5 Millionen Fachkräfte im Sicherheitssektor fehlen.

Die Lösung: Lernlabor Cybersicherheit für die Sicherheitsexperten von morgen

Um im Wettlauf mit den Cyberkriminellen nicht ins Hintertreffen zu geraten, müssen Fach- und Führungskräfte ihnen in Kenntnissen und Fähigkeiten stets einen Schritt voraus sein. Die Fraunhofer-Gesellschaft und ausgewählte Fachhochschulen reagieren auf diesen Bedarf und haben ein modulares, berufsbegleitendes Weiterbildungskonzept für IT-Sicherheit entwickelt: Dafür wurde der Kooperationsverbund Lernlabor Cybersicherheit geschaffen, der in den nächsten Jahren mit jeweils sechs Millionen Euro vom Bundesministerium für Forschung und Bildung gefördert wird.

Das Konzept: Kollaboration mit Fachhochschulen für aktuellstes Forschungswissen

Die Kooperation von Fraunhofer-Instituten und Fachhochschulen sorgt dafür, dass neueste oder absehbare Forschungserkenntnisse schnell in die Seminarangebote einfließen und aktuelles Fachwissen aus erster Hand weitergegeben wird. In modernen Laboren, in denen sich reale Bedrohungsszenarien nachstellen lassen, können die Teilnehmer das neue Wissen direkt anwenden und sich praxisnah in folgenden Themenfeldern qualifizieren:

- Industrielle Produktion/Industrie 4.0
- Kritische Infrastrukturen/Anwendungsfall Energie- und Wasserinfrastrukturen
- Hochsicherheit und Emergency Response
- Internetsicherheit und IT-Forensik
- Qualität softwarebasierter Systeme und Zertifizierung
- Embedded Systems, Mobile Security und Internet of Things

Das Erfolgsrezept: Kompetenzaufbau, der die Bedürfnisse erfüllt

Kompakte Veranstaltungsformate erlauben eine berufsbegleitende Qualifikation, ohne Ressourcen über längere Zeiträume zu binden. Und die flexibel kombinierbaren Module vermitteln IT-Sicherheit adressatengerecht für unterschiedliche Berufsrollen. Die Fraunhofer Academy entwickelt dabei bedarfsorientiert das Angebot und sorgt für ein durchgängiges Qualitätsmanagement.

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

MIT SICHERHEIT INTELLIGENT DIGITAL VERNETZT

Zur Sicherung der Software-Qualität gehören Maßnahmen und Techniken im Vorfeld der Software-Entwicklung (Secure Design), im Entwicklungsprozess und beim Software-Test mit der speziellen Ausrichtung auf Produkt-Zertifizierung. Dazu zählen aber auch Prozeduren und Maßnahmen zur nachträglichen Evaluierung und Zertifizierung von Software. Anwendung finden diese Themen sowohl generell in Informations- und Kommunikationstechnologien, aber auch branchenspezifisch in der vernetzten öffentlichen und privaten Sicherheit sowie in öffentlicher IT bei Behörden, Verwaltung und Unternehmen.

Die Weiterbildung richtet sich an Entscheider, Product Owner, Projektleiter, Software-Entwickler und -Tester, Qualitätssicherer, sowie IT-Sicherheitsbeauftragte, die in Zertifizierungsprozesse involviert oder daran beteiligt sind.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/softwarequalitaet

BETEILIGTE EINRICHTUNGEN

- Fraunhofer FOKUS
- Hochschule für Technik und Wirtschaft Berlin
- Technische Hochschule Brandenburg

THEMEN-SCHWERPUNKTE

- Secure Software Engineering
- Security Testing
- Quality Management & Product Certification
- Sichere E-Government-Lösungen
- Sichere Public-Safety-Lösungen

SCHULUNGEN 2017 | 18

Management

Strategische Fragen der IT-Sicherheit und ihre Auswirkungen auf Public-Safety-Lösungen | Bedrohungen öffentlicher und kritischer Infrastrukturen kennenlernen, Auswirkungen des IT-Sicherheitsgesetzes und EU-Datenschutzgrundverordnung verstehen und Strategien für die IT-Sicherheit in der Organisation entwickeln — 5.10.2018 Berlin

Vertrauen durch Produktzertifizierung | Vertrauen potenzieller Kunden in die Sicherheit ihrer IT-Produkte steigern: Überblick über gängige Zertifizierungen im IT-Sektor; Vorteile, Nutzen, Risiken und Aufwand einer Zertifizierung abzuschätzen und bewerten — 4.12.2017 8.3.2018 Berlin

Fachkräfte und Anwender

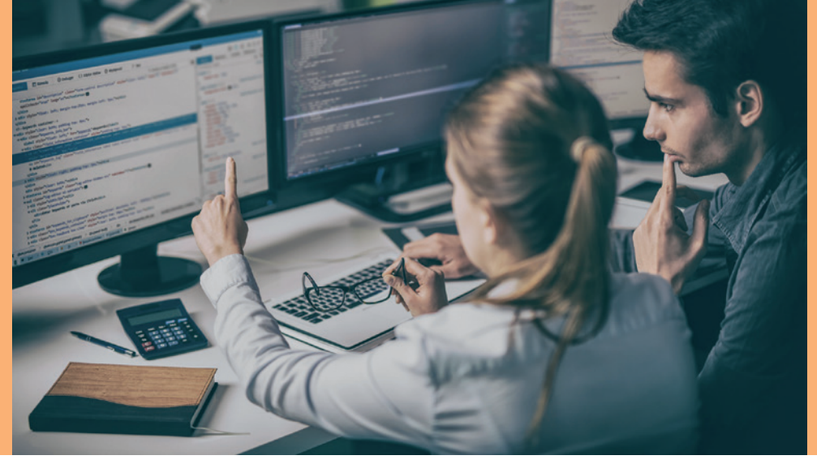
Grundlagen der IT-Sicherheit für Public-Safety-Infrastrukturen | Schutzbedarf öffentlicher und kritischer Infrastrukturen kennenlernen und Maßnahmen entsprechend den Anforderungen des IT-Sicherheitsgesetzes sowie der EU-Datenschutzgrundverordnung anwenden — 25.–26.1. | 20.–21.9.2018 Berlin

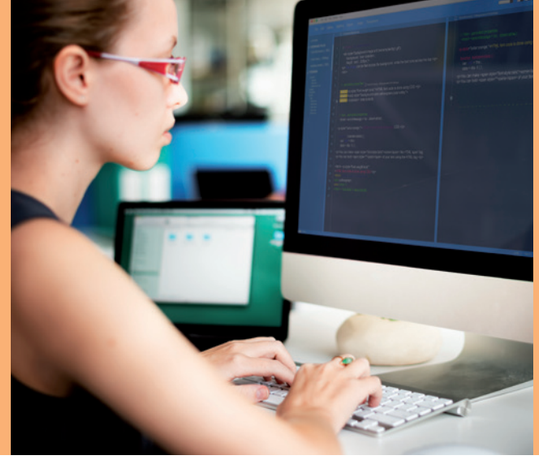
IT-Sicherheit für Public-Safety-Anwendungen | Entwicklung, Betrieb und Management von kritischen IT-Systemen: spezifische Anforderungen an IT-Systeme kennenlernen und spezifische Software-Engineering-Methoden im Entwicklungsprozess umsetzen, um sichere IT-Produkte herzustellen — 20.–22.6. | 7.–9.11.2018 Berlin

Secure Software Engineering | Prozesse und Methoden der Entwicklung sicherer Software verstehen: Überblick über Grundlagen der sicheren Softwareentwicklung und Motive und Methoden von Angreifern — 15.–17.1. | 14.–16.3. Brandenburg 21.–23.2. | 11.–14.5. Berlin

Sichere E-Government-Infrastrukturen | Überblick über die Grundlagen des BSI-Grundschutzes und Standards der IT-Sicherheit: ein Sicherheitskonzept nach BSI-Grundschutz lesen, verstehen sowie daraus Konsequenzen für die eigene Arbeit ableiten — 6.–7.2. | 24.–25.4.2018 Berlin

Sicherheitszertifizierung von Produkten: Überblick, Mehrwert, erste Schritte | Überblick über das deutsche Zertifizierungsschema erhalten, Kernkonzepte der Common Criteria (CC) verstehen, Ablauf einer Zertifizierung kennen, Anwendbarkeit der CC auf eigenes Produktportfolio bewerten sowie selbst eine CC-Zertifizierung initiieren — 25.–26.4.2018 Berlin





15.–17.1.2018 | 14.–16.3.2018
21.–23.2.2018 | 11.–14.5.2018

SECURE SOFTWARE ENGINEERING

Ganzheitliche Absicherung der Software-Entwicklung

Die Herausforderung: Softwaresysteme vor Angriffen schützen

IT-Systeme steuern heute alle zentralen und oft sicherheitskritischen Funktionen in städtischen Infrastrukturen, Autos, Bahnen, Fabriken oder Flugzeugen. Dies bedeutet ein enormes Bedrohungspotenzial in allen Arten von Anwendungen und Applikationen. Damit diese jederzeit funktionieren und vor Angriffen geschützt sind, muss die Systemqualität durchgehend gewährleistet werden. Hierfür ist es nötig, den gesamten Softwareentwicklungsprozess abzusichern und die Qualität stetig zu optimieren.

Die Lösung: Qualität und Sicherheit in der Softwareentwicklung herstellen

Für eine ganzheitliche Absicherung und Verbesserung der Qualität softwarebasierter Systeme und das Erkennen von Sicherheitslücken sind alle Software-Verantwortlichen gefragt: sowohl Architekten als auch Planer und Entwickler. Dafür müssen sie die Perspektive potenzieller Angreifer, ihre Motive und Methoden, aber auch die Sicht der Kunden kennen und berücksichtigen. Dieser Perspektivenwechsel bildet ein zentrales Element des Seminars »Secure Software Engineering«. Neben Motivation und Grundlagen der sicheren Softwareentwicklung liegt ein weiterer Schwerpunkt auf Secure Design, Coding sowie Software Security Tests. Darüber hinaus werden ein Ausblick in alle sicherheitsrelevanten Tasks des Lebenszyklus der Software gegeben sowie die unterschiedlichen Herausforderungen in verschiedenen Entwicklungsmethoden – etwa Agile oder Wasserfall-Entwicklung sowie die Integration in DevOps diskutiert.

Die Inhalte: Entwicklung, Testen und Warten von sicherer Software

Grundlagen sicherer Software
- Angreifer: Typ, Potenzial, Motivation
- Schutzziele: Unternehmenswerte, Compliance

Entwicklungsmethoden sicherer Software
Bedrohungsmodellierung
- Angriffsvektoren
- Risikoanalyse
- Maßnahmen
- Controls (Wirksamkeit)

Sicherer Software-Entwurf und Programmierung
- Schritte und Möglichkeiten für eine sichere Software-Architektur
- Vorgehen und Wege für sicheres Programmieren

Security Testing
- Besonderheiten von Sicherheitstests
- Penetrationtests

Wartung sicherer Software
- Response-Prozesse
- Security Incidents Handling (CERT)
- Kommunikationsstrategien

Die Lernziele: Sichere Software umsetzen

Die Teilnehmenden verstehen Methoden und Techniken, um sichere Software zu entwerfen und in eigenen Projekten zu implementieren.

Die Zielgruppe: Alle Software-Verantwortlichen

Software-Architekten, Software-Entwickler, Software-Planer

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… Angreifer und deren Motivation klassifizieren.
… Bedrohungen gegenüber der Software sowie der Entwicklung identifizieren.
… Risiken gegenüber der Software priorisieren und adressieren.
… Maßnahmen von den Risiken ableiten, bewerten und implementieren.

Dieses Seminar bietet Ihnen …
… einen passgenauen Mix aus Theorie und Praxis.
… viele Beispiele und anwendbares Wissen.
… Übungen zum vermittelten Inhalt an realitätsnahen Fallbeispielen, damit Sie Ihr Wissen direkt im Unternehmen einsetzen können.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/cybersicherheit-sse

INFORMATIONEN IM ÜBERBLICK

Kurs: Secure Software Engineering

Empfohlen sind:
- Erfahrung in der Software-Entwicklung sowie deren Methoden
- Kenntnisse zu Technologien wie Tomcat und Datenbanken
- Grundkenntnisse zur Programmiersprache Java

Dauer: 3 Tage in Präsenz

Kurssprache: Deutsch

Teilnehmerzahl: max. 12 Personen

Veranstaltungsort: Brandenburg an der Havel; Berlin

Termine: 15.–17.1. | 14.–16.3. Brandenburg
21.–23.2. | 11.–14.5. Berlin

Kosten: 1800 €

Veranstaltet durch: Technische Hochschule Brandenburg
University of Applied Sciences
Fachbereich Wirtschaft

UNSERE REFERENTEN

Marcel Niefindt
Doktorrand im Bereich Secure Software Engineering der TH Brandenburg sowie Manager Cyber Risk & Software Quality bei Deloitte

Sandro Hartenstein
Dozent für Secure System LifeCycle Management an der TH Brandenburg sowie freier IT-Security Analyst und Berater

ANSPRECHPARTNER

Marcel Niefindt | TH Brandenburg
marcel.niefindt@th-brandenburg.de

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

OHNE STROM UND WASSER? IT-SICHERHEIT FÜR KRITIS

Zu den Betreibern kritischer Infrastrukturen (KRITIS) gehören alle Versorgungsunternehmen für Strom, Gas, Wasser und Abwasser. Die betriebenen Verteilnetze und die darin eingesetzten Komponenten und Netzwerke nutzen spezifische Netzwerkprotokolle und sind aufgrund ihres Einsatzes besonders für Angriffe exponiert.

Das Themenfeld »Kritische Infrastrukturen/Anwendungsfall Energie- und Wasserinfrastrukturen« umfasst Techniken des »Smart Grid« sowie äquivalente Strukturen für die anderen Infrastrukturen. Betrachtet werden neben Schwachstellen bei Planung und Betrieb insbesondere Risikobewertung und -strategien vorbeugender Maßnahmen für Cyberangriffe.

Die Weiterbildung richtet sich vor allem an Planer und Betreiber von Versorgungsnetzen, aber auch an Akteure im Energiemarkt sowie Hersteller von Komponenten und Lösungen. Ein Schwerpunkt liegt hier bei Netzplanung und Netzsteuerung.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/kritis

BETEILIGTE EINRICHTUNGEN

- **Fraunhofer IOSB-AST**
- **Fraunhofer IDMT**
- **Hochschule Zittau/ Görlitz**

THEMEN-SCHWERPUNKTE

- **Gefährdungs-, Risiko- und Schwachstellenanalyse aus Versorgungssystem- und IKT-Sicht**
- **Gegenmaßnahmen für Bedrohungs- und Angriffsszenarien**

SCHULUNGEN 2017 | 18

Management

IT-Sicherheit im Unternehmen | Möglichkeiten von Cyberangriffen und Schutzmechanismen für das Unternehmen erfahren: Schwachstellen des eigenen Unternehmens identifizieren und Angriffe aktiv verhindern, gesetzliche Rahmen und Maßnahmen einschätzen, Mitarbeiter sensibilisieren und informierte Entscheidungen für prozessorientierte Maßnahmen treffen	30.11.2017 Ilmenau 17.4. | 16.5.2018 Ilmenau | Görlitz
IT-Sicherheit für Kritische Infrastrukturen | IT-Sicherheitsgefahren und Gegenmaßnahmen kennen: Angriffsbeispiele richtig beurteilen, Ablauf von Angriffen nachvollziehen und Angriffsversuche abwehren, typische strukturelle Schwachstellen erkennen sowie gesetzlichen Rahmen für das eigene Unternehmen beurteilen	24.10.2017 Ilmenau 23.1. | 6.6.2018 Ilmenau | Görlitz

Management und Fachkräfte

IT-Sicherheitsmanagement für Kritische Infrastrukturen | IT-Sicherheit als Prozess etablieren: Werkzeuge zur Einführung eines IT-Sicherheitsmanagementsystems, Risiken und Schwachstellen in Unternehmensprozessen identifizieren und bewerten, etablierte Standards abgrenzen und richtig bewerten sowie das Unternehmen auf eine Zertifizierungen vorbereiten	9.–10.11. | 5.–6.12.2017 Görlitz | Ilmenau 7.–8.3. | 20.–21.6.2018 Görlitz | Ilmenau

IT-SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

Welche Gefahren existieren, wie kann man ihnen begegnen?

Die Herausforderung: Kritische Infrastrukturen sind immer häufiger Ziel von Cyberattacken

Durch die zunehmende Digitalisierung erhöht sich die Anfälligkeit kritischer Infrastrukturen gegenüber Cyberattacken, während den Angreifern immer leistungsfähigere Werkzeuge und Methoden zur Verfügung stehen. Gleichzeitig steigt die Abhängigkeit von automatisierten Prozessen und IT-Systemen immer weiter an. Aufgrund dieser Bedrohungssituation hat der Gesetzgeber umfangreiche Gesetzesänderungen durchgeführt, welche die Betreiber Kritischer Infrastrukturen in die Pflicht nehmen. Neben den technischen Komponenten müssen auch die Mitarbeiter entsprechend geschult werden, da diese derzeit die am häufigsten ausgenutzte Schwachstelle von Cyberangriffen darstellen.

Die Lösung: Wissen, welche Gefahren drohen, und wie man ihnen begegnen kann

Anhand vieler ausführlich analysierter Angriffsbeispiele auf verschiedene kritische Infrastrukturen werden Ihnen die derzeitige Bedrohungslage sowie häufige Schwachstellen nähergebracht. Weiterhin wird die aktuelle und zukünftige Gesetzeslage für Unternehmen Kritischer Infrastrukturen beleuchtet. Sie lernen, Gefährdungen und Risiken einzuschätzen und häufige Versäumnisse zu vermeiden. Verschiedene branchenspezifische Standards und Normen werden Ihnen vorgestellt und Handlungsempfehlungen dargestellt. Weiterhin werden Sie selbst für die existierenden Gefahren sowohl im Alltag als auch beispielsweise unterwegs auf Dienstreisen sensibilisiert und in die Lage versetzt, dieses Wissen an Ihre Mitarbeiter weiterzugeben.

Die Inhalte

- Welche Angriffe auf Kritische Infrastrukturen gab es bereits, und wie liefen diese ab?
- Welche Auswirkungen hatten diese Angriffe?
- Wie hätten die Angriffe verhindert werden können?
- Welche Gesetze gelten für Kritische Infrastrukturen?
- Welche Änderungen erwarten mich mit der EUDSGVO?
- Welche Standards und Normen existieren bereits, wie können sie umgesetzt werden?
- Welcher Aufwand muss, welcher sollte betrieben werden?
- Wie kann ich mich selbst vor Cyberangriffen schützen?
- Wie sensibilisiere ich meine Mitarbeiter nachhaltig?

Die Lernziele

- Kennen der rechtlichen Rahmenbedingungen und Verstehen der resultierenden Auswirkungen auf das Unternehmen
- Kennen verschiedener Angriffsbeispiele und -szenarien
- Verstehen des typischen Angriffsablaufs
- Standards und Normen voneinander abgrenzen können
- Eigenes Handeln sicherer gestalten können
- Mitarbeiter für Themen der Cybersicherheit sensibilisieren können

Die Zielgruppe

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

24.10.2017
23.1.2018 | 6.6.2018

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… viele verschiedene Angriffe und deren Ablauf nachvollziehen sowie Angriffsversuche abwehren.
… typische strukturelle Schwachstellen benennen.
… den gesetzlichen Rahmen für Ihr Unternehmen beurteilen.
… Maßnahmen einleiten, welche den Gesetzen sowie aktuellen Standards entsprechen.

Dieses Seminar bietet Ihnen …
… Fachwissen über häufige Schwachstellen und Einfallstore.
… einen Überblick über die derzeitige KRITIS-Gesetzeslage.
… eine Einführung in vorhandene Standards und Normen.
… IT-Security-Awareness-Maßnahmen.

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

INFORMATIONEN IM ÜBERBLICK

Kurs: IT-Sicherheit für Kritische Infrastrukturen

Voraussetzungen: Keine

Dauer: 1 Tag in Präsenz

Kurssprache: Deutsch

Teilnehmerzahl: 8–22 Personen

Veranstaltungsort:
Ilmenau bzw. Görlitz

Termine: 24.10.2017 | 23.1.2018, Ilmenau; 6.6.2018 Görlitz

Kosten: 600 €

Veranstaltet durch:

Hochschule Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES

Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

UNSERE REFERENTEN

Prof. Dr.-Ing. Jörg Lässig
Professor für die Entwicklung von Unternehmensanwendungen an der Hochschule Zittau/Görlitz

Prof. Dr. Peter Bretschneider
Stellvertretender Leiter des Fraunhofer IOSB-AST und Leiter der Abteilung Energie

ANSPRECHPARTNER

Prof. Jörg Lässig | Fraunhofer IOSB-AST
Telefon +49 3581 7925354
joerg.laessig@iosb-ast.fraunhofer.de

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

IM NETZ? – ABER SICHER!

Das Internet stellt die wichtigste Infrastruktur für die Digitalisierung dar und bildet als solche die Basis vieler innovativer Anwendungen. In diesem Zusammenhang sind IT-Sicherheitsfragen von zentraler Bedeutung, da sich über die Vernetzung und die damit einhergehende Öffnung von IT-Systemen immer wieder Ansatzpunkte für Angriffe ergeben. Deshalb besteht hier ein umfangreicher Bedarf zur Verbesserung der IT-Sicherheit: zum einen im Bereich Internetsicherheit, also allen relevanten Internet-Technologien mit ihren Protokollen und den zum Betrieb von Netzwerken erforderlichen Diensten; zum anderen im Bereich IT-Forensik, was die Behandlung von Vorgehensweisen und Werkzeugen zur sicheren Identifikation und beweissicheren Extraktion von Spuren einschließt.

Die Weiterbildungen IT-Forensik richten sich an Anwender in unterschiedlichen Anwendungsbranchen und Betreiber von IT-basierten Infrastrukturen; im Bereich Internetsicherheit an Software-Entwickler, Netzwerkplaner und Netzwerkadministratoren sowie Entwickler von Technologien und Diensten im Themenbereich »Automotive«.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/it-forensik

BETEILIGTE EINRICHTUNGEN

- **Fraunhofer SIT**
- **Hochschule Mittweida**
- **Hochschule Darmstadt**

THEMEN-SCHWERPUNKTE

- **IT-forensische Erfassung von Spuren**
- **IT-forensische Analyse**
- **Multimediaforensik**
- **Open Source Intelligence**
- **Big-Data-Analysen/ Textmining**
- **Automotive Security Testing/Solutions**

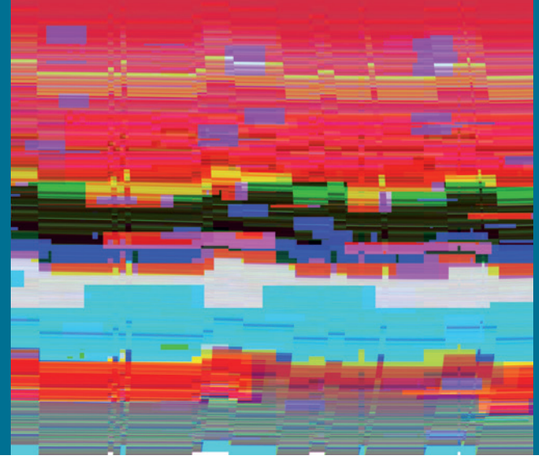
SCHULUNGEN 2018

Fachkräfte und Anwender

Praxis Automotive Security Testing | Durchführung von IT-Sicherheitsanalysen im Automobilbereich: aktuelle praktische Techniken zur Analyse sicherheitsrelevanter Software, Hardwarekomponenten und Protokolle in modernen Fahrzeugen	5.+6.3. | 7.+8.5. | 9.+10.7.2018 Darmstadt
IT-Forensik für Multimediadaten | Moderne Methoden zur forensischen Analyse von digitalen Multimediadaten praxisnah erlernen: Erfassung, Sichtung und Analyse unsichtbarer Spuren sowie datenschutzrechtlich zulässige Vorgehensweisen	13.–15.3. | 23.–25.5. | 3.–5.7.2018 Darmstadt
Datenschutz für IT-Forensik | Datenschutzrechtlich zulässigen Rahmen für IT-Forensiker verstehen, eigene Vorgehensweisen richtig einschätzen und Maßnahmen für datenschutzkonformes Arbeiten ergreifen	13.3. | 23.5. | 3.7.2018 Darmstadt
Schwachstelle Mensch: Social Engineering als Grundlage für Human-Hacking im Unternehmensalltag | Mit Open-Source-Werkzeugen personenspezifische Informationen aus sozialen Netzwerken aggregieren und auswerten	Auf Anfrage Mittweida
Einführung in die Open-Source-Analytik digitaler forensischer Spuren | Forensische Datenanalyse im Betriebssystem Linux sowie mit Open-Source-Werkzeugen, Erstellen von Shell-Skripten	Auf Anfrage Mittweida
Der Datenanalyst – Umgang mit BigData/Textmining im forensischen Kontext | Mit Open-Source-Werkzeugen (z. B. Pentaho, Rapidminer, Talend und Gate) einfache Textmining-Aufgaben realisieren	Auf Anfrage Mittweida
OSINT im Rahmen des digitalen investigativen Journalismus | Open Source Intelligence zur Informationsgewinnung nutzen: mit Betriebssystem Kali-Linux und Open-Source-Werkzeugen	Auf Anfrage Mittweida

Behörden

OSINT für Behörden und kriminalistische Institutionen | Open Source Intelligence für fallspezifische Untersuchungen: Betriebssystem Kali-Linux und Open-Source-Werkzeuge beherrschen und Prozessketten des Informationsgathering verstehen	Auf Anfrage Mittweida



13.–15.3.2018 | 23.–25.5.2018
3.–5.7.2018

IT-FORENSIK FÜR MULTIMEDIADATEN

Spuren in digitalen Bildern, Video- und Audiodaten finden und auswerten

Die Herausforderung: Spuren aus Multimediadaten effektiv analysieren und interpretieren

Digitale Multimediadaten können bei der Aufklärung von Straftaten oder bei Rechtsstreitigkeiten wertvolle Indizien liefern – ein Bild sagt oftmals mehr als tausend Worte! Eine Herausforderung ist dabei das effiziente Sichten großer Datenbestände an Mediendaten, wie sie bei forensischen Untersuchungen häufig anfallen. Zudem enthalten Mediendaten oftmals auch viele unsichtbare Spuren mit Hinweisen auf Ursprung, Beweiskraft oder gar Manipulationen der Medien sowie »versteckte« steganographische Botschaften im Medium. Als IT-Forensiker kann man diese Spuren auswerten, wenn man die Besonderheiten der Multimedia-Datenformate kennt und die hierfür speziellen Methoden für das Erfassen und Analysieren der Daten beherrscht.

Die Lösung: Moderne Methoden zur forensischen Analyse von digitalen Multimediadaten praxisnah erlernen

Sie werden zuerst in die Grundlagen Multimedia-Formate und ihre Besonderheiten eingeführt. Anschließend werden spezielle Methoden der Datenerfassung behandelt, etwa Metadaten-Erfassung oder Filecarving »gelöschter« Mediendaten. Dann werden Methoden behandelt, welche Sie bei der Sichtung großer Bildbestände unterstützen können, um eine mühsame manuelle Spurensuche zu erleichtern. Anschließend werden Ihnen moderne Analyseverfahren für unsichtbare Spuren in Mediendaten vermittelt. Hierzu gehören das nachträgliche Erkennen von Nachbearbeitungen und Datenmanipulationen oder das Identifizieren der Datenquelle. Schließlich werden auch Methoden der Stego-Analyse zum Aufspüren steganographisch »versteckter Botschaften« in scheinbar unverdächtigem Bildmaterial vermittelt.

Die Inhalte

Grundlagen: Motivation, Herausforderungen und Anwendungen; Basiswissen zu digitalen Bilddaten, Video, Audio; Besonderheiten zum Datenschutz
Datenerfassung: Untersuchung von Speichermedien; Mediensuche im Internet; Datenrekonstruktion per Filecarving
Effiziente Sichtung: Identifizierungsverfahren für Mediendaten; Nacktheitserkennung
Analyse: Metadaten-Untersuchung; Erkennen von Manipulationen und Datenquellen; Steganalyse; Anti-Forensik
Praktische Übungen: Bild-Metadaten auf Smartphones; Bilderkennung durch robuste Hash-Methoden; Erkennen von Bildmanipulationen; Detektieren von Stegonachrichten

Die Lernziele

- Bisherige forensische Fach- und Methodenkenntnisse auf die Analyse von Multimediadaten ausweiten
- Theoretische Grundlagen der wichtigsten Mediendateiformate kennenlernen
- Wichtige Verfahren zur Erfassung, Sichtung und Analyse der unsichtbaren Spuren innerhalb von Mediendaten nachvollziehen und anwenden können
- Datenschutzrechtlich zulässiges Vorgehen bei Ihrer Arbeit richtig einschätzen

Die Zielgruppe

IT-Forensiker in Unternehmen und Behörden, die ihre Fach- und Methodenkenntnisse auf den Bereich Multimedaten ausweiten möchten

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… verdächtige Medieninhalte aus Internetquellen oder Speichermedien erfassen.
… die Echtheit und die Quelle multimedialer Beweisstücke beurteilen.
… Verfahren zum Sichten großer Bilddatenmengen verstehen
… steganographische Botschaften ausfindig machen.
… Ihre Arbeiten datenschutzkonform durchführen.

Dieses Seminar bietet Ihnen …
… Anwendung moderner Methoden und aktueller Forschungsergebnisse auf praxisnahe Problemstellungen.
… praktische Forensik-Übungen zur Einübung bewährter Vorgehensweisen für Ihre eigenen Ermittlungen.
… Austausch und Vernetzung mit Experten und Anwendern der Multimedia-Forensik.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/it-forensik-multimedia

INFORMATIONEN IM ÜBERBLICK

Kurs: IT-Forensik für Multimediadaten

Voraussetzungen: Kenntnis der Methoden der forensischen Arbeitsweise, praktische Erfahrung in forensischer Untersuchung von Datenträgern, Grundkenntnisse des Datenschutzes in der Forensik (bei Bedarf wird Modul »Datenschutz für die IT-Forensik« empfohlen), Grundkenntnisse zu Kommandozeile/ Konsole unter Windows und Linux

Dauer: 2,5 Tage in Präsenz

Kurssprache: Deutsch

Teilnehmerzahl: max. 16 Personen

Veranstaltungsort: Darmstadt

Termine: 13.–15.3.2018 | 23.–25.5.2018 | 3.–5.7.2018

Kosten: 1500 €

Veranstaltet durch: Fraunhofer SIT

WEITERE SEMINARE

Falls Sie erst die rechtlichen Grundlagen kennenlernen wollen, sehen Sie sich unser Kurz-Modul »Datenschutz für die IT-Forensik« an:
www.academy.fraunhofer.de/datenschutz-it-forensik

UNSERE REFERENTEN

York Yannikos | Sascha Zmudzinski
unter der Leitung von Prof. Dr. Martin Steinebach, Media Security and IT Forensics am Frauhofer SIT

ANSPRECHPARTNER

Dr. Sascha Zmudzinski
Fraunhofer SIT
sascha.zmudzinski@sit.fraunhofer.de

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

MIT SICHERHEITSKOMPETENZ IN DIE DIGITALISIERUNG

Eingebettete Systeme (embedded systems), Sensoren und Aktoren sind in einer Vielzahl sicherheitskritischer Szenarien im Einsatz. Und auch mobile Endgeräte werden immer mehr in diesen Umgebungen verwendet, sodass zunehmend die Kompetenzen der verantwortlichen Fachkräfte gefragt sind.

Das Themenfeld »Embedded Systems, Mobile Security und Internet of Things« umfasst deshalb den gesamten Entwicklungsprozess vom Design bis zum Test und der Zertifizierung von Komponenten. Ein Schwerpunkt liegt dabei bei Security- und Privacy-Anforderungen im Design-Prozess, Sicherheitstechniken mit spezifischer Hardware-Unterstützung, Sicherheitsmaßnahmen für Hardware und Software-Implementierung von Sicherheitsfunktionen eingebetteter Systeme und dem sicheren Zusammenwirken von Komponenten in komplexen Szenarien.

Die Weiterbildung richtet sich vorwiegend an Entwicklungs-Ingenieure, Software-Designer und Tester über alle Branchen hinweg.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/embedded-systems

BETEILIGTE EINRICHTUNGEN

- **Fraunhofer AISEC**
- **Fraunhofer IIS**
- **Ostbayerische Technische Hochschule Amberg-Weiden**
- **Hochschule Aalen**

THEMEN-SCHWERPUNKTE

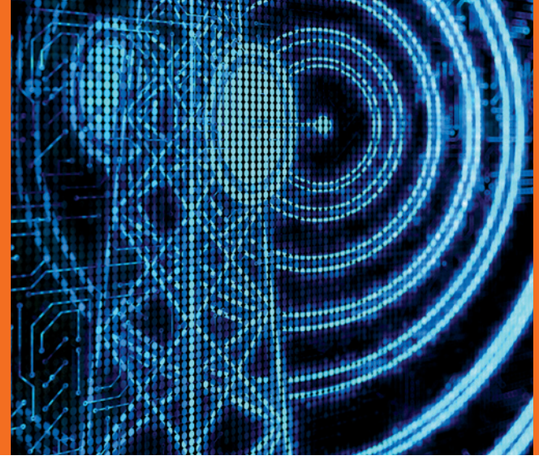
- **Sichere Softwareentwicklung**
- **Embedded OS und Linux Security**
- **Trusted Computing und TPM 2.0**
- **Secure Elements**
- **Kryptographie für das Internet of Things**

Management

IT-Sicherheit im Unternehmen | Überblick über aktuelle Bedrohungen und Aufgaben der Unternehmensführung zur IT-Sicherheit	16.11.2017 | 15.1. | 14.5. | 19.7.2018 Garching | Garching | Garching | Aalen
Top Cyber Security Trends | Aktuelle Entwicklungen im Bereich IT-Sicherheit, neue Technologien sowie Chancen und Möglichkeiten kennenlernen	16.1. | 11.6.2018 Garching bei München
Softwaresicherheit im Entwicklungsprozess | Aktuelle Vorgehensmodelle, Methoden und Werkzeuge für systematische Entwicklung sicherer Software bewerten	19.–20.2. | 26.–27.2. | 23.–24.7.2018 Aalen | Garching | Aalen
Sichere hardwaregebundene Identitäten | Einsatzmöglichkeiten von Physical Unclonable Functions (PUFs) richtig einschätzen	10.4.2018 Garching bei München
Blockchain für Manager | Blockchain-Technologie verstehen und Nutzungsszenarien für das eigene Unternehmen kennenlernen	14.6.2018 Garching bei München
Sichere eingebettete Systeme mit FPGAs | Schutzmechanismen in FPGAs verwenden, um sichere Embedded Systeme zu bauen	18.4. | 12.9.2018 Garching bei München

Fachkräfte und Anwender

Hacking: Pentesting | IT-Sicherheit aus der Perspektive des Angreifers prüfen und die eigenen Schwachstellen mit Penetrationstests aufdecken	15.–17.5. | 10.–12.7. | 27.–29.11.2018 Weiden
Digitale Identitäten | Identitätsmanagement verstehen und firmenübergreifende Systemzugriffe sicher machen	12.+13.4. | 7.+8.6. | 30.+31.7.2018 Garching bei München
IT-Sicherheit in der Fahrzeugkommunikation | Schutz der Privatsphäre und Schutz vor Manipulation bei fahrzeugexterner und -interner Kommunikation	20.2. | 17.4. | 11.9.2018 Garching bei München
Mobile Application Security | Überblick über das Sicherheitsmodell von Android und iOS, Analyseverfahren sowie Tools zur Analyse	24.–25.4. | 5.–6.6.2018 Garching bei München
Hacking: Binary | Grenzen vorhandener Schutzmechanismen erkennen und Exploits zum Aufzeigen von Schwachstellen entwickeln	24.–26.4. | 24.–26.7. | 11.–13.12.2018 Weiden | Garching | Garching
Maschinelles Lernen für mehr Sicherheit | Grundlagen maschinelles Lernen, Daten Mining und Modellierungsmethoden zur Anomalienerkennung	20.4. | 6.7.2018 Garching bei München
Blockchain | Hintergründe der Blockchain-Konzepte verstehen und Smart Contracts programmieren	27.2.–1.3. | 21.–23.11.2018 Weiden
Netzwerksicherheit | Maßnahmen zur Sicherungen von Computernetzwerken und frühzeitiges Erkennen von Schwachstellen	1.2. | 12.3. | 3.7.2018 Aalen | Garching | Aalen
IoT Security | Überblick über das Internet of Things und dessen besondere Risiken; gängige Kommunikationstechnologien im IoT absichern	24.1. | 21.3. | 25.6.2018 Aalen | Aalen | Garching
IT-Sicherheit in drahtlosen Kommunikationssystemen | Überblick über gängige Technologien, Risiken und Schutzmaßnahmen (am Beispiel von WLAN)	22.–23.11.2017 | 19.–20.4. | 11.–12.10.2018 Nürnberg
Mobile Endgeräte | Verschiedene Mobile Device Management Tools einsetzen und konfigurieren	25.4. | 20.6.2018 Garching | Aalen



22.–23.11.2017
19.–20.4.2018 | 11.–12.10.2018

IT-SICHERHEIT DRAHTLOSER KOMMUNIKATIONSSYSTEME

Ein Überblick über gängige Technologien, Risiken und Schutzmaßnahmen

Die Herausforderung: Drahtlose Vernetzung moderner Kommunikationssysteme weist gefährliche Sicherheitslücken auf

Mittlerweile sind in fast jedem Bereich des täglichen Lebens moderne Kommunikationssysteme im Einsatz: Wohnungen, Büroräume, Infrastrukturen, Kaufhäuser und Produktionsunternehmen. Im Internet of Things (IoT) werden bis 2020 schätzungsweise 50 Milliarden Endgeräte in unserem Alltag intergiert sein. Kommunikationssysteme entwickeln sich daher immer mehr zum zentralen Nervensystem für Anwendungsfelder wie Industrie 4.0 und Smart Home. Und besonders drahtlose Kommunikationssysteme wie WLAN finden im industriellen Bereich breite Anwendung und sind bei schlechter Konfiguration ein leichtes Ziel für Angriffe durch Kriminelle, Spione und Terroristen. So können z. B. Produktionsdaten abgehört, Prozesse gestört oder diese sogar manipuliert werden.

Die Lösung: Aufbau eines Sicherheitsbewusstseins für schützende Gegenmaßnahmen

In diesem Seminar erhalten die Teilnehmenden einen umfangreichen Überblick über gängige drahtlose Kommunikationstechnologien im IoT. Am Beispiel von WLAN werden in erster Linie die damit verbundenen potenziellen Sicherheitsrisiken und denkbaren Bedrohungsszenarien erörtert und durch ein Praxisbeispiel veranschaulicht. Nach der gemeinsamen Erarbeitung der Schutzziele werden mögliche Schutzmaßnahmen vorgestellt und diskutiert. Die Teilnehmenden verstehen das Spannungsfeld zwischen Erfüllung der Schutzziele (absolute Sicherheit) und der Anwendbarkeit in der Praxis und sollen somit ein Sicherheitsbewusstsein für ihre Anwendungen entwickeln.

Die Inhalte: Überblick über drahtlose Kommunikationstechnologien, deren Bedrohungen sowie mögliche Schutzmaßnahmen

- Überblick über drahtlose Kommunikationssysteme
- Bedrohungsszenarien und Risiken mit Labordemonstration
- Erarbeitung von Schutzzielen
- Vorstellung gängiger Schutzmaßnahmen
- Diskussion zu Security vs. Usability

Die Lernziele: Risikobewusstsein bei Anwendung und Betrieb drahtloser Kommunikationssysteme sowie Kenntnis über deren Absicherung

- Kenntnis der gängigen drahtlosen Kommunikationstechnologien, deren Anwendungen sowie deren Absicherung
- Wissen über Risiken und typische Bedrohungsszenarien drahtloser Kommunikationssysteme
- Entwicklung von Verständnis über Risiken drahtloser Kommunikationssysteme
- Verständnis der übergeordneten Schutzziele im Kontext der IT-Sicherheit
- Bewusstsein über den Zusammenhang zwischen Erfüllung der Schutzziele und Anwendbarkeit in der Praxis

Die Zielgruppe: Anwender und Betreiber drahtloser Kommunikationstechnologien

Administratoren, Tester, Betreiber oder Anwender, die in ihrer beruflichen Tätigkeit drahtlose Kommunikationsnetze konzipieren, aufbauen oder betreiben

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… Gefährdungen durch drahtlose Kommunikationstechnolgien richtig einschätzen.

Dieses Seminar bietet Ihnen …
… einen ausführlichen Überblick über die üblichen drahtlosen Kommunikationstechnologien.
… einen Einblick in potenzielle Sicherheitsrisiken und Schutzmaßnahmen.
… ein Sicherheitsbewusstsein für die praktische Umsetzbarkeit von Schutzzielen.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/drahtlose-kommunikationssysteme

INFORMATIONEN IM ÜBERBLICK

Kurs: IT-Sicherheit drahtloser Kommunikationssysteme

Voraussetzungen: Keine Vorkennnisse im Bereich IT-Sicherheit und Kommunikationstechnik notwendig. Mathematik-Kenntnisse über Schulniveau hinaus sind nicht erforderlich.

Dauer: 1,5 Tage in Präsenz

Kurssprache: Deutsch

Teilnehmerzahl: max. 16 Personen

Veranstaltungsort: Nürnberg

Termine: 22.–23.11.2017 | 19.–20.4.2018 | 11.–12.10.2018

Kosten: 900 €

Veranstaltet durch: Fraunhofer IIS

UNSERE REFERENTEN

Moritz Loske
Wissenschaftlicher Mitarbeiter am Fraunhofer IIS

Dominik Gertler
Wissenschaftlicher Mitarbeiter an der Ostbayerischen Technischen Hochschule (OTH) Amberg-Weiden

ANSPRECHPARTNER

Moritz Loske | Fraunhofer IIS
Telefon +49 911 58061-9316
moritz.loske@iis.fraunhofer.de

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

DIGITALISIERUNG IN DER PRODUKTION BRAUCHT IT-SICHERHEITSKOMPETENZ

Das Themenfeld »Industrielle Produktion/Industrie 4.0« umfasst Netzwerk- und Sicherheitstechniken für Automatisierungssysteme im Hinblick auf vernetzte Systeme, Internetanbindung und Cloud-Techniken für Automatisierungsaufgaben. Behandelt werden sowohl typische Schwachstellen in Design und Implementierung in eingebetteten Systemen und industriellen Komponenten (z. B. Industrie-Roboter) als auch neueste Entwicklungen im Bereich von Kommunikations-Protokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software für die zunehmend softwareintensiven Bereiche der industriellen Produktion.

Die Weiterbildung richtet sich sowohl an Planer und Betreiber von Automatisierungssystemen (Planungs-Ingenieure, Wartungstechniker) als auch an Entwickler von Automatisierungslösungen (Software-Designer, Programmierer). Zielgruppe sind auf Anwenderseite alle Branchen der produzierenden Industrie (z. B. Automobil, Chemie) sowie die Hersteller von Automatisierungslösungen.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/industrielle-produktion

BETEILIGTE EINRICHTUNGEN

– Fraunhofer IOSB
– Fraunhofer IOSB-INA
– Hochschule Ostwestfalen-Lippe

THEMEN-SCHWERPUNKTE

Netzwerk- und Sicherheitstechniken für
– Automatisierungssysteme
– Vernetzte Systeme
– Internetanbindungen
– Cloud-Techniken

SCHULUNGEN 2017 | 18

Management

Bedrohungslage für industrielle Produktionssysteme | Bewusstsein für Bedrohungslage der industriellen Produktionssysteme und den daraus resultierenden Handlungsbedarf erlangen sowie rechtlichen Rahmen und Grundzüge der benötigten IT-Sicherheitsprozesse kennenlernen
29.11.2017 Erkrath
23.1. | 17.4.2018 Karlsruhe

Fachkräfte und Anwender

Systemhärtung | Sichere Konfiguration von Betriebssystemen und Hardwarekomponenten umsetzen; sichere Softwareentwicklung verstehen und hardwarebasierte Sicherheitsmechanismen einsetzen
21.–23.3.2018 Lemgo

IT-Sicherheit in der Automatisierungstechnik | Sicherheitsaspekte bei der Transformation zu Industrie 4.0 kennen und Sicherheitskonzepte im eigenen Unternehmen richtig umsetzen; Methoden zur sicheren Industrie 4.0-Kommunikation anwenden, um Industrie 4.0-Anwendungsfälle wie Condition Monitoring, Plug & Work und Optimierung zu realisieren
21.–23.11.2017
13.–15.3.2018 Lemgo

Grundlagen der IT-Sicherheit für die Produktion | Produktionsanlagen und Automatisierungssysteme absichern; Grundlagen der Netzwerktechnik im Automatisierungsbereich sowie typische Angriffsflanken kennen und die entsprechenden Gegenmaßnahmen umsetzen
20.–22.2. | 22.–24.5.2018 Karlsruhe

21.–23.11.2017
13.–15.3.2018

IT-SICHERHEIT IN DER AUTOMATISIERUNGSTECHNIK

Auf dem Weg zur Industrie 4.0 – aber sicher!

Die Herausforderung: Sicherheitsaspekte bei der Transformation zu Industrie 4.0

Was bedeutet Industrie 4.0 für mein Unternehmen? Welche Chancen entstehen? Welche Risiken? Für produzierende Unternehmen im Mittelstand ist es notwendig, die Industrie 3.0 vollständig zu verstehen, bevor sie den Weg zur Industrie 4.0 beschreiten. Dabei stellt sich vor allem die Frage nach der Sicherheit. Unternehmen müssen im Zuge der digitalen Transformation ihre kritischen Systeme, Anlagen und Werte kennen, um geeignete Schutzmaßnahmen zu ergreifen.

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.

Die Inhalte: Automatisierungstechnik, Netzwerkanalyse und Schutzmechanismen

Schwerpunkt auf Lernen durch Anwenden: Die Inhalte werden durch praktische Übungen direkt ausprobiert und gefestigt; Verhältnis Praxis zu Theorie etwa 1:1.

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 und Profinet

Angriff und Absicherung
– Angriffsszenarien auf Automatisierungstechnik
– Absicherung von Netzwerkinfrastruktur
Praktische Übung: Angriffsszenarien, Firewall, Virtual Private Network (VPN)

Die Zielgruppe: Entwickler, Planer und Betreiber von Automatisierungstechnik

Das Seminar richtet sich an Mitarbeiterinnen und Mitarbeiter im Bereich von Entwicklung, Betrieb sowie Planung von industrieller Automatisierungstechnik und Personal mit IT-Hintergrund, das sich mit der industriellen Automatisierungstechnik vertraut machen möchte.

Die Lernziele: Sichere Kommunikations- und Automatisierungstechnik kennen und umsetzen

In diesem Seminar lernen Sie die aktuellen Automatisierungssysteme kennen – vom klassischen System bis zum cyberphysischen Produktionssystem im Sinne der Industrie 4.0. Sie wenden etablierte Methoden zur sicheren Industrie 4.0-Kommunikation mit OPC UA an, um Industrie 4.0-Anwendungsfälle wie Condition Monitoring, Plug & Work und Optimierung zu realisieren. Die erlernten Sicherheitskonzepte stärken und sensibilisieren Sie für sicherheitskritische Vorgänge und ermöglichen eine zielgerichtete aufbauende Fortbildung.

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
Termine: 21.–23.11.2017 | 13.–15.3.2018
Kosten: 1800 €

Veranstaltet durch:
Fraunhofer IOSB-INA
Hochschule Ostwestfalen-Lippe
University of Applied Sciences

UNSERE REFERENTEN

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

ANSPRECHPARTNER

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

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

PROTECT AND REACT!

Das Themenfeld »Hochsicherheit und Emergency Response« umfasst Techniken, Prozeduren und Strategien für den Hochsicherheitsbereich, insbesondere für den öffentlichen Geheimschutz und für Betreiber kritischer Infrastrukturen. Schwerpunkte sind Untersuchungen von Angriffstechniken und Schadsoftware. Als besonderer Angriffsvektor werden hier auch Firmware-Backdoors betrachtet. Weiterhin gehören Strategien und Prozeduren für Incident Response und IT-Forensik sowie Internet of Things, insbesondere Gebäudeautomation zum betrachteten Themenfeld. Im Bereich Geheimschutz sind weiterhin verdeckte Informationsabflüsse ein Sicherheitsrisiko. Der gesamte Themenkomplex wird durch Methoden der Usable Security begleitet, um den Faktor Mensch gebührend zu berücksichtigen.

Die Weiterbildung richtet sich an IT-Sicherheitsanalysten und Betreiber von IT-Infrastrukturen und Gebäudeautomation sowie öffentlichen Einrichtungen.

Mehr Informationen und Anmeldung unter:
www.academy.fraunhofer.de/emergency-response

BETEILIGTE EINRICHTUNGEN

- **Fraunhofer FKIE**
- **Hochschule Bonn-Rhein-Sieg**

THEMEN-SCHWERPUNKTE

- **Techniken und Strategien für den Hochsicherheitsbereich**
- **Untersuchung von Angriffstechniken und Schadsoftware**
- **Strategien und Prozeduren für Incident Response**
- **IT-Forensik und Internet of Things**

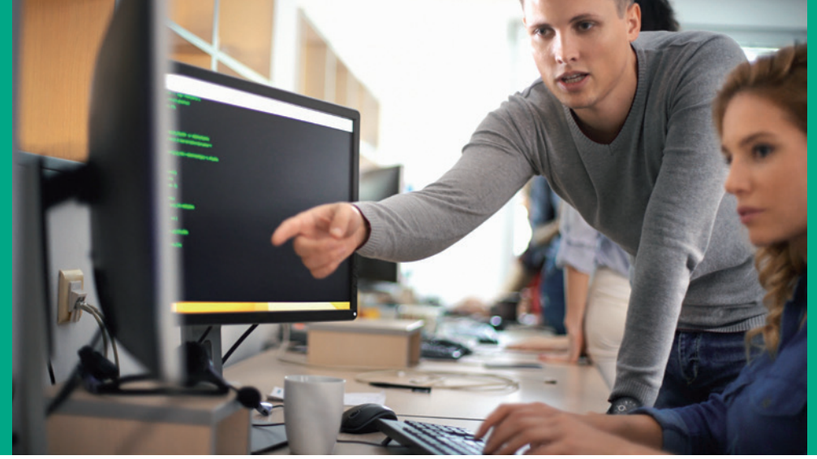
SCHULUNGEN 2017 | 18

Management

IT-Sicherheit im Unternehmen | Problematiken von IT-Sicherheit im Spannungsfeld von Komplexität, Usability, Bequemlichkeit, Kostendruck und sozialer Interaktion	22.11.2017 15.1. | 25.4.2018 Bonn

Fachkräfte und Anwender

Grundlagen der Python-Programmierung für Analysten | Spezifische Konzepte von Python mit Hilfe von praktischen Übungen verstehen, um Programme inkrementell zu entwickeln	20.–21.2.2018 Bonn
Netzwerkgrundlagen für Analysten | Grundlagen zu Netzwerktechnologie erlernen und Angriffe sowie Verteidigungsmaßnahmen in einem Testnetzwerk erproben	12.–15.3.2018 Bonn
Grundlagen der IT-Sicherheit für Fachkräfte | Potenzielle Sicherheitsrisiken identifizieren, IT-Sicherheitskonzepte aus Sicht eines Systementwicklers nachvollziehen und praktisch umsetzen	11.–13.4. | 24.–26.10.2018 Bonn
Einführung Schadsoftware | Schadsoftware und deren Vorgehen auf befallenen Systemen verstehen: Eigenschaften und Motivationen bei Sicherheitsvorfällen nachvollziehen	16.4.2018 Bonn
Grundlagen Windows für Analysten | Grundsätze moderner Betriebssysteme kennen: Windows-Architektur und -Eigenheiten verstehen, Analyse von Schadsoftware üben	17.4.2018 Bonn
Grundlagen Schadsoftwareanalyse Windows | Grundkenntnisse für Detailanalyse von Schadsoftware unter Windows; Systemaufrufe und Netzwerkprogrammierung in Assembler sowie statische und dynamische Analyse von Windows-Schadsoftware	12.–14.6.2018 Bonn
Einführung in die Datenträger- und Netzwerkforensik | Vorgehen in der digitalen Forensik: Auffinden und Wiederherstellen von Volumes, Analysen von Dateisystemen und Netzverkehr	10.–11.7.2018 Bonn
Biometrische Sicherheit I | Techniken der biometrischen Sicherheit kennenlernen sowie Angriffsmechanismen und deren Bekämpfung theoretisch und praktisch erfahren	13.–14.9.2018 Bonn
IoT-Sicherheitsmodelle I | Standardisierungsaktivitäten und Sicherheitsmechanismen kennenlernen, praktische Umsetzung und Usability von Sicherheitsmechanismen und Verwendung sicherer Entwicklungspraktiken erfahren	20.–21.9.2018 Bonn
Funkbasierte Gebäudetechnik I | Protokollmechanismen und deren Schwachstellen (WLAN, Bluetooth, ZigBee, Z-Wave, 6LowPAN etc.) sowie Angriffs- und Verteidigungsmethoden funkbasierter Gebäudetechnik verstehen	27.–28.9.2018 Bonn
Fortgeschrittene Schadsoftwareanalyse Windows | Verschleierungsmethoden von Schadsoftware erkennen, bewerten und selbst programmatisch auflösen	7.–8.8.2018 Bonn



7.–8.8.2018

FORTGESCHRITTENE SCHADSOFTWARE-ANALYSE WINDOWS

Fortgeschrittene Schadsoftware entschleiern und analysieren

Die Herausforderung: Schadsoftware immer schwieriger aufzuspüren

Moderne Schadsoftware versucht, ihre Analyse durch die Verwendung von verschleiernden Techniken hinauszuzögern. Dynamisches Entpacken von Code, Verschlüsselung von Strings und Code-Injektionen sind nur einige der genutzten Techniken. Diese Techniken zielen sowohl auf die dynamische als auch auf die statische Analyse ab. Sofern eine Detailanalyse einer bestimmten Schadsoftware angestrebt wird, muss ein Schadsoftwareanalyst in der Lage sein, diese Techniken zu identifizieren und anschließend zu entschleiern, damit eine Schadsoftwareanalyse überhaupt möglich ist.

Die Lösung: Verschleierungstechniken von Schadsoftware kennen und aufdecken

Im Seminar vermitteln wir Ihnen Kenntnisse über gängige Verschleierungsmaßnahmen und erklären, wie diese – auch mittels Automation – umgangen werden können. Sie erfahren, wie gängige Verschleierungstechniken, etwa z.B. Applikationspacking, Code-Injektionen sowie String-Verschlüsselung, funktionieren. In vielen Praxisübungen lernen Sie diese zu erkennen und aufzulösen. Eine besondere Rolle spielt hierbei die Automatisierung von statischen Analysewerkzeugen wie IDA Pro. Diese bieten Python-Schnittstellen, mittels derer wiederkehrende Aufgaben sowie massenhafte Bearbeitung von Verschleierungstechniken ermöglicht werden.

Die Inhalte

- Manuelles Entpacken von Programmen mit anschließender IAT-Rekonstruktion
- Manuelles Entpacken von schadsoftwarespezifischen Packern
- Härten einer virtuellen Maschine
- Erkennung und Umgehung von Code-Injektionen
- Automatisierung von IDA Pro mittels IDAPython und Sark
- Erkennung und Umgehung von Stringverschlüsselung
- Erkennung und Umgehung von API-Verschleierung

Die Lernziele

Kennen
- Gängige Verschleierungsmethoden wie String-Verschlüsselung, API-Verschleierung, Code-Injektionen
- Möglichkeiten und Grenzen der Entschleierung

Verstehen
- Applikationspacker, Code-Injektionen, API/String-Verschleierung

Die Zielgruppe

Angehende Schadsoftwareanalysten, die bereits erste Erfahrungen mit dynamischer und statischer Analyse haben

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …
… Verschleierungsmethoden erkennen und bewerten.
… einfache Verschleierungsmethoden selbst programmatisch auflösen.

Dieses Seminar bietet Ihnen …
… einen Überblick über gängige Verschleierungsmethoden, präsentiert durch einen Fachexperten.
… Techniken zur Erkennung und zum Auflösen von Verschleierungsmethoden.
… viele praxisnahe Übungen mit aktueller und relevanter Schadsoftware zum Auflösen von Verschleierungsmethoden.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/fortgeschrittene-schadsoftwareanalyse-windows

INFORMATIONEN IM ÜBERBLICK

Kurs: Fortgeschrittene Schadsoftwareanalyse Windows
Voraussetzungen:
- Theoretische und praktische Kenntnisse in der Analyse von Windows-Schadsoftware (siehe Modul »Grundlagen Schadsoftwareanalyse für Windows«)
- Umgang mit Windows/Linux
- Umgang mit IDA Pro und Debugger (z. B. x64dbg)
- Netzwerkkenntnisse
- Programmierkenntnisse in Python (wichtig) sowie C/C++ (vorteilhaft)
- Verständnis von x86-Assembler

Dauer: 2 Tage in Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: Fraunhofer FKIE in Bonn
Termin: 7.–8.8.2018
Kosten: 1200 €

Veranstaltet durch: Fraunhofer FKIE

WEITERE SEMINARE AUS DEM BEREICH

Sie interessieren sich zunächst für eine Einführung zur Analyse von Windows-Schadsoftware? Dann sehen Sie sich doch unseren Basic-Kurs »Grundlagen Schadsoftwareanalyse Windows« an: **www.academy.fraunhofer.de/schadsoftwareanalyse-windows**

UNSER REFERENT

Thomas Barabosch
Wissenschaftlicher Mitarbeiter bei Fraunhofer FKIE

ANSPRECHPARTNER

Thomas Barabosch | Fraunhofer FKIE
thomas.barabosch@fkie.fraunhofer.de

ORGANISATORISCH

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de

QUALIFIZIERUNG AUF DEM AKTUELLSTEN STAND

AN WEN SICH DAS WEITERBILDUNGSANGEBOT RICHTET

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.

Management

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 ein »Bewusstsein« und Verständnis für Cybersicherheit zu erzeugen, stellt einen Teil der Weiterbildung dar. Darüber hinaus findet auch Beratung statt, z. B. in Form einer Zertifizierungsunterstützung oder der Information über aktuelle Standards, Normen und Gesetzeslagen.

Fachkräfte & Anwender

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-Beauftragte und Sachverständige 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.

IT-Sicherheit sowohl für Unternehmen als auch für 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.

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 (Industrial Data Space, Center for Research in Security and Privacy, Kompetenzzentrum für angewandte Sicherheitstechnologie etc.) eingebunden.

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

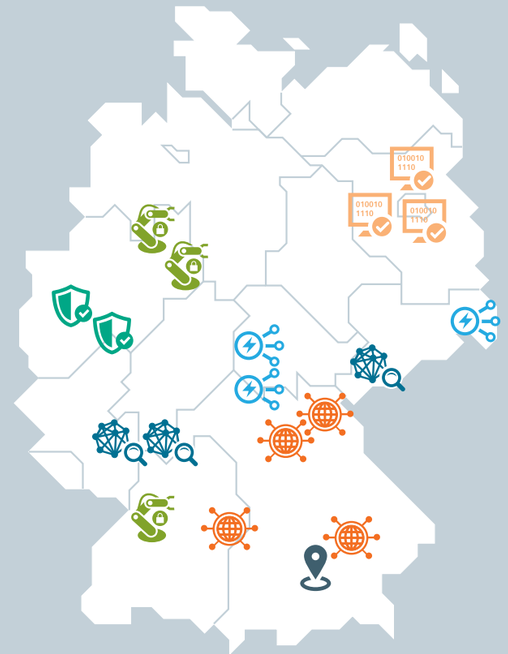
Die beteiligten Fachhochschulen haben durch ihre Kooperation mit der Wirtschaft, insbesondere mit den ansässigen KMU, eine starke regionale Verankerung. Zudem spielen sie eine tragende Rolle in der Ausbildung von Fach-und Führungskräften in Deutschland. Sie bilden insbesondere für die regional ansässige Industrie einen wichtigen Talentpool für die Einstellung neuen Personals. Das mit Fraunhofer bearbeitete Themenfeld fügt sich stimmig in das Portfolio und die Entwicklungsstrategie der Hochschule. Die Kooperation mit weiteren Partnern ist angedacht.

Beteiligte Fraunhofer-Institute

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

Beteiligte Fachhochschulen

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



Ihre Ansprechpartner für das Lernlabor Cybersicherheit

Martin Priester
Koordination Weiterbildung
Stellvertretender Leiter der
Fraunhofer Academy

Dr. Birgit Geier
Koordination Forschung
Abteilung Mikroelektronik,
IuK, Life Sciences

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 unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung.

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

www.cybersicherheit.fraunhofer.de

Oder folgen Sie uns auf
Facebook, Twitter, Google+
und Xing

Herausgeber
Fraunhofer Academy
Hansastraße 27c
80686 München

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

Redaktion: Theresia Gierull

Layout und Satz:
Vierthaler & Braun,
Visuelle Kommunikation

Druck: Universal Medien

Abbildungen: © Fraunhofer, istock, Hochschule Mittweida, Myrzik und Jarisch; Stand Oktober 2017