## IHR NUTZEN AUF EINEN BLICK

- Praktische Anwendungen in Experimentallaboren
- Transfer von neuestem Forschungswissen
- Fachreferenten mit führendem Expertenwissen
- Bedarfsorientierte Trainings auf Basic-, Advanced- und Expert-Level
- Effektives Training in kleinen Gruppen
- Bei Bedarf individuell angepasste Inhouse-Trainings

### HABEN SIE NOCH WEITERE FRAGEN…

zu Themen und Trainings?


**Lernlabor Cybersicherheit**
Hochsicherheit und Emergency Response
Fraunhofer FKIE
**Ansprechpartnerin:**
**Annemarie Theis**
Telefon +49 228 50212-590
lernlabor@fkie.fraunhofer.de


zu ähnlichen Weiterbildungsangeboten?


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


**www.fkie.fraunhofer.de/lernlabor**


*Stand: März 2019*




Fraunhofer
ACADEMY


IT-Sicherheits-Seminare

# LERNLABOR CYBERSICHERHEIT
IT-SICHERHEIT. VON PROFIS.
PRAXISNAH TRAINIERT.

## WERDEN SIE IT-SICHER!

Die Fraunhofer Academy, die Weiterbildungsplattform der Fraunhofer-Gesellschaft, bietet mit verschiedenen »Lernlaboren Cybersicherheit« Weiterbildungsangebote zur Vermittlung von IT-Sicherheitskompetenzen an. Das Lernlabor »Hochsicherheit und Emergency Response« überführt aktuelle Erkenntnisse aus Wissenschaft und Forschung des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE und der Hochschule Bonn-Rhein-Sieg rund um das Thema Cybersicherheit in Fortbildungen.

Fach- und Führungskräfte aus Industrie und öffentlichen Organisationen erhalten in topmodernen Experimentallaboren eine bedarfsgenaue und praxisnahe Vermittlung von IT-Sicherheitskompetenzen.

## IT-SICHERHEIT IM UNTERNEHMEN

Aufgrund des dynamisch fortschreitenden Bedrohungspotenzials von Cyberangriffen gewinnt das Thema IT-Sicherheit immer mehr an Bedeutung. Denn je mehr automatisiert wird, desto mehr (sensible) Informationen sind potenziell abgreifbar. Um aktuelle und zukünftige IT-Sicherheitsanforderungen erfolgreich zu erfüllen, bedarf es eines Bewusstseins für Cybersicherheit sowie der notwendigen Kompetenzen für den Umgang mit entsprechenden Risiken.

### Lösungsorientierte Trainings für Fach- und Führungskräfte

**IT-Sicherheitsstrategie für Führungskräfte**
- Grundlagen der IT-Sicherheit und aktuelle Bedrohungslage kennen
- Aktuelle Herausforderungen der IT-Sicherheit und deren Bedeutung für Ihr Unternehmen bewerten

**IT-Sicherheit – Kryptographie und Netzwerkschutz**
- Kryptographische Verfahren, deren Einsatzzwecke und Angriffsmöglichkeiten kennenlernen und nutzen
- Netzwerksicherheit gewährleisten durch Erkennung von Risiken und Abwehr von Angriffen

**Sicherheit webbasierter Systeme**
- Bedrohungen identifizieren und bewerten
- Schutzmechanismen auf Netzwerk-, Protokoll- und Anwendungsebene kennenlernen und Gegenmaßnahmen erproben

## INTERNET OF THINGS (IOT) – SICHERE VERNETZUNG UND NEUE TECHNOLOGIEN

IoT-Geräte und damit einhergehende Technologien sind beliebte Angriffsziele geworden, da sie eine meist unzureichend abgesicherte Internet-Anbindung besitzen und innerhalb von IT-Sicherheitsstrategien oft vernachlässigt werden. Gleichzeitig eröffnen sie Zugang zu vertraulichen Bereichen des persönlichen Lebens oder zu schützenswerten Unternehmensbereichen. So können z. B. Produktionsdaten abgehört, Prozesse gestört oder diese sogar manipuliert werden.

### Praxis-Trainings für Fachkräfte und Anwender

**Sicherheit in drahtlosen Netzen**
- Mechanismen verstehen, Angriffe simulieren und Sicherheitsaspekte bewerten
- Schutzmechanismen für drahtlose Technologien erarbeiten und anwenden

**Sichere und zuverlässige Protokolle**
- Aufbau, Sicherheit und Zuverlässigkeit von Protokollen für IoT-Geräte kennenlernen
- Herausforderungen und Risiken bei Energieverbrauch und Firmware-Updates bewerten

**Blockchain – Funktionsweise und Bausteine**
- Funktionsweise und Prinzipien der Technologie verstehen
- Mit neuen Entwicklungen kritisch auseinander setzen und lösungsorientierte Anwendungen finden

## VERTEIDIGUNG GEGEN CYBERKRIMINALITÄT

Cyberkriminalität und Cyberspionage haben sich professionalisiert. Aus diesen Gründen gilt es, präventive Maßnahmen zur Sicherung der IT-Systeme zu ergreifen, bestehende Netze und Geräte zu überwachen sowie Bedrohungen erkennen, analysieren und abwehren zu können.

### Basic-, Advanced- und Expert-Trainings für Spezialisten

**Schadsoftware – Erkennen, analysieren, bekämpfen**
- Schadsoftware erkennen und analysieren
- Methoden und Werkzeuge zur statischen und dynamischen Analyse von Schadsoftware anwenden
- Praktische Anwendungen an realer Schadsoftware erproben

**Firmware – Extrahieren, entpacken, analysieren**
- Firmware eigenständig extrahieren und analysieren
- Vorgehensweisen für die Entwicklung eigener automatisierter und manueller Analysen erstellen
- Praktische Anwendungen an realer Hardware, z.B. Routern, erproben

**Netzwerkforensik – Extrahieren, analysieren, reagieren**
- Netzwerkmitschnitte extrahieren und analysieren sowie Gegenmaßnahmen ergreifen
- Netzwerkmitschnitte automatisiert und manuell auswerten
- Realitätsnahe Szenarien erproben

## SEMINARMODALITÄTEN

**Veranstaltungsorte**
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Zanderstraße 5
53177 Bonn

Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20
53757 Sankt Augustin

**Dauer je Training**
1 bis 2 Tage

Fraunhofer FKIE

Hochschule Bonn-Rhein-Sieg
University of Applied Sciences