

WEITERBILDUNG IM LERNLABOR CYBERSICHERHEIT





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

DIGITALISIERUNG BRAUCHT IT-SICHERHEITSKOMPETENZ

Informations- und Kommunikationstechnologien (IKT) sind heute aus dem Alltag von Gesellschaft, Wirtschaft und Behörden nicht mehr wegzudenken. Der Einsatz von IKT ist in praktisch allen Wirtschaftsbranchen ein entscheidender Faktor für die Wettbewerbsfähigkeit der Unternehmen. IKT durchdringt branchenübergreifend Wertschöpfungsketten und ist inzwischen einer der wichtigsten Treiber von Innovationen. Dadurch ist IKT einerseits von zentraler Bedeutung für Wirtschaft und Wohlstand in Deutschland, andererseits entstehen durch den breiten Einsatz von IKT erhebliche Risiken für Wirtschaft und Gesellschaft. Das gilt insbesondere dann, wenn informationstechnische Systeme, Anwendungssoftware oder Infrastrukturen nicht hinreichend sicher sind. Diese Risiken bestehen sowohl für Anwender und Hersteller von IKT sowie für Anbieter von IKT-basierten Diensten.

Mit der zunehmenden Digitalisierung der Gesellschaft wächst das Bedrohungspotenzial von Cyberattacken deutlich an. Neben bisherigen Angriffen treten auch Angriffsszenarien auf kritische Infrastrukturen und hochskalierte Angriffe auf Industrieanlagen in den Vordergrund. Daher ist IT-Sicherheit bzw. Cybersicherheit eine Querschnitts- und Schlüsseltechnologie für eine funktionierende moderne Gesellschaft und Industrie.

Die rasanten Veränderungen in der Informationstechnologie betreffen heute nicht nur IT-Sicherheitsfachkräfte, Entwickler, Anwender und Tester, aber auch Führungskräfte auf den unterschiedlichsten Entscheider-Ebenen, insbesondere in kleineren und mittelständischen Unternehmen sowie Behörden benötigen eine große Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und Konsequenzen von IT-Sicherheitsproblemen. Ziel ist es, mögliche Risiken für das unternehmerische Handeln zu reduzieren und sicher zu beherrschen.

Cybersicherheit steht für die Erlangung digitaler Souveränität an erster Stelle. Daher ist für Wirtschaft und Behörden eine ausreichende Zahl an Fachkräften mit einem hohen Qualifizierungsniveau im Bereich Cybersicherheit erforderlich. Politik und Wirtschaft sind sich darin einig, dass das Thema Cybersicherheit von zentraler Bedeutung ist. Daher stellt das BMBF seit 2016 sechs Mio € pro Jahr für das Lernlabor Cybersicherheit zur Verfügung. Diese Initiative sichert die anwendungsnahe Erforschung praktikabler Sicherheitskonzepte und deren unmittelbare Umsetzung in Qualifizierungsprogramme für Kunden aus Industrie und öffentlicher Verwaltung.



»IT-Sicherheit muss als integraler Bestandteil aller Phasen und Entwicklungsstufen im Lebenszyklus von Produkten, Systemen, Infrastrukturen und Dienstleistungen betrachtet und mitbedacht werden. Dies schließt auch die Menschen und deren Ausbildung ein.« *Strategie- und Positionspapier der Fraunhofer-Gesellschaft zur Cybersicherheit 2020*

Mit Qualifizierung Sicherheits- und Kompetenzlücken schließen

Das Lernlabor Cybersicherheit der Fraunhofer Academy ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT-Infrastruktur. Sie stellen dort reale Bedrohungsszenarien nach, lernen deren Bedeutung und Konsequenzen zu erkennen und studieren geeignete Lösungskonzepte praxisnah in ihrem Einsatz und ihrem Wirkungsgrad.

In Anlehnung an bewährte Kooperationsmodelle zwischen Fraunhofer und Fachhochschulen wird für die Weiterbildung von IT-Sicherheitsfachkräften ein Modell umgesetzt, das die Fachhochschulen in der kooperativen Forschung, in der Entwicklung der Weiterbildungskonzepte und Lehrmodule und schließlich in der Vermittlung der Lehrinhalte als Partner einbindet.

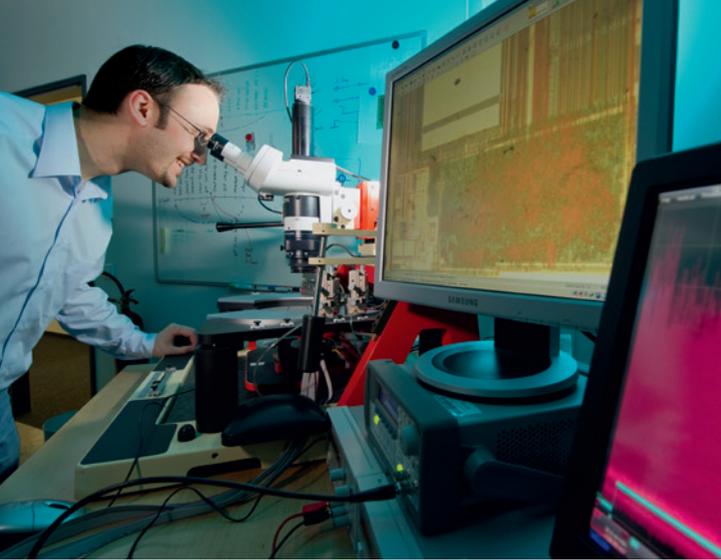
Durch den Aufbau des Lernlabors Cybersicherheit und der Vernetzung des Weiterbildungsangebots verschiedener Partnerkonsortien werden Anwender und Entscheider adressiert. Die Module sind branchen-, themen- und funktionspezifisch auf die Bedarfe der Industrie und öffentlichen Verwaltung abgestimmt.

Es werden Module in den nachfolgenden Themenfeldern angeboten:

- »Industrielle Produktion/Industrie 4.0«
- »Kritische Infrastrukturen/Anwendungsfall Energie- und Wasserinfrastrukturen«
- »Hochsicherheit und Emergency Response«
- »Internetsicherheit und IT-Forensik«
- »Softwarequalität/Produktzertifizierung«
- »Embedded Systems, Mobile Security und Internet of Things«

Aus Sicht der Wirtschaft ist es wichtig, dass Inhalte modular aufgebaut sind und sich passgenau an praktischen Fragestellungen orientieren. Hierbei ist zu berücksichtigen, dass der Praxisanteil in dem Weiterbildungsprogramm einen großen Umfang hat. Darüber hinaus ist es notwendig, dass sich die Weiterbildung für Fachkräfte möglichst einfach mit dem Berufsalltag der Angestellten kombinieren lässt. Das bedeutet, dass die einzelnen Module des Angebots kompakt (ein- bis dreitägig) sind und nicht über längere Zeiträume Ressourcen binden.

Die Qualität der Schulungen wird durch die Einbeziehung der Fraunhofer Academy gesichert. Diese ist verantwortlich für die Berücksichtigung aktuellster Erkenntnisse aus der Lern- und Bildungsforschung in der Angebotsentwicklung sowie für ein durchgehendes Qualitätsmanagement. Weiterhin koordiniert sie sowohl die Angebotsentwicklung und -vermarktung als auch eine (spätere) Personenzertifizierung.



Kompetenzaufbau für die Wirtschaft im Fraunhofer-Fachhochschul-Laborverbund

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

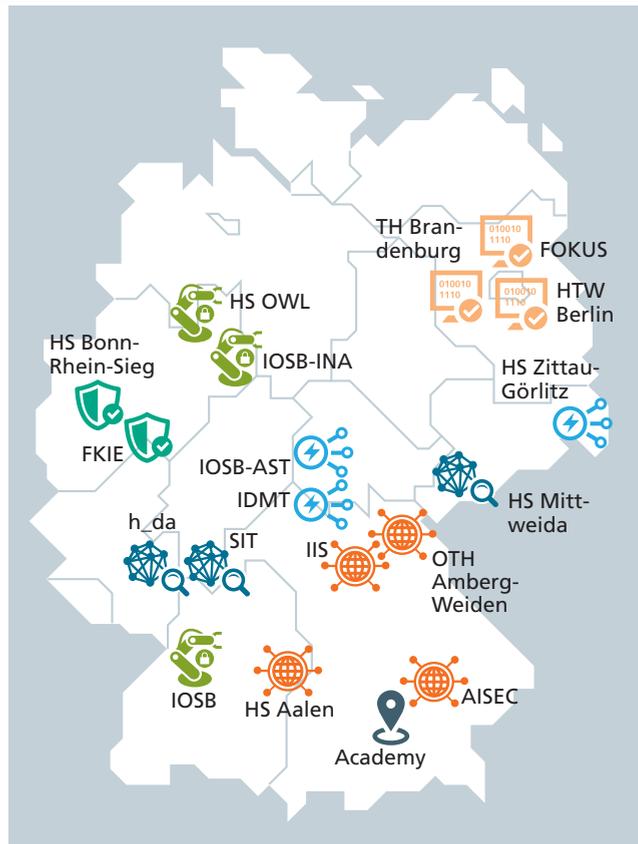
Die Fraunhofer Academy ist die Plattform der Fraunhofer-Institute, auf der sie gemeinsam mit ausgewählten Partnern ihre Kompetenzen für den Wissenstransfer aus der Fraunhofer-Forschung in die Praxis einbringen. Die Angebotsentwicklung, Vermarktung und Qualitätssicherung koordiniert die gemeinsame Geschäftsstelle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

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.



Softwarequalität/Produktzertifizierung



KRITIS – Energie- und Wasserinfrastrukturen



Internetsicherheit und IT-Forensik



Embedded Systems, Mobile Security und Internet of Things



Industrielle Produktion/Industrie 4.0

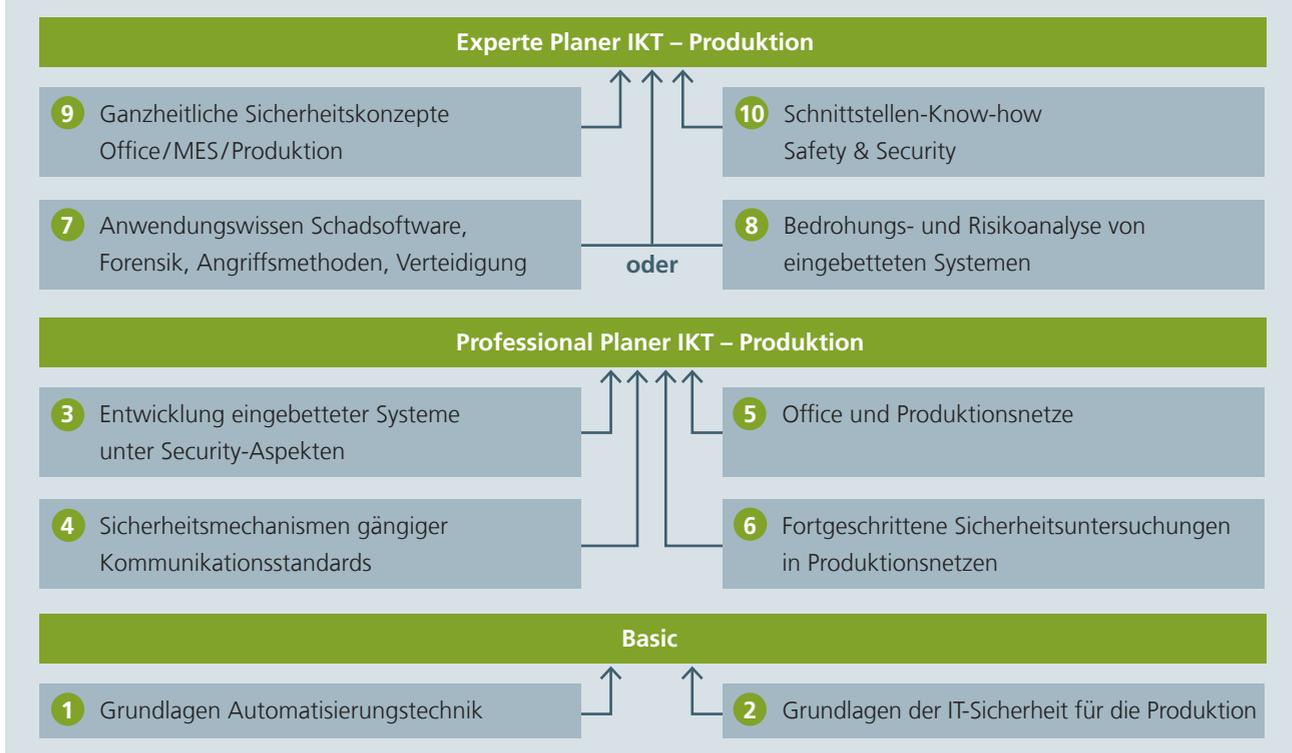


Hochsicherheit und Emergency Response



Geschäftsstelle der Fraunhofer Academy

Beispiel: Modulangebot für Planer IKT in der »Industriellen Produktion«



Beispiel: Zielgruppen im Themenfeld

»Industrielle Produktion«

- **Management:** Der Fokus des mittleren und gehobenen Managements liegt in der Sensibilisierung. Die eigene Lage reflektieren und in Verbindung mit aktuellen Problemen aus der Industrie 4.0 setzen, um ein »Bewusstsein« für Cybersicherheit zu erzeugen, stellt einen Teil der Weiterbildung dar. Darüber hinaus soll auch die Beratung stattfinden, z. B. in Form einer Zertifizierungsunterstützung oder der Information über aktuelle Standards, Normen und Gefahren.
- **IT-Beauftragte der Produktion:** Der Fokus von Sachverständigen aus dem Bereich IT liegt in der Vertiefung des bereits profunden Wissens. Dieses soll bereichert werden durch Best-Practices und Informationen zum State-of-the-Art von Kommunikationsarchitekturen. Die Sachkompetenz kann darüber hinaus durch Informationen zur aktuellen Gesetzes- und Richtlinienlage erweitert werden.
- **Planer/Entwickler:** Der Fokus von verantwortlichen Entwicklern industrieller Anlagen liegt in der Qualifikation anhand praktischer Fallarbeiten. Best-Practices und Informationen zum State-of-the-Art im Bereich Security & Safety sowie im Bereich industrieller Kommunikationssysteme werden bezogen auf die IT-Sicherheit behandelt. Unterschiedliche Kommunikationsschnittstellen sowie intelligente Datenanalyse bis in die Feldebene können in den Weiterbildungslaboren erprobt werden, um für die berufliche Praxis Handlungsoptionen aufzuzeigen.
- **Anwender:** Der Fokus aller Anwender, hierzu zählen im Allgemeinen die Betreiber z. B. Mitarbeiter im Bereich der Wartung, aber auch die Maschinenbediener, sollen wiederum hinsichtlich eines sicherheitskonformen Verhaltens sensibilisiert werden. Generelle Informationen zu IT-Bedrohungslage und Umgang mit Daten sollen so die firmeneigene Informationspolitik unterstützen.

Ihre Ansprechpartner für das Lernlabor Cybersicherheit



Martin Fischer

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 Weiterbildungsmodulare 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

GEFÖRDERT VOM



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