Fraunhofer ACADEMY

Weiterbildung im
Lernlabor Cybersicherheit

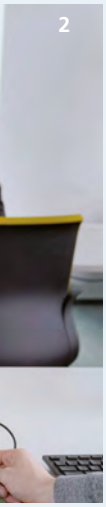
Know-how für mehr IT-Sicherheit

Sicherheit in Software-Entwicklung & Netzwerken

www.cybersicherheit.fraunhofer.de

Inhalt

1



2

3

Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy im Bereich Information und Kommunikation. Im Zentrum des umfassenden Angebots des Lernlabors stehen alle Themen rund um die IT-Sicherheit.

Impressionen aus unseren Lernlaboren Cybersicherheit:

1 Im Lernlabor Cybersicherheit am Fraunhofer AISEC erhalten Sie Einblick in aktuelle Forschungsthemen, z.B. die Absicherung der Kommunikation in und mit Fahrzeugen. Das Automotive Labor ermöglicht praxisnahe Einblicke.

2 Das Lernlabor Cybersicherheit beim Fraunhofer SIT.

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

4 Im Lernlabor Cybersicherheit des Fraunhofer FOKUS in Berlin werden verschiedene Gefahrenszenarien simuliert und vernetzte Technologien und Lösungen für die öffentliche Sicherheit praxisnah erprobt.

Mehr Sicherheit mit unseren Weiterbildungen

5 Gründe für die Weiterbildung im Lernlabor Cybersicherheit

5

Anerkannte Expertinnen und Experten

Profitieren Sie vom langjährigen Spezialwissen unserer Expertinnen und Experten aus der Forschung und unseren Entwicklungs- und Beratungsprojekten. In Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen erhalten Sie verwertbare, neueste Erkenntnisse auf allen Gebieten der Cybersicherheit.

Bei uns bekommen Sie Wissen aus erster Hand

Unsere Kurse sind nicht nur auf dem aktuellsten Stand der Forschung, sie orientieren sich auch passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Im Team trainieren und erarbeiten Sie Lösungskonzepte in den Bereichen, die für Sie tatsächlich relevant sind.

Maßgeschneiderte Inhouse-Seminare

Integrieren Sie die Weiterbildung zum Thema Cybersicherheit direkt in Ihr Unternehmen, für mehrere Mitarbeitende oder Abteilungen. Dafür passen wir die Inhalte individuell auf Ihre Bedarfe an. Wir beraten Sie gerne, welche Lösung für Sie die optimale darstellt.

Für jede Situation das passende Seminar

Ein Universalkonzept bei IT-Sicherheitslösungen gibt es nicht! Die Komplexität und das Spektrum an Problemfeldern ist einfach zu groß. In unserem breiten Themenangebot finden Sie jedoch garantiert die passende Weiterbildung. Zugeschnitten auf Ihren Kenntnisstand und auf Ihr Spezialgebiet. Ob als Onlineseminar, Präsenzseminar oder Mix aus beidem.

Lernlabore

An zahlreichen Standorten in Deutschland können Sie in unseren modernen Lernlaboren mithilfe hochwertiger technischer Infrastruktur reale Bedrohungsszenarien nachstellen und durchspielen. Anhand konkreter Anwendungsfälle wird so das Gelernte für Sie erfahrbar und direkt umsetzbar.

Kompetenzaufbau auf allen Ebenen

IT-Sicherheitswissen betrifft nicht mehr nur Spezialistinnen und Spezialisten, auch entscheidungsbefugte Personen, Fachkräfte und Anwendende sollten lernen, Sicherheitsrisiken abzuschätzen und diese zu beherrschen. Hierfür benötigen die Mitarbeitenden eine Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und die Konsequenzen von IT-Sicherheitsproblemen in ihrem Verantwortungsbereich. Das Lernlabor richtet sich deshalb an folgende Zielgruppen mit jeweils spezifischen Seminaren:

Führungskräfte, die Entscheidungsprozesse verantworten müssen, benötigen einen verständlichen Überblick über aktuelle Gefahren, Sicherheitsstrategien und Methoden.

Sicherheitsexpertinnen und -experten mit einer IT-Sicherheits-ausbildung oder entsprechender Berufserfahrung können ihr Wissen auf den neuesten Stand bringen.

Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

IT-Nutzerinnen und -Nutzer ohne spezifische Fachkenntnisse, von denen erwartet wird, dass sie Sicherheitsbewusstsein aufbauen und sicherheitskonformes Verhalten entwickeln.

Erklärung der Symbole auf den Seminarseiten

- Abschluss
- Voraussetzungen
- Zielgruppe
- Dauer
- Kosten
- Örtlichkeit

Entwicklung und Testing sicherer Software

Neueste Software muss Sicherheit integrieren

Bei der Entwicklung neuester Software werden Sicherheitsaspekte gegenüber den funktionalen Anforderungen gern vernachlässigt. Dabei lassen sich viele Schwachstellen und Gefahren durch eine systematische Herangehensweise vermeiden. Sicherheit beginnt schon mit den ersten Entwicklungsschritten.

Wer zu spät kommt, den bestraft das Leben oder in dem Fall der Hacker, denn Cybersicherheit ist nicht nur eine Frage, die erst im Bedrohungsfall auftritt, sondern muss bereits bei der Entwicklung von Beginn an mitgedacht werden. Das Stichwort heißt: Security by Design. Dazu gehören auch regelmäßige Sicherheitstests von Software und Systemen. Die Erfahrung zeigt: Über 90% aller Softwaresicherheitsfälle werden durch Angreifer verursacht, die bereits bekannte Sicherheitslücken ausnutzen!

Daraus lässt sich schließen, dass die meisten Angriffe und Vorfälle vermeidbar sind! Strukturierte Risikoanalysen, Penetrationstests und Hacking erlauben es, sicherheitsrelevante Schwachstellen aufzudecken und zu bewerten.

Im Lernlabor Cybersicherheit, lernen Sie auf Basis wissenschaftlicher Erkenntnisse, mit aktuellen Bedrohungen umzugehen, und erfahren, wie sich Sicherheitsaspekte bereits beim Design berücksichtigen lassen.

Über 90% aller Softwaresicherheitsfälle werden durch Angreifer verursacht, die bereits bekannte Sicherheitslücken ausnutzen!

Moderne und sichere Softwareentwicklung

Gemeinsam schneller zum Ziel? Aber sicher!

Bedeutende Erfolgsfaktoren moderner Software (-Entwicklung) sind nicht nur die Verwendung aktueller Technologien und veränderter Betriebskonzepte, wie etwa der Cloud. Insbesondere Werte wie Kundenorientierung, Sicherheit, Agilität, Automatisierung und Einfachheit erfordern die aktive und erfolgreiche Zusammenarbeit aller am Software-Lebenszyklus beteiligten Rollen, von den Kunden über das Management, Entwicklerinnern und Entwickler und Tester bis hin zu den Admins. Die Seminarreihe „Moderne und sichere Software-Entwicklung" vermittelt auf aktive Weise, welche Grundprinzipien, Technologien und Prozesse ineinandergreifen, um sichere, wartbare, erweiterbare und nutzwerte Software für verschiedenste Zielumgebungen zu gestalten und diese in den Betrieb zu überführen.

Inhalte des Seminars

Einführungsmodule
- Modul 1: Eine gemeinsame Sprache für Software
- Modul 2: Moderne Buzzwords und Cargo Cults: Agile, Blockchain, Microservices und Co
- Modul 3: Motivation – Digitale Transformation verstehen
- Modul 4: Dimensionen der Sicherheit von Software
- Modul 5: Prinzipien des modernen Software-Engineering

Aufbaumodule
- Modul 6: Aktuelle Software-Architekturen: Eine Übersicht
- Modul 7: Keep IT Simple
- Modul 8: Die Cloud
- Modul 9: Die Rolle von CI/CD und Dev(Sec)Ops
- Modul 10: Kaskadierende Effekte verteilter Systeme

Ihr Nutzen

- Durch die Seminarreihe erhalten Sie einen klaren und kritischen Blick auf Software und moderne Software-Entwicklung mit Schwerpunkt auf Sicherheit.
- Durch eine hohe Interaktivität und praxisnahe Übungseinheiten in den einzelnen Modulen können Sie Erlerntest unmittelbar in Ihrer Arbeit anwenden.
- Die Seminarreihe ist in ihrer Verständlichkeit auch für Nicht-Programmierer*innen geeignet.

Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Im Bereich Softwareentwicklung, -betrieb oder -management tätig

Führungskräfte, Management, Softwarearchitekt*innen, -Entwickler*innen, -Projektmanagement, Tester*innen, Admins, Designer*innen

Nach individueller Vereinbarung

Bis zu 30 h Online (in 10 Modulen à 3 Stunden)

300,– pro Modul (Buchung von mind. 5 Modulen)

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Hannes Restel
wiss. Mitarbeiter
Fraunhofer FOKUS

Johannes Einhaus
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/moderne-sichere-software-entwicklung

Informationen im Überblick

Grundlagen des Softwaretestens (z.B. ISQTB Certified Tester Foundation Level)

Produktmanager*innen, Projektleiter*innen in der Produktentwicklung, Produkt-, Anforderungs- und Testentwickler*innen, Testanalysten*innen, Testmanager, Abnahmetester*innen, Qualitätsmanager und -berater*innen

2 Tage online
10–16 Uhr

1200,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Jürgen Grossmann, Projektleiter Fraunhofer FOKUS

Martin Schneider, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/security-tester-basic

Security Tester – Basic

Ist meine Software sicher?

Über 90% aller Software-Sicherheitsvorfälle werden durch Angreifer verursacht, die bekannte Sicherheitslücken ausnutzen. Die Einführung eines Sicherheitstestprozesses sowie die Verwendung einfacher Basistechniken des Sicherheitstestens erlauben es, sicherheitsrelevante Schwachstellen zu erkennen und zu bewerten. Dieses Seminar vermittelt die allgemeinen Grundlagen des Sicherheitstestens und befähigt Sie, grundlegende Sicherheitstestmethoden anzuwenden.

Inhalte des Seminars

Testen allgemein
- Grundlagen des Testens
- Grundlagen des Sicherheitstestens
- Klassifikation der Testansätze
- Testprozesse
- Test Level
- Terminologie

Sicherheitsziele
- Anforderungserhebung und -management
- Sicherheitsanforderungen
- Informationssicherheitsmethoden
- Sicherheitsaudits

Sicherheitstestprozess
- Sicherheitstestziele und -strategien
- Sicherheitstestplan
- Entwurf von Sicherheitstestprozessen

Methoden des Sicherheitstestens im Softwarelebenszyklus
- Abbildung des Sicherheitstestens auf den Softwarelebenszyklus
- Bedeutung der Sicherheit für die Prozessrollen
- Sicherheitsmechanismen
- Sicherheitstestausführung
- Bewertung von Sicherheitstests
- Sicherheitstestwerkzeuge

Ihr Nutzen

- Nach dem Seminar können Sie grundlegende Sicherheitstesttechniken auswählen und anwenden sowie einen Sicherheitstestprozess aufsetzen und leiten.
- Sie können einfache Sicherheitsmechanismen testen.
- Sie wissen, wie und welche Test- und Sicherheitsteststandards anzuwenden sind.

Grundlagen des Security Testens

Modulare Schulungsreihe zum Sicherheitstesten

Sicherheitsanforderungen an moderne IT-Systeme steigen und sind nicht allein durch konstruktive Maßnahmen realisierbar. Eine systematische Verzahnung von Sicherheitstest-aktivitäten mit anderen Life Cycle Aktivitäten im Softwareentwicklungsprozess erlauben es, Sicherheitslücken bereits frühzeitig zu identifizieren und damit kosteneffizient beseitigen zu können. Die Seminarreihe »Grundlagen des Security Testens« vermittelt die allgemeinen Grundlagen des Sicherheitstestens, von Sicherheitstestprozessen und zeigt, wie insbesondere das Sicherheitstesten durch die Einbindung in ein konsequentes Risikomanagement optimiert werden kann.

Inhalte des Seminars

1. Modul: Sicherheitstests während des gesamten Software-Lebenszyklus
- Rolle des Sicherheitstestens in der Anforderungsspezifikation
- Rolle des Sicherheitstestens beim Entwurf
- Rolle des Sicherheitstestens in der Implementierungsphase
- Sicherheitstests in während der System- und Abnahmetests
- Sicherheitstests in der Wartung

2. Modul: Sicherheitstestprozesse
- Definition des Sicherheitstestprozesses
- Planung von Sicherheitstests
- Entwurf von Sicherheitstests
- Durchführung von Sicherheitstests
- Auswertung und Berichterstattung von Sicherheitstests

3. Modul: Risikomanagement und Sicherheitstests
- Risikomanagement im Gesamtkontext der Organisation
- Risikoidentifizierung
- Risikoanalyse
- Risikoevaluierung
- Risikobehandlung
- Risikobasiertes Sicherheitstesten
- Testbasierte Risikoanalyse und Risikoevaluation

4. Modul: Testen von Sicherheitsmechanismen
- Systemhärtung
- Authentifizierung und Autorisierung
- Verschlüsselung
- Firewalls
- Angriffserkennung
- Malware-Scan
- Datenmaskierung

Ihr Nutzen

- Dieses Seminar bietet Ihnen eine systematische Einführung in die Grundlagen des Sicherheitstestens und in Sicherheitstesttechniken wie das Fuzzing, Scan-ning etc.
- Sie sind danach in der Lage, einfache Sicherheitstestmaßnahmen im Software-lebenszyklus anzuwenden und systematisch zu integrieren.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Praktische Erfahrungen rund um Entwicklung, Betrieb und Testing von Software.

Produktmanager*innen, Projektleiter*innen, Produktentwickler*innen, Anforderungsentwickler*innen, Testentwickler*innen, Testanalyst*innen, Testmanager*innen, Abnahmetester*innen, Qualitätsmanagment und -beratung

Bis zu 32 h

2600,– (bei Buchung aller 4 Module)

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:


Jürgen Grossmann, Projektleiter Fraunhofer FOKUS


Martin Schneider, wiss. Mitarbeiter Fraunhofer FOKUS


Dorian Knoblauch, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/reihe_grundlagen-security-testen

Informationen im Überblick

Grundlagen des Softwaretestens (z.B. ISQTB Certified Tester Foundation Level)

Produktmanager*innen, Projektleiter*innen in der Produktentwicklung, Produktentwickler*innen, Anforderungsentwickler*innen, Testentwickler*innen, Testanalyst*innen, Testmanager*innen, Abnahmetester*innen, Qualitätsmanager*innen und -berater*innen

1 Tag (6 Stunden)

nach Absprache

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Jürgen Grossmann, Projektleiter Fraunhofer FOKUS

Dorian Knoblauch, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheitstests-software-lebenszyklus

Sicherheitstests während des gesamten Software-Lebenszyklus

Seminarreihe Grundlagen des Security Testing

Eine systematische Verzahnung von Sicherheitstestaktivitäten mit anderen Life Cycle Aktivitäten im Softwareentwicklungsprozess erlauben es, Sicherheitslücken bereits frühzeitig zu identifizieren und damit kosteneffizient beseitigen zu können.Der Kurs vermittelt die allgemeinen Grundlagen des Sicherheitstestens. Es werden spezielle Sicherheitstestmethoden, Auswahlkriterien für Sicherheitstesttechniken, die einzelnen Testschritte sowie ihre Rolle im Entwicklungszyklus erläutert.

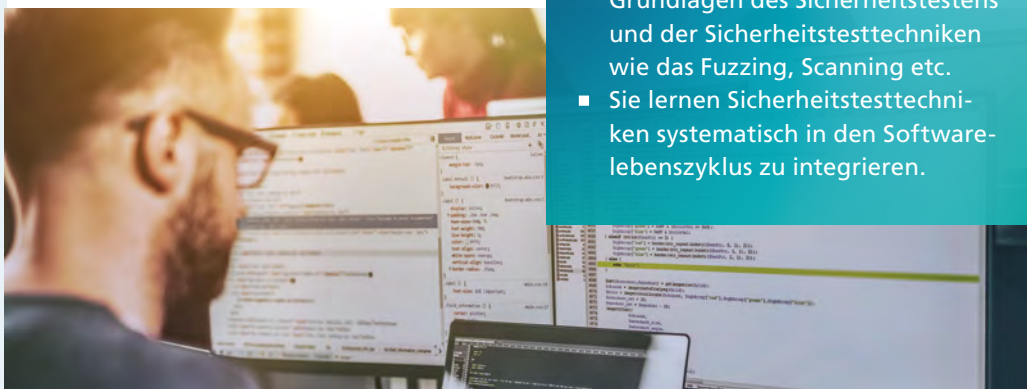
Inhalte des Seminars

Die Teilnehmenden sind nach dem Kurs in der Lage, einfache Bedrohungsanalysen für klassische Internet-Anwendungen durchzuführen und auf deren Basis, Sicherheitsrisiken zu klassifizieren, Sicherheitstestziele zu formulieren sowie Sicherheitstests systematisch zu erstellen und auszuführen.

- Analyse eines Anforderungssatzes aus der Sicherheitsperspektive, um Mängel zu identifizieren
- Analyse eines Entwurfsdokuments aus der Sicherheitsperspektive, um Schwachstellen zu identifizieren
- Rollenverständnis von Sicherheitstests während der Komponententestphase
- Sicherheitstestentwurf auf Komponentenebene anhand einer definierten Implementierungsspezifikation
- Testergebnisanalyse auf Komponentenebene, um die Angemessenheit des Codes aus der Sicherheitsperspektive zu bestimmen
- Verständnis der Grundprinzipien eines statischen Code-Checkers
- Anwendung eines automatisierten, statischen Code-Checkers und Verständnis über die Fallstricke der Automatisierung
- Erstellen eines End-to-End-Testszenarios für Sicherheitstests, das vorgegebene Sicherheitsanforderungen verifiziert und einen beschriebenen funktionalen Prozess testet
- Definieren einer Reihe von Abnahmekriterien für die Sicherheitsaspekte eines bestimmten Abnahmetests
- Erstellen eines End-to-End-Ansatzes für Sicherheitstests/Regressionstests auf der Grundlage eines gegebenen Szenarios
- Verstehen der Unterschiede zwischen Regressionstests, Re-Tests und Penetrationstests

Ihr Nutzen

- Nach dem Seminar können Sie grundlegende Sicherheitstesttechniken auswählen und Sicherheitstestmethoden und einfache Sicherheitstestmaßnahmen im Softwarelebenszyklus anwenden.
- Dieses Seminar bietet Ihnen systematische Einführung in die Grundlagen des Sicherheitstestens und der Sicherheitstesttechniken wie das Fuzzing, Scanning etc.
- Sie lernen Sicherheitstesttechniken systematisch in den Softwarelebenszyklus zu integrieren.



Sicherheitstestprozesse

Seminarreihe Grundlagen des Security Testing

Durch das Planen, Überwachen und Durchführen systematischer Sicherheitstestprozesse können Sicherheitslücken in der Software umfassend und nachvollziehbar identifiziert und behoben, sowie der Fortschritt und Abschluss gemessen und festgestellt werden. Der Kurs vermittelt die allgemeinen Grundlagen und die Struktur von Sicherheitstestprozessen.

Inhalte des Seminars

Sicherheitstestprozesse werden im Kontext verschiedener Anwendungslebenszyklusmodelle betrachtet. Die konkreten Aufgaben in den verschiedenen Phasen des Sicherheitstestprozesses werden analysiert. Praktische Sicherheitstests werden entlang der verschiedenen Phasen erläutert und durchgeführt. Dabei werden einige typische Schwachstellen und Testmethoden erläutert. Die organisatorischen Rahmenbedingungen von Sicherheitstests in den Phasen des Sicherheitstestprozesses werden ebenfalls betrachtet.

Die Teilnehmenden sind nach dem Kurs in der Lage, die wichtigsten Aktivitäten für einen systematischen Sicherheitsprozess auszuwählen, zu planen, durchzuführen und zu analysieren. Dazu gehört:

- Definieren der Elemente eines effektiven – Definieren effektiver Sicherheitstestprozesselemente
- Analysieren eines Sicherheitstestplans
- Entwurf konzeptioneller Sicherheitstests
- Entwurf von Testfällen zur Validierung von Sicherheitsrichtlinien und -verfahren
- Verständnis von Schlüsselelementen und Merkmalen einer effektiven Sicherheitstestumgebung
- Verständnis von Planung und Genehmigung vor und Analyse nach der Durchführung von Sicherheitstests und geeigneten Kontrollmechanismen zur Datenerfassung
- Analyse eines Zwischenberichts

Ihr Nutzen

- Nach dem Seminar verstehen Sie die Sicherheitstestprozesse in verschiedenen Anwendungslebenszyklusmodelle und können Sicherheitstestprozesse und die Aktivitäten in dessen Phasen planen und grundlegende Methoden für die Aktivitäten in den einzelnen Phasen des Sicherheitstestprozesses auswählen und anwenden.
- Dieses Seminar bietet Ihnen eine systematische Einführung in Sicherheitstestprozesse und Sicherheitstesttechniken wie das Fuzzing und die Testbewertung.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundlagen des Softwaretestens (z.B. ISQTB Certified Tester Foundation Level)

Produktmanager*innen, Projektleiter*innen in der Produktentwicklung, Produktentwickler*innen, Anforderungsentwickler*innen, Testentwickler*innen, Testanalyst*innen, Testmanager*innen, Abnahmetester*innen, Qualitätsmanager*innen und -berater*innen

1 Tag (6 Stunden)

nach Absprache

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Martin Schneider, wiss. Mitarbeiter Fraunhofer FOKUS

Dorian Knoblauch, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheitstestprozesse

Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundlagen der Softwareentwicklung

Entwickler*innen, Systemadministrator*innen, Testentwickler*innen

1 Tag (6 Stunden)

nach Absprache

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Jürgen Grossmann, Projektleiter Fraunhofer FOKUS

Johannes Viehmann, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/risikomanagement-sicherheitstests

Risikomanagement und Sicherheitstests

Seminarreihe Grundlagen des Security Testing

Vertrauen schaffende Sicherheit bei komplexen, vernetzten IT-Systemen zu erreichen, ist alles andere als einfach. Wo keine perfekte Sicherheit erzielt werden kann, sollte ein sorgfältiges, systematisches Risikomanagement die Grundlage für alle sicherheitsrelevanten Maßnahmen sein. Dieser Kurs soll für die Dringlichkeit des Risikomanagements sensibilisieren und zeigen, wie insbesondere das Sicherheitstesten durch die Einbindung in ein konsequentes Risikomanagement optimiert werden kann. Er vermittelt die notwendige Methodik und das zugehörige Wissen, um ein risikobasiertes Sicherheitstesten selbstständig durchzuführen.

Inhalte des Seminars

Die Teilnehmenden sind nach dem Kurs in der Lage, ein Risiko-Management zu implementieren und basierend auf den Risikomodellen optimierte Sicherheits-tests durchzuführen.

- Risikomanagement im Gesamtkontext der Organisation
- Risikoidentifizierung
- Risikoanalyse
- Risikoevaluierung
- Risikobehandlung
- Risikobasiertes Sicherheitstesten
- Testbasierte Risikoanalyse und Risikoevaluation
- ISO 31000 Risk Management
- Risk Based Security Testing
- Test Based Risk Assessment

Ihr Nutzen

- Dieses Seminar bietet Ihnen die theoretischen Grundlagen des Risikomanagements und ermöglicht ein Lernen an Hand von praktischen Beispielen.
- Nach dem Seminar können Sie ein systematisches Risikomanagement durchführen und aus Risikomodellen Sicherheitstestfälle ableiten und priorisieren. Sie können dann die Ergebnisse von Sicherheitstests im Hinblick auf das Risikobild auswerten.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Testen von Sicherheitsmechanismen

Seminarreihe Grundlagen des Security Testing

Sicherheit bei modernen IT-Systemen lässt sich durch eine Vielzahl an Mechanismen herstellen. Zu den gängigsten zählen Firewalls, Malware-Scanner, Autorisierung und Authentifizierung. Je nachdem wie das jeweilige System beschaffen ist, werden geeignete Mechanismen implementiert, deren Wirksamkeit es zu testen gilt. Der Kurs vermittelt Testmethoden und Konzepte zum Test der gängigen Sicherheitsmechanismen. Hierbei werden grundlegende konzeptionelle und technische Kenntnisse vermittelt, die mittels konkreter Beispiele verdeutlicht werden.

Inhalte des Seminars

Die Teilnehmenden können die Testmethoden der Sicherheitsmechanismen während eines Angriffs auf ein IT-System ausprobieren. Dabei werden charakteristische Schwachstellen ausgenutzt, und zugleich Methoden vermittelt, um diese zu identifizieren und zu schließen. Die Teilnehmenden sind nach dem Kurs in der Lage je nach System geeignete Sicherheitsmechanismen zu verstehen, zu implementieren und zu testen. Hierzu zählt:

- Verstehen des Konzepts der Systemhärtung so wie des Testens der Härtung von Linux-Systemen mittels OpenScap
- Verstehen des Zusammenhangs zwischen Authentifizierung und Autorisierung und die Fähigkeit entsprechende Mechanismen zu implementieren
- Passwörter knacken mittels hashcat
- Verschlüsselung anhand von https-Kommunikation verstehen, Mitschneiden und Entschlüsseln der Https-Kommunikation des Browsers
- Konzept und Anwendung der Firewalls bei der Sicherung von Informationssystemen verstehen und mittels Portscans testen
- Das Prinzip von Angriffserkennungswerkzeugen verstehen und deren Einsatz bei einem Linux-System lernen
- Potenziale und Grenzen von Malware-Scannern analysieren und erproben
- Datenmaskierung erkennen und aushebeln

Ihr Nutzen

- Dieses Seminar bietet Ihnen eine systematische Einführung in das Testen von Sicherheitsmechanismen.
- Anhand von praktischen Beispielen lernen die Teilnehmenden, das neue Wissen an einem Scenario direkt anzuwenden.
- Nach dem Seminar können Sie Sicherheitsmechanismen einsetzen und Testmethoden für die gängigen Sicherheitsmechanismen anwenden.

Informationen im Überblick

Grundlagen des Softwaretestens (z.B. ISQTB Certified Tester Foundation Level)

Entwickler*innen, Systemadministrator*innen, Testentwickler*innen

1 Tag (6 Stunden)

nach Absprache

Präsenz oder online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Jürgen Grossmann, Projektleiter Fraunhofer FOKUS

Johannes Viehmann, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheitsmechanismen

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundkenntnisse der Softwaretechnik (Software Engineering): Softwareentwicklungsprozesse, Anforderungsanalyse, Softwaredesign, Nachvollziehen von C-Programmbeispielen, Softwaretest

Softwarearchitekt*innen; -ingenieur*innen; Fachexpert*innen und technische (Projekt-) Leiter*innen in Entwicklungsprojekten

2 Tage

1200,–

Weiden in der Oberpfalz oder online

Veranstaltet durch

Fraunhofer AISEC

Referent:

Felix Schärtl, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sse-automobil

Softwaresicherheit im automobilen Entwicklungsprozess

Step by Step zu mehr Sicherheit

Die Herausforderung: Software kann nur schwer im Nachhinein sicher gemacht werden. Der erhöhte Komplexitätsgrad im Entwicklungsprozess des Software Engineering führt zu mehr Angriffsfläche auf die Systeme. Umso wichtiger ist es deshalb, Sicherheitsaspekte in jedem Entwicklungsschritt mitzubedenken! Aber wie lässt sich dies umsetzen? In diesem Seminar werden Sie mit den wichtigsten Aspekten der Softwaresicherheit vertraut. Anhand praktischer Beispiele lernen Sie die Best Practices in jedem Stadium der Softwareentwicklung kennen.

Inhalte des Seminars

Tag 1
- Übersicht über die Entwicklung sicherer Software
- Vorgehensmodelle
- Reifegradmodelle und Standards
- Risiko- und Anforderungsanalyse
- Workshop Requirements: Strukturanalyse mit DFD, Bedrohungsanalyse mit STRIDE, Risk Modeling, Requirements Specification
- Secure Design: Prinzipien und Entwurfsmuster

Tag 2
- Sichere Implementierung: Angriffsflächen am Beispiel Automotive
- Typische Implementierungsschwachstellen und Gegenmaßnahmen
- Seitenkanalangriffe
- Workshop Implementierung: Finden und Vermeiden von Programmierfehlern
- Testen von Schutzkonzepten

Ihr Nutzen

- Nach dem Seminar können Sie Sicherheitsbelange in allen Stadien der Softwareentwicklung berücksichtigen.
- Sie können wichtige Bedrohungen für sichere Software einschätzen und abwehren.
- Sie wissen, wie Sie wesentliche Sicherheitslücken in Software vermeiden, aufspüren und beseitigen.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Maschinelles Lernen für mehr Sicherheit

Mit ML unbekannte Angriffe erkennen!

Die Herausforderung: Sicherheitslösungen skalieren bei zunehmenden Datenmengen nicht. In der Cybersicherheit fallen, wie in vielen anderen Bereichen auch, immer mehr Daten an, die es zu analysieren gibt, z. B. Log-Dateien oder Mitschnitte von Netzwerkverkehr. Diese Daten von Menschen analysieren zu lassen, skaliert nicht. Auch signaturbasierte Analysetools lösen dieses Problem nicht, da sie sich auf Signaturen verlassen, die wiederum von Menschen erstellt werden – was auch die Erkennung von unbekannten Angriffen (Zero-Days) einschränkt. Die Folge: Nur, was in den Signaturen abgedeckt ist, kann (unter kostspieligem Einsatz von Experten) überhaupt erkannt werden.

Inhalte des Seminars

Überblick über die Schnittmenge von Cybersicherheit und maschinellem Lernen

Datengewinnung und Preprocessing mit Fokus auf Cyber-Security-Daten

Grundlegende Prinzipien ML: Konzepte und Algorithmen

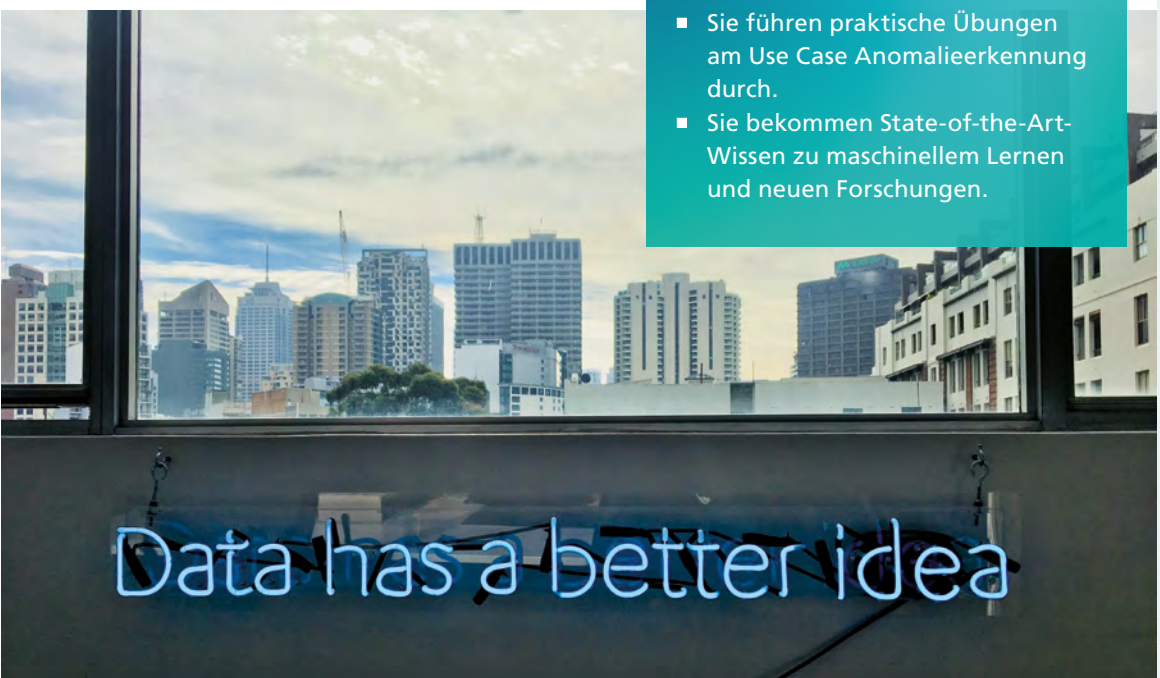
Use Case: Anomalieerkennung

Praktische Hinweise/Tools/Hilfestellung bei der Erstellung eigener ML-Systeme

Ausblick & State of the Art, z.B. Adversarial Machine Learning

Ihr Nutzen

- Nach dem Seminar können Sie einschätzen, in welchen Bereichen Sie maschinelles Lernen sinnvoll einsetzen können.
- Sie können Programmierungen und Modellierungen zur Anomalieerkennung vornehmen.
- Sie bekommen einen Einstieg in die Themen der Cybersicherheit, bei welchen maschinelles Lernen relevant ist.
- Sie führen praktische Übungen am Use Case Anomalieerkennung durch.
- Sie bekommen State-of-the-Art-Wissen zu maschinellem Lernen und neuen Forschungen.



Informationen im Überblick

Basiswissen zu Programmierung, IT-Sicherheit und maschinellem Lernen

Sicherheitsingenieur*innen, Analyst*innen der IT-Sicherheit, Entwickler*innen sicherer Systeme/Software

1 Tag

600,–

Garching bei München oder online

Veranstaltet durch

Fraunhofer AISEC

Referenten:

Nicolas Müller, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/maschinelles-lernen

</> Entwicklung und Testing sicherer Software
Präsenz

Informationen im Überblick

Basiswissen Linux: Routinierter Umgang mit der Bourne-Again Shell (BASH) und GNU Debugger (GDB); Programmierkenntnisse: Flüssiges Lesen und Verstehen von C-Code; Programmiererfahrung mit C oder Python Assembler: x86_64 Assembler lesen und verstehen.

Mitarbeitende, die bei Entwicklung, Testen, Betreiben oder Anwendung das Vorgehen eines Hackers kennenlernen wollen, um mithilfe dieser Erkenntnisse die Sicherheit ihrer Systeme zu verbessern.

3 Tage Präsenz

1800,–

Weiden in der Oberpfalz

Veranstaltet durch

Fraunhofer AISEC

Referent:

Tilo Fischer, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/binary-exploitation

Hacking: Binary Exploitation

Buffer Overflows und deren Folgen

Die Herausforderung: Neue Angriffsszenarien im Zuge steigender Vernetzung. Unternehmen müssen heutzutage ihre Systeme in adäquater Weise absichern. Trotz vorhandener Schutzmechanismen, wie z. B. durch nicht ausführbare Speicherregionen, Randomisierung von Adressen oder durch den Compiler eingefügte Stack Cookies, werden Schwachstellen in Anwendungen dennoch erfolgreich ausgenutzt. In diesem Seminar lernen Sie, wie Sie sich auf derartige Angriffe vorbereiten. Gerade der Bereich Binary Exploitation steht dabei im Fokus. Geben Sie Hackern keine Chance!

Inhalte des Seminars

Tag 1
- Grundlagen Buffer Overflows, Debugging, Dissassembler
- Praktische Übung: Debuggen und Reverse Engineering
- Einführung in die Thematik des Stacks
- Praktische Übung: Erster Exploit ohne Schutzmaßnahmen

Tag 2
- Schutzmaßnahmen durch Compiler
- Praktische Übung: Exploit mit Compilerschutzmaßnahmen
- Schutzmaßnahmen durch System
- Praktische Übung: Exploit mit Systemschutzmaßnahmen

Tag 3
- Einführung in die Thematik des Heaps
- Praktische Übung: Exploit ohne Schutzmaßnahmen
- Praktische Übung: Exploit mit Schutzmaßnahmen (optional)

Ihr Nutzen

- Nach dem Seminar können Sie das Vorgehen eines Hackers nachvollziehen und Exploits zum Aufzeigen der Schwachstelle entwickeln.
- Sie kennen typische Programmierfehler in C-Code und die Grenzen der Schutzmechanismen.
- Sie können die Anwendbarkeit der Schutzmechanismen für die eigene Entwicklung einschätzen.

Hacking: Pentesting

IT-Sicherheit aus der Perspektive des Angreifers prüfen

Die Herausforderung: Viele Unternehmen verlieren beim Prozess der Digitalisierung ihres Unternehmens schlicht den Überblick über die Sicherheit ihrer Systeme oder vernachlässigen diesen Aspekt bei der Umsetzung von Softwareprojekten. Penetrationstests können dabei helfen, eigene Schwachstellen aufzudecken! Dieses Seminar ist der perfekte Einstieg für künftige Penetrationstester. Es ermöglicht Ihnen aus Angreifersicht, d. h. mit Hackingmethoden, Ihr System auf Herz und Nieren zu prüfen. Legen Sie los!

Inhalte des Seminars

Tag 1
Test vorbereiten: Penetrationstest definieren Sammeln von Zielinformationen
- Google Hacking
- Portscanner
- Praktische Übung: Netzwerk analysieren
- Schwachstellen-Scanner
- Praktische Übung: Schwachstellen finden

Tag 2
Risikoanalyse
- Risikomatrix erstellen und evaluieren

Ausnutzen von Schwachstellen
- Schwachstellen ausnutzen mithilfe von Exploit
- Praktische Übung: Schwachstellen ausnutzen
- Angriffe auf schwache Authentifizierung
- Praktische Übung: Passwort knacken

Tag 3
- Weiterführende Angriffe: Lokale Exploits und Backdoors
- Praktische Übung: Rechteausweitung
- Ausblick auf Angriffe im Zielnetzwerk

Ihr Nutzen

- Nach dem Seminar können Sie die Perspektive eines Hackers einnehmen.
- Sie können sicherheitsrelevante Schwachstellen von Software aufdecken und analysieren.
- Sie können Risiken abwägen und richtig einschätzen.

</> Entwicklung und Testing sicherer Software
Präsenz

Informationen im Überblick

Grundlegendes Wissen über Netzwerkprotokolle: basale Funktionen geläufiger Protokolle wie imap, pop3, ssh, http usw. kennen. Grundlegende Begriffe aus dem Bereich IT-Sicherheit verstehen und einordnen können, Grundlegendes Wissen in Linux

Netzwerkadministrator*innen, Sicherheitsbeauftragte, Softwareentwickler*innen, die die Perspektive eines Hackers einnehmen möchten, um dadurch die Schwachstellen und deren Risiken besser einschätzen zu können

3 Tage Präsenz

1800,–

Weiden in der Oberpfalz

Veranstaltet durch
Fraunhofer AISEC

Referent:

Tilo Fischer,
wiss. Mitarbeiter
Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/pentesting

Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundlegende Erfahrungen im Bereich Softwareentwicklung, Flüssiges Lesen von C-Codes

Softwareentwickler*innen, Softwarearchitekt*innen, -planer*innen und -designer*innen

2 Tage

1200,–

Weiden in der Oberpfalz oder online

Veranstaltet durch

Fraunhofer AISEC

Referent:

Tilo Fischer,
wiss. Mitarbeiter
Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicheres-implementieren-c-online

Sicheres Implementieren und Testen in C

Softwareprodukte sicher entwickeln

Die Herausforderung: Wie kann man Software sicher entwickeln? Softwareentwicklung kann im Hinblick auf Sicherheitsaspekte problematisch sein: Jeder Schritt im Entwicklungszyklus muss beachtet werden! Dieses Seminar vermittelt sichere Methoden zur Softwareentwicklung. Zudem auch einen Einblick in die Vor- und Nachteile, die beim Implementieren von C auftreten können.

Inhalte des Seminars

Security Requirements Engineering

Sicheres Softwaredesign

Sicherheitsrelevante Probleme in der Implementierung von Software in C

Praktische Übungen im Hackinglabor

Software auf Schwachstellen testen

Ihr Nutzen

- Nach dem Seminar können Sie einschätzen, welche Techniken notwendig sind, um ein sicheres Softwareprodukt in C zu entwickeln.
- Sie können sicherheitskritische Fehler in der Software erkennen.
- Sie wissen, wie Sie Testmaßnahmen einführen, um die Softwaresicherheit zu erhöhen.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Post-Quanten-Sicherheit

Trends und Entwicklung der modernen Kryptographie

Die Herausforderung: Quantencomputer brechen viele der heute gängigen Verfahren der IT-Sicherheit. Die IT-Sicherheit adressiert heutzutage Aufgabenstellungen, die von einem gewöhnlichen Computer nicht oder nur mit unverhältnismäßig großem Aufwand gelöst werden können. Wie kann IT-Sicherheit jedoch zukunftsfest gestaltet werden? Der Kurs bietet einen Einstieg in die Technologie der Quantencomputer. Lernen Sie, wie Sie Gefahren besser abschätzen und wie sich quantenresistente Verfahren entwickeln lassen.

Inhalte des Seminars

Funktionsweise eines Quantencomputers

Quantengatter und einfache Quanten-Algorithmen mit Hands-on-Simulationen

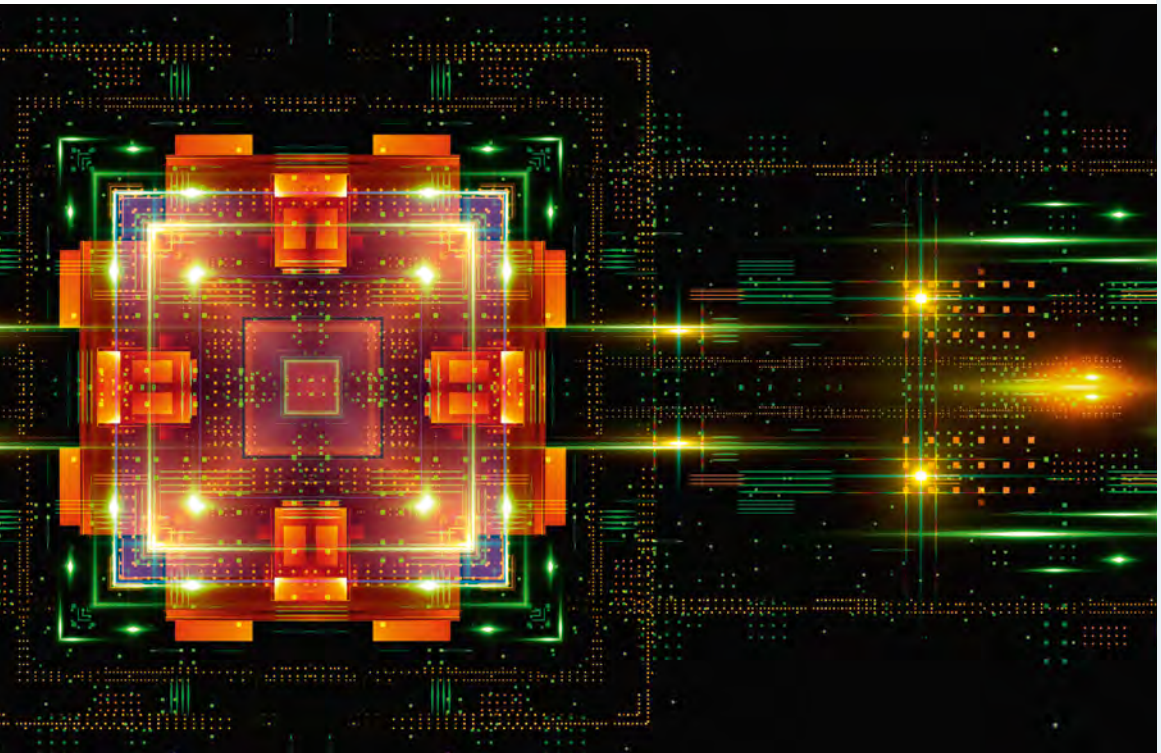
Die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie

Einführung in Post-Quanten-Kryptographie, praxisnahe Übungen zu dem Thema

Die laufende Standardisierung der NIST

Ihr Nutzen

- Nach dem Seminar können Sie die Funktionsweise eines Quantencomputers nachvollziehen.
- Sie können Quantengatter und einfache Quanten-Algorithmen programmieren.
- Sie wissen, wie man die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie abschätzt.
- Sie können Post-Quanten-Kryptographie anwenden.



Informationen im Überblick

Grundlegende Kenntnisse in IT-Sicherheit und Kryptographie von Vorteil, aber nicht zwingend

Administrator*innen, die schon heute ihre IT-Infrastruktur post-quantensicher machen wollen, Anwendende von IT-Sicherheit, die verstehen wollen, wie sich die IT-Sicherheit in den nächsten Jahren entwickelt, Fachkräfte und Spezialist*innen aus der Hochsicherheitsindustrie

2 Tage

1200,–

Weiden in der Oberpfalz oder online

Veranstaltet durch

Fraunhofer AISEC

Referent:

Prof. Dr. Daniel Loebenberger, Leiter der Forschungsgruppe Secure Infrastructure Fraunhofer AISEC / OTH Amberg-Weiden

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/post-quanten-sicherheit

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundlagen in Computerarchitektur und Netzwerke, Kenntnis einer Programmiersprache

Administrator*innen und Entwickler*innen, die sich mit dem Einsatz und der Konfiguration kryptographischer Methoden befassen

1 Tag

600,–

Weiden in der Oberpfalz oder online

Veranstaltet durch

Fraunhofer AISEC

Referenten:

Prof. Dr. Daniel Loebenberger, Leiter der Forschungsgruppe Secure Infrastructure Fraunhofer AISEC / OTH Amberg-Weiden

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/kryptographische-protokolle

Kryptographische Protokolle und deren Anwendung

Gängige verfahren im Praxiseinsatz

Die Herausforderung: Kryptographische Verfahren in der Praxis nutzen. Welche Verfahren entsprechen dem aktuellen Technikstand? Welche Parameter benötigt man für welches Verfahren, und wie wirken sie im Zusammenspiel? Solche Fragen treten bei der praktischen Anwendung Kryptographischer Verfahren immer wieder auf. Dieser Kurs stellt eine kurze Einleitung in die praktischen Anwendungsmöglichkeiten der Kryptographie und deren Umsetzung dar. Lernen Sie, selbstsicher mit kryptographischen Verfahren umzugehen.

Inhalte des Seminars

Überblick symmetrische Verfahren

Überblick Public-Key-Kryptographie

Bewertung des Sicherheitslevels kryptographischer Verfahren

Gängige Schlüssellängen und andere Sicherheitsparameter

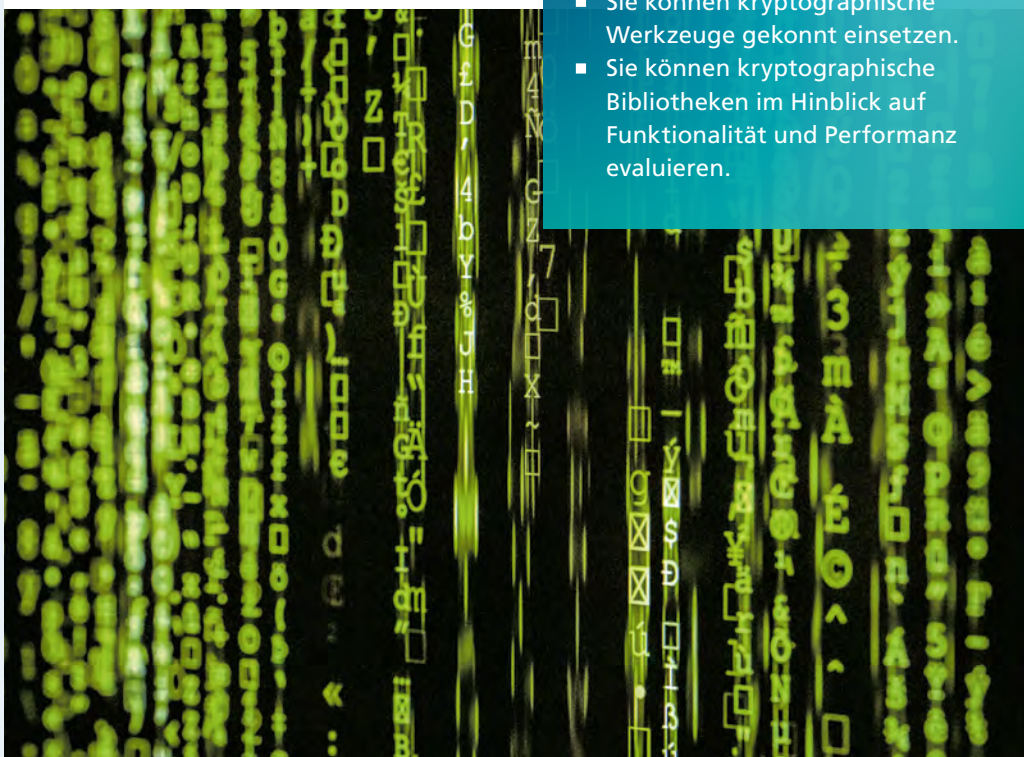
Nützliche nationale Standards

Internationale Normierung

Kryptographische Bibliotheken

Ihr Nutzen

- Nach dem Seminar können Sie kryptographische Protokolle auf ihre Sicherheit hin bewerten.
- Sie können kryptographische Parameter sicher einschätzen.
- Sie können den Einsatz von nationalen und internationalen Standards kryptographischer Funktionen beurteilen.
- Sie können kryptographische Werkzeuge gekonnt einsetzen.
- Sie können kryptographische Bibliotheken im Hinblick auf Funktionalität und Performanz evaluieren.



Blockchain: Einsatzmöglichkeiten und Anwendungen

Funktionsweise verstehen und anwenden

Die Herausforderung: Entwicklung, Chancen und Risiken von Blockchain richtig einschätzen. Mit Einführung der Kryptowährung Bitcoin wurden im Bereich Blockchain schlagartig neue Technologien entwickelt, die sowohl das Interesse von Start-ups als auch von etablierten Unternehmen geweckt haben. Doch das Erkennen und Verstehen von Forschungszusammenhängen oder Hacks der Blockchain Start-ups fällt sogar Fachleuten schwer! Der Kurs gibt einen Einblick in die Welt von Blockchain und vermittelt die Funktionsweise von Bitcoin. Praktische Übungen unterstützen das Verständnis.

Inhalte des Seminars

Grundlagen der Blockchain-Technologie und zugrunde liegenden Kryptographie
- Überblick zur Blockchain und den Plattformen
- Einblick in aktuelle Anwendungsfälle
- Die Entwicklung der Blockchain: Bitcoin
- Transaktionen
- Adressen & Wallets
- Public-Key-Kryptographie & Hashfunktionen

Konsens
- Blöcke (Double-Spending-Problem & Konsens)
- Forking (Proof-of-Work, Proof-of-Stake und alternative Konsensalgorithmen)
- Smart Contracts
- Scripting, Mining, Privacy

Praxis
- Ethereum: Detailansicht & Praxis
- Multichain: Detailansicht & Praxis

Ihr Nutzen

- Nach dem Seminar können Sie Einsatzmöglichkeiten von Blockchain einschätzen.
- Sie können Probleme, welche sich effizient mit Blockchain lösen lassen, von unergiebigen Blockchain-Applikationen unterscheiden.
- Sie können selbst erste Erfahrungen im Programmieren von Smart Contracts sammeln.
- Sie können einen Bitcoin-Client bedienen.

</> Entwicklung und Testing sicherer Software
Präsenz | Online

Informationen im Überblick

Grundlegende Kenntnisse im Bereich IT-Sicherheit und einer Programmiersprache; Mathematikkenntnisse über Schulniveau hinaus sind nicht erforderlich

Administrator*innen, Entwickler*innen, Testende, Betreiber*innen oder Anwendende, die Blockchain-Technologien konfigurieren oder einsetzen

2 Tage

1200,–

Weiden in der Oberpfalz oder online

Veranstaltet durch
Fraunhofer AISEC

Referenten:

Prof. Dr. Daniel Loebenberger, Leiter der Forschungsgruppe Secure Infrastructure Fraunhofer AISEC / OTH Amberg-Weiden

Tilo Fischer, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/blockchain

</> Entwicklung und Testing sicherer Software
Präsenz

Informationen im Überblick

Verständnis von einfachen Programmierkonzepten (z.B. Variablen, Schleifen)

Entwickler*innen, Beratende, Testende, IT-Leiter*innen mit fachlichem Verständnis

1 Tag Präsenz

600,–

Bonn

Veranstaltet durch

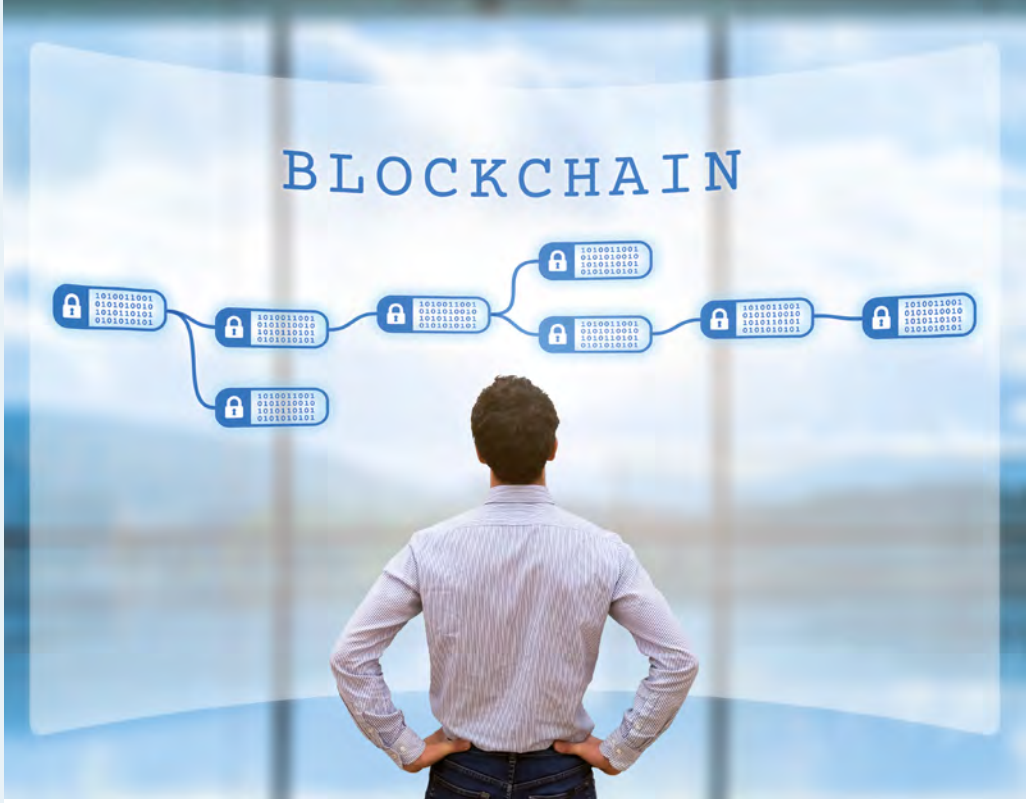
Fraunhofer FKIE

Referent:

Dr. Michael Rademacher, IT-Sicherheitsforscher, Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/blockchain-technologie



Blockchain-Technologie

Schnelleinstieg in die Funktionsweise und Bausteine

Die Herausforderung: Flexible und sichere FPGA-Systeme (Field Programmable Gate Array) bauen. Rekonfigurierbare Hardware-Bausteine, sogenannte FPGAs, ermöglichen die Beschleunigung von Netzwerkfunktionen. Ihre Programmierbarkeit erlaubt neue Flexibilität. Ein Vorteil, der auch Angriffsmöglichkeiten bietet. Für die IT-Sicherheit zeigt das: Es braucht ein hohes Maß an Erfahrungswissen. Dieses Seminar stattet Sie damit aus. In einem Vorgespräch lassen sich die Inhalte des Seminars deshalb unternehmensspezifisch anpassen.

Inhalte des Seminars

Theorie
- Evolution der Blockchain
- Public, Private und Federated Blockchains
- Hashfunktionen, Signaturen und Asymmetrische Kryptographie
- Peer-to-Peer-Netzwerke
- CAP-Theorem und byzantinischer Fehler
- Übertragung digitaler Werte
- Konsensmechanismen (z.B. Proof-of-Work)
- Mögliche Anwendungsgebiete

Praxis
- Hashfunktionen
- Signaturen
- Proof-of-Work-Konsens

Ihr Nutzen

- Sie lernen, Anwendungsgebiete der Blockchain-Technologie einzuschätzen.
- Sie können mit praxisnahen Übungen zum Thema Hashing, Signaturen und Proof-of-Work die Funktionsweise der Technologie nachvollziehen.
- Sie erhalten eine verständliche Herleitung der wichtigsten Innovationen der Blockchain-Technologie.

</> Entwicklung und Testing sicherer Software
Online

Security Champion Training

Security im Unternehmensalltag etablieren

Die Security-Anforderungen an Softwareprodukte steigen stetig, da sie zunehmend mehr schützenswerte Daten verarbeiten und immer häufiger kritische Dienste bereitstellen. Mit unserem Training qualifizieren wir Sie zum Security Champion, wodurch Sie eine Vielzahl an Methoden, Werkzeugen und Softskills erler-nen, um die Sicherheit Ihrer Produkte gewährleisten zu können. Das Training ist verteilt auf 13 Wochen und umfasst sequenzielle Trainingsmodule mit dazwischenliegenden Praxisphasen. In der abschließenden Prüfung bestätigen Sie Ihren Lernerfolg.

Inhalte des Seminars

Einführung
- Bedeutung von Security anhand von Praxisbeispielen
- Terminologie, Abgrenzung und Trends
- Rolle und Aufgaben eines Security Champions

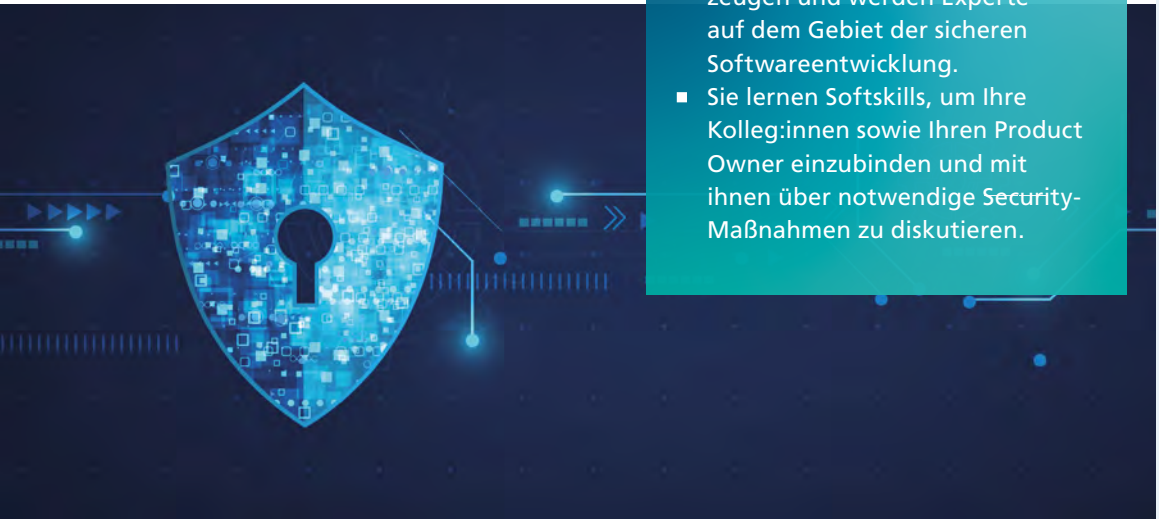
Anforderungs- und Risikoanalyse
- Security gewährleisten im agilen Entwicklungsprozess
- Definition von Security-Anforderungen
- Klassifikation von Risiken und Risikobehandlung
- Security-Gesetze und -Normen

Effektive Methoden und Werkzeuge für die Entwicklung
- Prinzipien und Muster für einen sicheren Entwurf
- Richtlinien zum sicheren Programmieren
- Kryptographie: Sichere Speicherung und Übertragung von Daten
- Automatische und manuelle Code Reviews
- DevSecOps: Maßnahmen zum sicheren Betrieb der Software

Security Champion in der Praxis
- Workshops durchführen, das Team methodisch beraten und Veränderungen aktiv gestalten
- Softskills, um der Rolle gerecht zu werden: Fragetechniken, Kommunikationsmodelle und Konfliktmanagement
- Praxisphasen zwischen den Sessions zur Vertiefung der Inhalte und den Transfer auf das eigene Projekt

Ihr Nutzen

- Nach dem Training sind Sie in der Lage, das Thema Security bei der Entwicklung Ihrer Softwareprodukte umfassend zu berücksichtigen.
- Sie beherrschen eine Vielzahl von Security-Methoden und Werkzeugen und werden Experte auf dem Gebiet der sicheren Softwareentwicklung.
- Sie lernen Softskills, um Ihre Kolleg:innen sowie Ihren Product Owner einzubinden und mit ihnen über notwendige Security-Maßnahmen zu diskutieren.



Informationen im Überblick

Eine Ausbildung oder Hochschulstudium in Informatik, Wirtschaftsinformatik oder vergleichbaren Fachrichtungen, Grundkenntnisse in Java

Softwareentwickler*innen

13 Wochen in Teilzeit (ca. 98 Stunden), Live-Online-Sessions jeweils von 08:30 – 12:30 Uhr

4900,–

online

Veranstaltet durch

Fraunhofer IEM

Referenten:

Dr. Stefan Dziwok, Senior Researcher am Fraunhofer IEM

Thorsten Koch, Wissenschaftlicher Mitarbeiter am Fraunhofer IEM

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/security-champion-training

Informationen im Überblick

Keine Voraussetzungen

Product Owner, Produktmanager*innen

6 Wochen in Teilzeit (ca. 20 Stunden insgesamt), Live-Online-Sessions jeweils von 08:30 – 12:30 Uhr

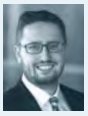
1950,–

online

Veranstaltet durch

Fraunhofer IEM

Referent:



Dr. Stefan Dziwok, Senior Researcher am Fraunhofer IEM

Thorsten Koch, Wissenschaftlicher Mitarbeiter am Fraunhofer IEM

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/software-security-training-product-owner

Software Security Training für Product Owner

Security in der Produktentwicklung etablieren

In der sicheren Softwareentwicklung nimmt der Product Owner eine zentrale Rolle ein, da er nicht nur für neue Features, sondern auch für die Security des Produktes verantwortlich ist. Doch wie lässt sich Security aus Sicht des Product Owners überhaupt kontinuierlich berücksichtigen? Dieser Kurs zeigt Ihnen, wie Sie eine Umgebung schaffen, in der ein Team Freude hat, neue Werkzeuge und Methoden zu kombinieren, um flexibler, schneller und sicherer Produkte zu entwickeln.

Inhalte des Seminars

Einführung & Sensibilisierung
- Sensibilisierung für Software Security anhand aktueller Studien, Trends, Praxisbeispielen und Live-Hacking

Rollenverständnis
- Rolle und Aufgaben des Product Owners bzgl. Software-Security

Software-Security Grundlagen
- Terminologie, Schutzziele und Bedrohungsarten

Risikomanagement
- Relevante Security-Gesetze und Normen
- Definition von Security-Anforderungen
- Risikoanalyse und Risikobehandlung

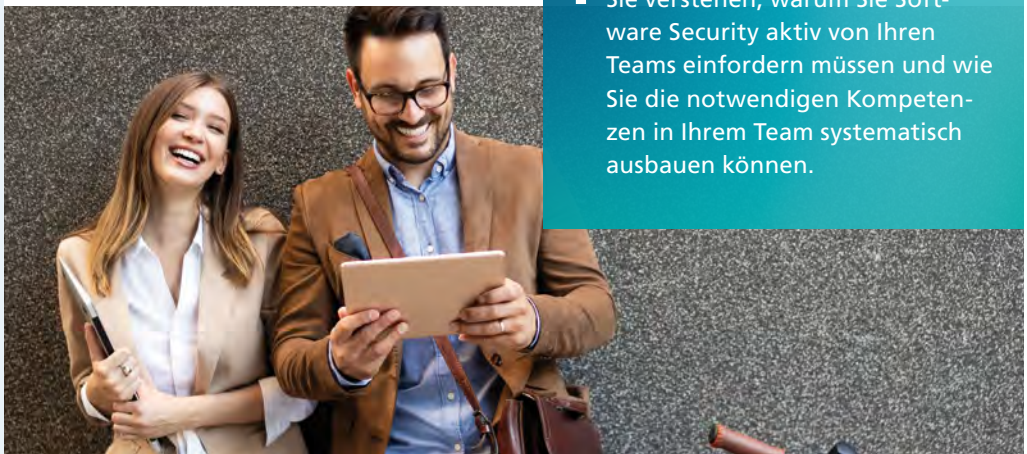
Product Security Incident Response
- Schwachstellen und Angriffe erkennen und gezielt darauf reagieren
- Etablierung eines Product Security Incident Response Teams (PSIRT)

Software-Security etablieren
- Security Champions im Team etablieren
- Systematische Steigerung der Security-Kompetenzen im Team
- Warum ein Invest für Security auch eine Chance ist

Coaching-on-the-Job
- Anwendung der Trainingsinhalte auf das eigene Produkt
- Reflexion der gewonnenen Erkenntnisse mit dem eigenen Team, z.B. Durchführung einer Retro bzgl. Awareness und Kompetenz
- Abschließende Individuelle Reflexion mit den TrainerInnen

Ihr Nutzen

- Sie verstehen, warum sie als Product Owner aktiv handeln müssen.
- Sie lernen Ihre Rolle (Verantwortung und Aufgaben) bezüglich Software Security kennen und erlernen die zur Ausführung notwendigen Kompetenzen.
- Sie verstehen, warum Sie Software Security aktiv von Ihren Teams einfordern müssen und wie Sie die notwendigen Kompetenzen in Ihrem Team systematisch ausbauen können.



Software Security Training für Führungskräfte

Security als Führungsaufgabe

Sicherheitslücken in Softwareprodukten bedrohen in zunehmendem Maße den Unternehmenserfolg. Trotzdem wird die Verantwortung für Sicherheitsvorfälle häufig allein bei den Entwickler*innen gesehen. Dabei können insbesondere Führungskräfte Security aktiv angehen und in ihrem Verantwortungsbereich systematisch verankern. In diesem Seminar lernen Führungskräfte, wie sie Bedingungen schaffen, die eine sichere Softwareentwicklung ermöglichen und fördern. Sie werden befähigt Risiken zu erkennen und geeignete Maßnahmen im Entwicklungsumfeld einzuleiten.

Inhalte des Seminars

- Sensibilisierung für das Thema Software Security
- Software Security Grundlagen (Terminologie, Schutzziele etc.), Gesetze und Normen, Stakeholder-Management
- Risikoanalyse
- Bereichsentwicklung (u.a. der Kompetenzaufbau ihrer Mitarbeitenden)
- Anwendung in der Praxis via eines Coaching-on-the-Job

Ihr Nutzen

- Nach dem Seminar können Sie die Bedeutung und die Auswirkungen von sicherheitskritischen Vorfällen besser einschätzen.
- Sie können verschiedene Aspekte von Software Security erläutern und sich mit relevanten Stakeholder-Gruppen darüber austauschen.
- Sie sind in der Lage den Ist-Stand in ihrem Bereich zu erfassen und Risiken anhand von verschiedenen Kriterien zu analysieren.
- Sie kennen verschiedene Handlungsoptionen und können konkrete Maßnahmen ergreifen, welche die Software Security steigern.

</> Entwicklung und Testing sicherer Software
Online

Informationen im Überblick

Keine Voraussetzungen

Führungskräfte (insb. von Product Ownern und Entwicklungsteams)

7 Wochen in Teilzeit (ca. 23 Stunden), Live-Online-Sessions jeweils von 08:30 – 12:30 Uhr

2100,–

online

Veranstaltet durch

Fraunhofer IEM

Referenten:

Dr. Stefan Dziwok, Senior Researcher am Fraunhofer IEM

Dr. Matthias Becker Abteilungsleiter am Fraunhofer IEM

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/software_securitytraining_führungskräfte

Produktzertifizierung

Produkte zertifizieren? – Aber bitte!

Das breite Angebot an Produkten erschwert es Kaufenden, die richtige Wahl zu treffen. Deshalb sind verlässliche Anhaltspunkte gefragt, die den potenziellen Kundenkreis informieren und die Auswahl erleichtern.

Zertifizierungen sind mehr als nur Labels. Sie sind notwendig, um Märkte zu strukturieren und zu ordnen. Sie schaffen einheitliche Standards, die von Inhabern des Zertifikats gemeinsam getragen werden. Ziel ist es, ein hohes Maß an Qualität der Produkte zu bestätigen, Leistungsfähigkeit sicherzustellen und, daraus resultierend, einen sicheren Raum zu schaffen, der potenzieller Kundschaft Vertrauen bietet. Doch auch aufseiten der herstellenden Unternehmen können sich Türen zu geregelten Märkten öffnen.

Der Weg zur Zertifizierung ist jedoch nicht immer leicht zu bewältigen. Die Auswahl der passenden Zertifizierung sowie das Abwägen von Kosten-Nutzen-Faktoren können so einige Stolpersteine bereithalten. Schaffen Sie sich daher einen Überblick und besuchen Sie einen der angebotenen Kurse des Lernlabors Cybersicherheit!

In diesen lernen Sie nachzuvollziehen, wie einzelne Zertifizierungen aufgebaut sind, und was Sie beachten sollten. Erfahren Sie, welchen Nutzen, aber auch welche Risiken hinter einer Zertifizierung stehen können. Im Lernlabor können Sie von der wissenschaftlichen Expertise der Mitarbeitenden profitieren und so ihre Produkte zukunftssicher machen.

Zertifikate sind mehr als nur Labels. Sie schaffen Vertrauen und Vergleichbarkeit durch einheitliche Standards bzgl. Funktionalität, Qualität und Sicherheit zertifizierter Produkte.

International Data Space Komponentenzertifizierung

Ist mein Produkt IDS-Ready?

Um Daten als Wirtschaftsgut nutzen zu können, ist ein geregelter und sicherer unternehmensübergreifender Datenaustausch notwendig. Die Initiative International Data Space zielt darauf ab, einen sicheren Datenraum zu schaffen, der Unternehmen verschiedener Branchen und aller Größen die souveräne Bewirtschaftung ihrer Datengüter ermöglicht. Im IDS sollen Daten sicher ausgetauscht und mit Nutzungsrestriktionen versehen werden. Die Akzeptanz des IDS im Kontext des Austauschs unternehmenskritischer Daten ist zu gewährleisten. Um dieses Ziel zu erreichen, fällt dem Prozess der Zertifizierung eine zentrale Rolle zu.

Inhalte des Seminars

Modul 0 (2 Stunden als vorbereitende Websession)
- Klärung der Komplexität und der Reife des Produkts
- Ziel: Inhalt und Umfang des Workshops festlegen

Modul I (1 Tag)
- Vorstellung des IDS-Zertifizierungsschemas
- Gemeinsamkeiten und Unterschiede IDS-Zertifizierung und 62443-4-2
- Übersicht Kriterienkatalog
- Produktvorstellung (Kunde)

Modul II (1–3 Tage, nach Bedarf)
- Besprechung der Kriterien
- IDS-spezifische Kriterien
- 62443-4-2-Kriterien
- Entwicklungsspezifische Kriterien

Modul III
- Zusammenfassung der Ergebnisse
- Next Steps für die IDS-Zertifizierung

Ihr Nutzen

- Nach dem Workshop besitzen Sie ein Verständnis von den Komponenten im IDS auf technischer Ebene.
- Sie können die Zertifizierbarkeit des eigenen Produkts beurteilen.
- Sie können Vorteile, Nutzen und Risiken einer IDS-Zertifizierung bewerten.
- Sie können den Aufwand einer IDS-Zertifizierung für das eigene Produkt einschätzen.
- Der Workshop bietet Ihnen eine Entscheidungsgrundlage für die IDS-Zertifizierung Ihres Produkts und eine Einschätzung des Abdeckungsgrades der bereits vorhandenen Kriterien.
- Sie erarbeiten eine konkrete Roadmap mit den noch nötigen Schritten zur IDS-Zertifizierung Ihres Produkts.

Produktzertifizierung | Präsenz | Online

Informationen im Überblick

Kenntnisse des Referenzarchitekturmodells IDS, idealerweise Mitglied im IDSA

Unternehmen: Herstellende von IDS-Komponenten; Teilnehmende: Techniker*innen, Entwickler*innen, Product Owner

3–5 Tage (abhängig vom Produkt), Präsenz oder online

nach Vereinbarung

Berlin od. Garching bei München, inhouse oder online

Veranstaltet durch

Fraunhofer FOKUS

Referent*innen:

Nadja Menz, Gruppenleiterin Fraunhofer FOKUS

Sascha Wessel, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/ids-komponentenzertifizierung

Informationen im Überblick

Keine Voraussetzungen

Produktmanager*innen, Projektleiter*innen, Produktentwickler*innen, technische Einkäufer*innen für Sicherheitsprodukte

1 Tag Präsenz

600,–

Berlin

Veranstaltet durch

Fraunhofer FOKUS

Referent*innen:

Nadja Menz, Gruppenleiterin Fraunhofer FOKUS

Thilo Ernst, wiss. Mitarbeiter Fraunhofer FOKUS

Jaroslav Svacina, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheitszertifizierung-produkte

Sicherheitszertifizierung von Produkten

Den ersten Schritt wagen!

Die Auswahl der passenden Zertifizierung ist nicht immer einfach. Risiken und Vorteilen müssen gegeneinander abgewägt werden. Wenn Sie mit dem Gedanken spielen, eine Common-Criteria-Zertifizierung (CC) zu erwerben, dann bietet dieses Seminar die geeignete Grundlage. Sie lernen die Kernkonzepte kennen und erfahren, wie CC auf Ihrem Produktportfolio anwendbar wäre. Profitieren Sie von den (Wettbewerbs-)Vorteilen, die eine CC-Zertifizierung Ihrem Produkt bietet.

Inhalte des Seminars

Überblick zur Produktzertifizierung
- Prinzip der Zertifizierung: unabhängige Evaluierung, zweite Prüfebene
- Nutzen: Produktqualität, Vertrauenswürdigkeit, Zugang zu regulierten Märkten, Imagevorteile
- Zertifizierungskriterien als dokumentierte Best Practices zum Qualitätsmanagement in der Produktentwicklung

Sicherheitszertifizierung nach Common Criteria
- Fokussierung auf Sicherheitseigenschaften als essenzielles Qualitätsmerkmal
- Vorgeschichte, internationale Standardisierung
- Nationale Schemata und internationale Anerkennung
- Akteure und Arbeitsverteilung in der CC-Zertifizierung
- Konkreter Ablauf des Zertifizierungsverfahrens
- CC-Standarddokumente und Basiskonzepte

Ihr Nutzen

- Nach dem Seminar können Sie das deutsche Zertifizierungsschema des BSI nachvollziehen.
- Sie können die zentralen Konzepte der Common Criteria anwenden.
- Sie lernen, wie man notwendige Aktivitäten auf Herstellerseite abschätzen kann.
- Sie verstehen, die Anwendbarkeit von CC bzgl. Ihres Portfolios abzuschätzen, und können eigens eine CC-Zertifizierung initiieren.

Netzwerksicherheit

Netzwerksicherheit bildet die Basis!

Egal ob im Unternehmensnetz oder im offenen Internet, bei IoT- oder Cloud-Nutzung – die Sicherheit der Netzwerkstruktur gewährleistet die Verfügbarkeit von Daten und deren reibungslose Übertragung. Denn Computernetzwerke bilden die Grundlage für sämtliche digitale Kommunikation. Doch IT-Sicherheit bei Netzwerken gestaltet sich als äußerst komplex und facettenreich. Bei mäßiger Konfiguration können kritische Schwachstellen auftreten, die ein Netzwerk zum leichten Ziel für Angriffe und Manipulationen machen.

Die Vernetzung von IT-Systemen und der Austausch von Daten unter ihnen ist mittlerweile Standard und weder aus dem Privatgebrauch noch aus dem Unternehmensumfeld wegzudenken. Durch die ständig wechselnde Bedrohungslage und die Komplexität der Vernetzungen ist es umso essenzieller, Netzwerksysteme aktuell zu halten und sie zu schützen. Gerade bei Unternehmen spielen IoT- und mobile Geräte eine verstärkte Rolle, was das Risikopotenzial für Angriffe und weitere Bedrohungen deutlich erhöht. Hinzu kommt, dass im Firmennetzwerk oft mit sensiblen Daten gearbeitet wird und Produktionsabläufe von deren Stabilität abhängig sind. Schwachstellen können deshalb ernsthafte Schäden anrichten.

Bestehende Firewalls oder Virenscanner sind oft unzureichend und können so Tür und Tor für unautorisierte Fremde öffnen. Eine unzureichende Verschlüsselung macht das WLAN-Netz zum Angriffsziel. Sind Fälle wie diese erst mal eingetroffen, können Produktionsdaten ausgelesen, gestört und manipuliert werden!

Im Lernlabor Cybersicherheit werden Sie auf die aktuelle Bedrohungslage anhand wissenschaftlicher Kenntnisse und auf künftige Szenarien vorbereitet. Durch die verschiedenen Kurse erfahren Sie, wie Sie Schwachstellen in Netzwerksystem aufdecken und absichern.

Das Risikopotenzial für Angriffe bei IoT- und mobilen Geräten spielt gerade in Unternehmen eine verstärkte Rolle.

Informationen im Überblick

- Keine Voraussetzungen
- Anwender*innen und Einsteiger*innen
- 1 Tag Präsenz
- 600,–
- Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Dr. Michael Rademacher, IT-Sicherheitsforscher Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/grundl-netzwerksicherheit

IT-Sicherheit – Netzwerksicherheit

Im Handumdrehen Netzwerke sichern

Die Herausforderung: Netzwerkinfrastrukturen sind beliebte Angriffsziele Computernetzwerke bilden das Rückgrat unserer digitalen Infrastruktur: Im Unternehmensnetzwerk, im Heimnetzwerk oder über das Mobilnetz – nahezu jeder Nutzer kommt mit diesem Thema in Berührung. Da unsere gesamte digitale Kommunikation über diese Kanäle verläuft, stellt die Netzwerkinfrastruktur ein lohnendes Ziel für Angreifer dar. Doch wie lassen sich Netzwerke schützen? In diesem Seminar lernen Sie Grundbegriffe der Netzwerksicherheit kennen und verstehen. Indem Sie selbst die Perspektive des Angreifers übernehmen, schärfen Sie Ihr Bewusstsein für Sicherheitslücken und können so präventiv agieren.

Inhalte des Seminars

Kennenlernen der Grundbegriffe der Netzwerksicherheit

Angriffe auf Netzwerkprotokolle

Sichere Kommunikation mit TLS/HTTPS

Sichere Mechanismen für Netzwerke

Werkzeuge der Netzwerkanalyse (Wireshark, Nmap)

WLAN-Sicherheit

Ihr Nutzen

- Sie lernen verschiedene Schwachstellen und Angriffsszenarien in Netzwerken kennen, um Risiken zu identifizieren und diesen entgegenwirken zu können.
- Sie lernen gängige Angriffswerkzeuge kennen.
- Verschiedene Angriffsszenarien und deren effektive Abwehr werden im Training demonstriert und erprobt.

Netzwerksicherheit | **Präsenz**

Netzwerksicherheit Radius, NAC, VPN

Unternehmensnetzwerke brauchen besonderen Schutz

Die Herausforderung: Schutz des Unternehmensnetzwerks vor vielseitigen Bedrohungen durch Angriffe. Gerade in Unternehmen mit unterschiedlichen Niederlassungen und an das Unternehmensnetz angebundenen Außendienstmitarbeitenden besteht das Problem, dass Fremdgeräte mit dem Unternehmensnetzwerk verbunden werden können. Doch was passiert, wenn Datenlecks entstehen? In diesem Seminar lernen Sie, eine sichere Netzwerkinfrastruktur aufzubauen. Dabei kommen NAC-, Radius- und VPN-Lösungen zum Einsatz!

Inhalte des Seminars

Wie legt man berechtigte User/Clients fest?

Wie darf der User/Client im Netz kommunizieren?

Welcher Netzwerkbereich ist für den User/Client erreichbar?

Zu welchen Daten hat der User/Client Zugang?

Wie kann zuverlässige und sichere Kommunikation von extern realisiert werden?

Welche Sicherheitsrisiken sind beim Einsatz von VPN-Systemen relevant, und wie können diese minimiert werden?

Wie müssen Client und Server konfiguriert sein, um eine sichere VPN-Verbindung zu ermöglichen?

Ihr Nutzen

- Nach dem Seminar können Sie Geräte im Netzwerk erkennen und deren Zugriff verwalten.
- Sie wissen, wie man wichtige Konfigurationsfehler vermeidet.
- Sie können VPNs konfigurieren, um Endgeräte anbinden.
- Sie können verbleibende Restrisiken einschätzen und eine Abwägung zwischen Kompatibilität und Sicherheit der eingesetzten Lösungen treffen.

Informationen im Überblick

Grundlagen der IT-Sicherheit, insbesondere Kryptographie: Anwendung von symmetrischer und asymmetrischer Verschlüsselung, Hash-Funktionen. Grundlagen der Computer-Netzwerke: Aufbau, Funktionsweise, Sniffing, Portscans

Admins von KMU im Open-Source-Umfeld, Betreiber*innen von Open-Source-Lösungen

1 Tag Präsenz

600,–

Garching b. München

Veranstaltet durch

Fraunhofer AISEC

Referent:

Sascha Wessel, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/netzwerksicherheit-nac-vpn


Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Energie- & Wasserversorgung und Public Safety
www.cybersicherheit.fraunhofer.de
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
IT-Forensik
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Organisatorische IT-Sicherheit & Datenschutz
www.cybersicherheit.fraunhofer.de
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Embedded Security

Möchten Sie Informationen zu einem anderen Themengebiet?

Hier finden Sie alle Broschüren rund um die Weiterbildungen im Lernlabor Cybersicherheit: www.cybersicherheit.fraunhofer.de/downloads

Inhouse- oder Firmen- und Behördenschulungen

Inhouse-Schulungen individuell auf Sie zugeschnitten

Wollen Sie Inhalte aus unserem Kursangebot individuell zusammenstellen, oder finden Sie in unserem Angebot keinen passenden Termin oder Ort? Kein Problem: Stellen Sie Ihre ganz persönlichen Bedürfnisse in den Vordergrund.

Sie haben die Wahl, so geht's:

- Wählen Sie ein Wunschseminar aus unseren vielfältigen Themen aus und bestimmen Sie den Zeitraum und Schulungsort.
- Nennen Sie uns Inhalte aus unseren Kursangeboten, die geschult werden sollen, und wir konzipieren ein passendes Seminar.
- Sie sagen uns, welches spezielle Wissen geschult werden soll, und wir entwickeln eine individuelle Schulung für Sie.

Bei einem individuellen Inhouse-Seminar erhalten Sie genau auf Ihre Bedürfnisse abgestimmtes Wissen – für Ihr Unternehmen, Abteilungen Ihres Unternehmens, für Ihre Behörde, Fachreferate oder einzelne Mitarbeiterinnen und Mitarbeiter. Dabei stehen wir Ihnen sehr gerne beratend zur Verfügung, wenn es um für Sie maßgeschneiderte, inhaltliche Zusammenstellung der vielfältigen Kombinationsmöglichkeiten unserer Themen geht.

Wir als Lernlabor Cybersicherheit bieten Ihnen alle relevanten Elemente aus einer Hand: Die didaktische, mediale sowie technische Umsetzung der Inhalte, aber auch Konzept und Umsetzung.

Fragen Sie uns an!

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne

telefonisch unter +49 89 1205-1555

e-mail: cybersicherheit@fraunhofer.de

www.cybersicherheit.fraunhofer.de

Hier erhalten Sie aktuelles Wissen!

Aktuelle Informationen zu unseren Seminarangeboten, Veranstaltungen und Themen im Bereich Cybersicherheit finden Sie hier:

www.cybersicherheit.fraunhofer.de

Stöbern Sie in unserem Blog und erfahren Sie, was unsere Fachexpertinnen und -experten über aktuelle Themen im Bereich Cybersicherheit berichten:

www.cybersicherheit.fraunhofer.de/de/blog

Abonnieren Sie unseren Newsletter und bleiben Sie so auf dem Laufenden:

www.cybersicherheit.fraunhofer.de/newsletter

Weitere Informationen rund um das Thema Weiterbildung bei der Fraunhofer Academy erhalten Sie hier:

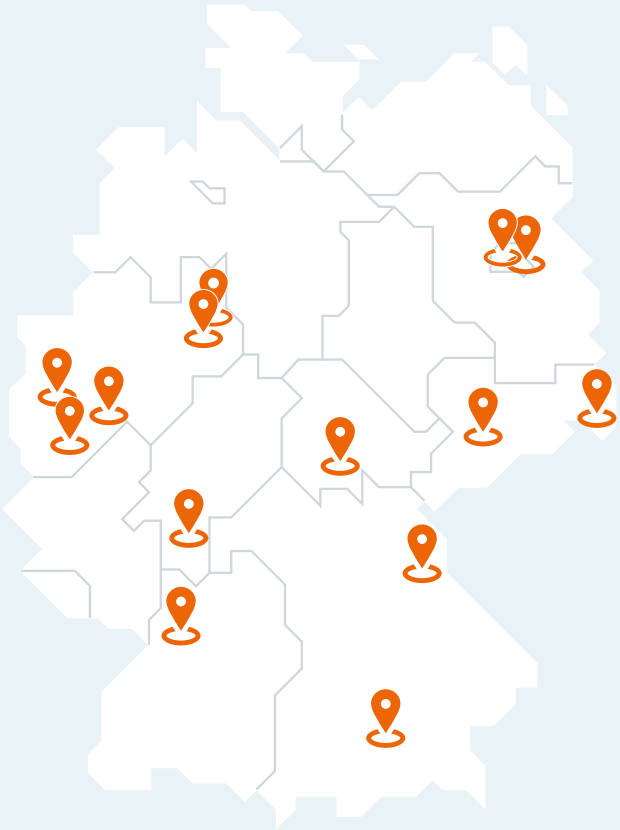
Aktuelle Qualifizierung aus der angewandten Forschung

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 weitergegeben. Die Fraunhofer Academy ist die Geschäftsstelle und 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

- Ostbayerische Technische Hochschule Amberg-Weiden
- Hochschule für Technik und Wirtschaft Berlin
- Hochschule Bonn-Rhein-Sieg
- Hochschule Mittweida
- Hochschule Niederrhein
- Technische 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 IEM
- Fraunhofer IOSB
- Fraunhofer IOSB-AST
- Fraunhofer IOSB-INA
- Fraunhofer SIT

Know-how schafft Sicherheit! Seit 5 Jahren unterstützen wir deshalb Unternehmen auf dem Weg zu mehr IT-Sicherheit.«

Dr. Raphaela Schätz,
Qualitäts- und Programm Management
im Lernlabor Cybersicherheit

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: Elly Leimenstoll

Layout und Satz, Illustrationen:
Vierthaler & Braun

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 Ihrer Organisation aufzubauen.

Adem Salgin

Ihr Ansprechpartner im Lernlabor Cybersicherheit

Seminarberatung
und Anmeldung

Stand September 2022

Sie erreichen uns

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

www.cybersicherheit.fraunhofer.de