Fraunhofer ACADEMY

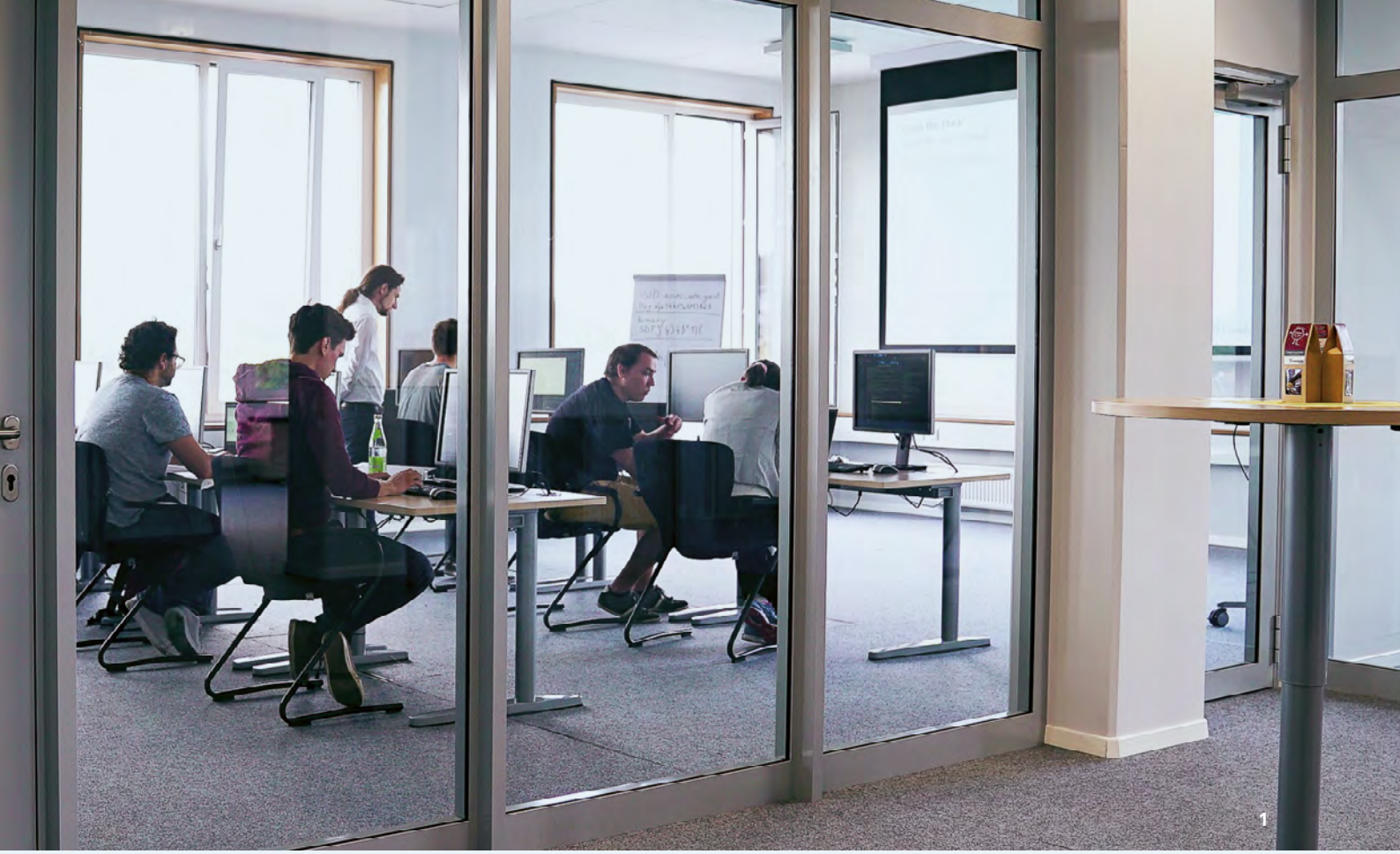
Weiterbildung im
Lernlabor Cybersicherheit

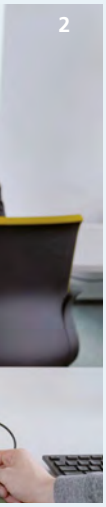
Know-how für mehr IT-Sicherheit

Organisatorische IT-Sicherheit & Datenschutz

www.cybersicherheit.fraunhofer.de

Inhalt





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 Das Hacking-Labor in Weiden bietet in hellen Räumlichkeiten ein mit modernster Technik ausgestattetes Labor direkt am Campus der OTH und ist speziell für Hacking-Schulungen eingerichtet.

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.

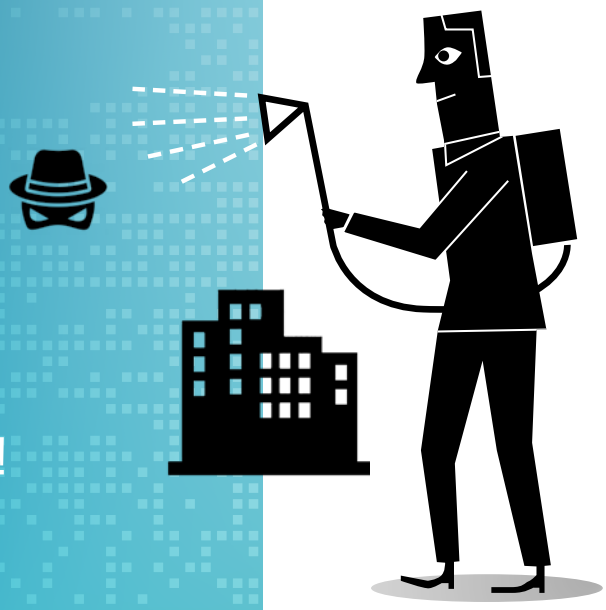
Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

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

Organisatorische IT-Sicherheit



Unternehmen brauchen einen Rundumplan für die IT-Sicherheit!

Betriebe und Unternehmen stehen im Bereich Cybersicherheit vor enormen Herausforderungen. Sei es durch Cyberangriffe, Risikomanagement oder IT-Sicherheit am Arbeitsplatz. Die Vielfalt und Komplexität der einzelnen Problembereiche wächst stetig an.

IT-Sicherheit wird gern und oft auf den technischen Aspekt reduziert. Viele wähnen sich aufgrund einfacher Softwarelösungen in trügerischer Sicherheit. Die Probleme beginnen aber dann, wenn Unternehmen unaufmerksam sind, weil sie die Gefahren durch Hackerangriffe unterschätzen, Mitarbeiter ungeschult sind oder die Führungsebene diesbezüglich unzureichende Richtlinien beschließt und vor gezielten Sicherheitsmaßnahmen zurückschreckt. Dabei könnte mit den nötigen Know-how ein Großteil der Sicherheitsvorfälle vermieden werden.

Gerade durch den gestiegenen Datenverkehr innerhalb des Unternehmens, aber auch zwischen verschiedenen Akteuren, entstehen Sicherheitslücken. Der Einsatz von mobilen Endgeräten und IoT vergrößert die Angriffsfläche, und ein leichtsinniger Umgang mit Daten kann schnell zu Datendiebstahl und -manipulationen führen. Sind diese erst mal eingetreten, ist der Wiederaufbau meist mühselig und mit vielen Kosten verbunden.

Im Lernlabor Cybersicherheit werden Sie auf den Ernstfall vorbereitet. In unseren Kursen können Sie erlernen, welche Sicherheits-strategie für welches Szenario genutzt werden kann. Unsere Expertinnen und Experten helfen Ihnen dabei, das IT-Sicherheitsniveau in ihrem Unternehmen mit geeigneten Maßnahmen zu steigern.

Möchten Unternehmen auch weiterhin effizient und zukunftssicher agieren, braucht es ein solides Management von IT-Sicherheitsfragen auf allen Ebenen!

Organisatorische IT-Sicherheit | **Online**

Cyberangriffe – Aufklärung über moderne Kriminalität

Wie hoch ist die Gefahr wirklich

Unternehmen sind immer häufiger Cyberangriffen ausgeliefert. Dennoch wird das Problem nicht selten unterschätzt. Mit der richtigen Aufklärung über Angriffsarten, Motive und Konsequenzen können die Risiken minimiert werden. Dieses Seminar bereitet Sie auf die ansteigende Bedrohungslage vor, Sie erhalten Wissen in Bezug auf aktuelle IT-Sicherheitsaspekte und -risiken, die in jedem Unternehmen relevant sind. Schützen Sie Ihr Unternehmen vor schweren Folgeschäden!

Inhalte des Seminars

Definition und Kategorisierung
- Der Begriff »Hacking« und dessen Bedeutung
- Technisches Versagen
- Menschliches Versagen
- Organisationsmangel
- Höhere Gewalt

Angreifer und deren Motivation
- White-Hat-, Black-Hat, Grey-Hat-Hacker
- Scriptkiddies
- Hacktivists
- Staatlich gesponserte Hacker
- Spionage-Hacker
- Whistleblower oder Malicious Insiders
- Cyberterroristen

Angriffsarten – Beispiele
- Social Engineering
- Malware, Exploits, Bufferoverflow
- Backdoor, Spyware, Scareware
- Passwörter (Brute Force, Botnetze…)
- Pishing, SPAM und Hoax
- DoS und DDoS

Gefährdete Unternehmen – Beispiele
- KRITIS
- Lebensmittelbranche
- IT-Dienstleister
- Online-Banken
- Unternehmen allgemein

Ihr Nutzen

- Nach dem Seminar können Sie Risiken durch Hackerangriffe und Cyberkriminalität für das Unternehmen richtig einschätzen.
- Sie können konkrete Angriffsarten und die Motive dahinter benennen.
- Sie wissen, wie Sie interne Bedrohungen wie Social Engineering oder technisches Versagen aufdecken und die Mitarbeitenden dahingehend informieren.
- Sie kennen nun die Welt der Hacker und deren Motive.

Informationen im Überblick

keine Vorkenntnisse

Sämtliche Unternehmen, die das Internet nutzen

3 Stunden on Demand-Kurs

199,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/cyberangriffe

Informationen im Überblick

Grundwissen oder vergleichbare Vorkenntnisse in IT-Risikomanagement

IT-Sicherheitsbeauftragte, IT-Risiko-Manager, Business Continuity Manager, CISOs, Krisen-, Risikomanager, Verantwortliche aus den Bereichen Compliance, Corporate Governance und interne/externe Revision, Qualitätsmanager

4 Stunden
on Demand-Kurs

300,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu,
wiss. Mitarbeiter
Fraunhofer FOKUS

Michael Holzhüter,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/it-risikomanagement

IT-Risikomanagement – Risiken erkennen, bewerten und managen

Gefahr erkannt, Gefahr gebannt!

Die Identifizierung, Analyse und Bewertung von Risiken ist nicht immer einfach und erfordert gerade im Bereich IT besonderes Wissen. Zu wissen, welcher Nutzen oder welcher Schaden bei positiven und negativen Fällen entsteht, kann Entscheidungen maßgeblich beeinflussen. Ausschlaggebend ist vor allem eine strukturierte Vorgehensweise, um Informationssicherheitsrisiken richtig abschätzen zu können. Dieses Seminar stattet Sie mit praxiserprobten Methoden im Bereich IT-Risikomanagement aus. Erhöhen Sie die IT-Sicherheitskultur in ihrem Unternehmen!

Inhalte des Seminars

Einführung
- Begriffe, Compliance und Standards
- Ableitung einer IT-Risikostrategie bzw. Informationssicherheitsstrategie
- Standards im IT-Risikomanagement: ISO/IEC-27000-Reihe, ISO 31000, BSI-Risikomanagement-Standard 200-3 etc.

Prozess des IT-Risikomanagements in der Praxis
- Identifikation, Bewertung, Steuerung und Reporting von IT-Risiken

Werkzeuge und Methoden
- Kollektionsmethoden, analytische Methoden und Anwendung in Fallstudien

Risikomanagement und ITIL in der Praxis
- Business Continuity Management (BCM) und Business Impact Analyse (BIA)
- Bewertung von Abhängigkeiten zwischen IT-Risiken und zwischen IT- und Business-Risiken
- Maßnahmen zur präventiven und reaktiven Steuerung von IT-Risiken

Awareness, Sensibilisierung und Risikokultur
- Anwendung von IT-Risikoplanspielen in der Praxis
- Überblick über Softwarelösungen im IT-Risikomanagement

Ihr Nutzen

- Nach dem Seminar können Sie Risiken identifizieren (Risk Identification).
- Sie wissen, wie eine »Risk Analysis« durchzuführen ist.
- Sie können Risiken evaluieren und bewerten (Risk Evaluation).
- Sie wissen, wie Prozesse modelliert werden und eine Risikobehandlung durchgeführt wird.

Notfallmanagement im Bereich IT-Sicherheit

Aufbaukurs zur eigenständigen Entwicklung eines Notfallmanagementplans

Die Herausforderung ist, komplexen Problemen mit gezielter Prävention begegnen. Probleme und Ausfälle im IT-Bereich werden durch die zunehmende Technologisierung und damit verbundene Komplexität immer wahrscheinlicher. Um so wichtiger ist es, präventiv dagegen vorzugehen. Dieses Seminar hilft Ihnen dabei, einen unternehmensspezifischen Notfallmanagementplan zu erstellen. Sie lernen, Ausfälle zu verhindern und Schäden zu minimieren. Werden Sie aktiv!

Inhalte des Seminars

Planung und Erstellung von Notfallvorsorgekonzepten
- Notfallmanagementplan
- Präventiv Krisen im Unternehmen abblocken
- Bereits aufgetretene Probleme mindern
- Auf neue Herausforderungen vorbereitet sein

Ihr Nutzen

- Nach dem Seminar können Sie einschätzen, was zu den kritischen Prozessen Ihres Unternehmens gehört.
- Sie wissen, wie sich ein Notfallplan für Ausnahmesituationen nach dem BSI-Standard 100-4 erstellen lässt.
- Sie finden geeignete Möglichkeiten, dass bei Notfällen oder Krisen möglichst wenig Schaden angerichtet wird.
- Sie wissen, wie Sie bei einer Unterbrechung auf Verfahren zurückgreifen können, um möglichst schnell wieder zum Normalbetrieb übergehen zu können.

Informationen im Überblick

Grundkenntnisse von Planungs- und Umsetzungsaktivitäten, Zugang zu Sicherheitsprotokollen, Wissen von zukünftigen Projekten und geplanten Aktivitäten

Sicherheitsbeauftragte, Unternehmensleitung/ Führungskräfte

4 Stunden on Demand-Kurs

300,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/notfallmanagement-it-sicherheit

Informationen im Überblick

Grundlegende IT-Kenntnisse

Mitarbeitende (IT-fern, Digital Immigrants, Digital Natives) in operativen Bereichen von privatwirtschaftlich und institutionell ausgerichteten Organisationen

1 Stunde
on Demand-Kurs

50,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu,
wiss. Mitarbeiter
Fraunhofer FOKUS

Michael Holzhüter,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/it-sicherheit-arbeitsplatz

IT-Sicherheit am Arbeitsplatz

Grundlagenwissen für Mitarbeitende

IT-Angriffe auf Organisationen und Unternehmen adressieren heute vorwiegend den Faktor Mensch. IT-Sicherheitsvorfälle haben ihren Ursprung meist nicht im technischen Bereich, sondern entstehen durch menschliches Versagen. Zum Beispiel durch das Öffnen von Phishingmails, das Benutzen des gleichen Passworts für alle Plattformen oder ein zu offenherziger Umgang mit privaten, sicherheitskritischen Informationen. Entsprechend liegt es in der Verantwortung einer jeden Organisation, ihre Mitarbeitenden gegenüber Gefahren der IT-Sicherheit zu sensibilisieren.

Der hier vorgestellte Kurs entstammt der Praxis und zeigt Unterschiede zwischen der digitalen Welt und der analogen Welt auf, erklärt typische Denkmuster vieler Mitarbeitenden und regt zum kritischen Hinterfragen der individuellen Arbeitsprozesse an. Er liefert weiterhin vielfältige Anleitungen »für ein sicheres Arbeiten« und für »Hinterfragen von ungewöhnlichen Situationen nicht nur im Arbeitsalltag«. Der Kurs versucht den Lernenden für Themen der IT-Sicherheit zu begeistern und zugleich selbstbewußter in seinen jeweiligen Arbeitsabläufen zu machen.

Inhalte des Seminars

Grundlegende Eckdaten und Einblicke in das Thema

Chancen und Risiken einer digital vernetzten Gesellschaft

Zahlen einer digitalen Welt

Stereotype und Klischees in unseren Köpfen

Unterschiede zwischen dem vertrauten analogen Verhalten unserer Vergangenheit und den Chancen und Risiken einer digital vernetzten Gesellschaft/ Unternehmung

Ihr Nutzen

- Nach dem Seminar werden Sie typische Vorgehensmuster von IT-Angriffen besser erkennen und verstehen.
- Sie können auf ungewöhnliche Vorkommnisse in Ihren Arbeitsabläufen richtig reagieren.
- Sie verstehen, wie das Denken der Mitarbeitenden in Stereotypen für IT-Angriffe ausgenutzt werden kann.
- Sie werden sich ein Stück sicherer fühlen.

Erstellung Sicherheitskonzept

Wie Sie die IT-Sicherheit Ihres Unternehmens erhöhen

Eine gestiegene Bedrohungslage, aber auch Geschäftspartner verlangen ein klares und deutlich ausgeprägtes IT-Sicherheitskonzept. Dabei gibt es viele Facetten zu bedenken. Somit ist die Erstellung eines Sicherheitskonzeptes nicht nur zeitaufwändig sondern auch schwierig. Gerade kleine und mittelständische Unternehmen haben wenig Ressourcen, um die Dokumentation komplett zu entwerfen. Dieser Kurs hilft Ihnen dabei, selbstständig ein IT-Sicherheitskonzept, das die Unternehmenssicherheit stärkt, zu erstellen. Sichern Sie sich ab!

Inhalte des Seminars

Erstellung von Sicherheitskonzepten für Fachanwendungen

Anwenden des BSI-Standard 200-2/200-3

Erstellung der Strukturanalyse
- Gruppierung
- Relevante Geschäftsprozesse identifizieren
- Relevante Anwendungen identifizieren und mit Geschäftsprozess verknüpfen, Technologieübersicht schaffen
- Netzplan, IT-Systeme, Kommunikationspfade
- Räumlichkeiten und Gebäudesicherheit

Schutzbedarfsfeststellung

Definition Schutzbedarfskategorien

Schutzbedarfsfeststellung für Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Räume und Gebäude

Modellierung des Informationsverbunds
Modellierung IT-Infrastruktur, IT-Systeme, Netze, Anwendungen, Prozessbausteine, Systembausteine

IT-Grundschutz-Check

Risikoanalyse

Abbildung von Schnittstellenbeschreibungen

Ihr Nutzen

- Nach dem Seminar können Sie effektiv und umfassend Sicherheitskonzepte erstellen.
- Sie können die Sicherheit stärken, durch anerkannte und verbreitete Methoden.
- Sie haben die Verfahrensweise für Festlegung und Systematisierung der Sicherheitslücken, Sicherheitschecks und Risikoanalyse verstanden.

Organisatorische IT-Sicherheit | **Online**

Informationen im Überblick

Tiefen Einblick in eigene Softwarestruktur, Grundlagenwissen zu IT-Sicherheit (Kurs Risikomanagement und Bedrohungs- und Angriffsszenarien ratsam, aber nicht unbedingt notwendig)

Sicherheitsbeauftragte, Unternehmensleitung/ Führungskräfte, Projektleiter*innen, Product Owner

12 Stunden on Demand-Kurs oder 3 Tage Blended Learning-Seminar (Selbstlerninhalt + 2 Tage hybrid)

1800,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/erstellung-sicherheitskonzept

Sichere Digitale Lehre

Nutzung sicherer und datenschutzkonformer Kommunikationsmedien für die Lehre

Plattformen, Tools, Wikis oder Apps eröffnen neue innovative Möglichkeiten für Qualifizierungsansätze, jedoch auch Probleme. Digitale Medien werden dabei zum integrierten Lern- und Arbeitsmittel. Dabei dürfen die Voraussetzungen für die rechtskonforme Verarbeitung von Daten und die Sicherheit dieser nicht außer Acht gelassen werden. Mit diesem Seminar vermeiden Sie rechtliche, finanzielle und imageschädigende Folgen. Lernen Sie, wie Sie Ihre Lehre sicher und datenschutzkonform gestalten können.

Facebook, Snapchat, Youtube

Videokonferenztools, eLearning Plattformen

Was sind die Konsequenzen bei Fehlverhalten?

Existiert ein Werbeverbot?

Inhalte des Seminars

Grundlagen IT-Sicherheit und Datenschutz für die Lehre

Datenschutzkonformer Umgang mit Social Media und digitaler Lehre

Kommunikation mit Eltern und Schüler-*innen und Studierenden

Grundlagen im Umgang mit personenbezogenen Daten in der Lehre

- Wie könnte eine Kommunikation aus sicherheitstechnischer und datenschutzrechtlicher Sicht ablaufen?
- Dürfen private Geräte für die Lehre verwendet werden? (Mischung berufliche und private Daten?)
- Dürfen private E-Mail-Adressen für die Kommunikation mit den Schülern und Eltern verwendet werden?

Ihr Nutzen

- Nach dem Seminar können Sie die Dienste von E-Learning-Plattformen und Videokonferenztools datenschutz- und sicherheitskonform in Anspruch nehmen.
- Sie lernen, wie Sie Maßnahmen und Verfahren entwickeln, um die Nutzung von E-Learning-Plattformen und Videokonferenztools beurteilen zu können.
- Sie können im Einklang mit nationalem Recht Regelungen für Personen umsetzen, die mit ihren persönlichen elektronischen Geräten auf eine E-Learning-Plattform oder Videokonferenztools zugreifen.

Informationen im Überblick

Keine Voraussetzungen

Lehrer*innen, Trainer*innen, Weiterbildungsverantwortliche

6 Stunden
on Demand-Kurs

600,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu,
wiss. Mitarbeiter
Fraunhofer FOKUS

Michael Holzhüter,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/sichere-digitale-lehre

Security Awareness – Bewusstsein schaffen, Sicherheit gewinnen

Grundlagenkurs

Die Herausforderung: Bei einem Cyberangriff nutzt der Angreifer das vermeintlich schwächste Glied der Sicherheitskette: Den Menschen. Mehr als die Hälfte aller Cyberangriffe in den vergangenen Jahren nutzten die Schwachstelle Mensch als Einfallstor.

Durch die Digitalisierung erhalten Angriffsmuster aus dem Bereich Social Engineering eine neue und größere Bedeutung. Durch eine zunehmende Informationsverbreitung und Informationsvielfalt werden Cyberkriminellen eine größere Angriffsfläche geboten, welche sie nutzen um in Unternehmensnetze einzudringen. Hierbei kann der Angreifer oftmals auf eine Vielzahl von öffentlichen Informationen z.B. in sozialen Netzwerken zurückgreifen, um so authentische Phishing-Mails zu verfassen.

Schützen Sie sich und Ihr Unternehmen! Der Schutz vor Social Hackern erfordert vor allem Awareness zu diesem Thema und das Wissen darüber, wie Angreifer vorgehen und welche Schwachstellen sie ausnutzen.

Inhalte des Seminars

Teil 1: Schulung: Passwortsicherheit

Teil 2: Schulung: Social Engineering

Teil 3: E-Mail-Sicherheit

Teil 4: Schutz sensibler Daten

Teil 5: Sichere Internetnutzung

Ihr Nutzen

- Nach dem Webseminar können Sie Social Engineering Angriffe erkennen.
- Sie können sichere Passwörter erstellen.
- Sie wissen, wie man Phishing vorbeugen und Maßnahmen einleiten kann.
- Sie sind in der Lage den Umgang mit Informationen zu verbessern und somit Social Hacking Angriffe vorzubeugen
- Sie erkennen Gefahren im Internet

Informationen im Überblick

Internetfähiger PC – Browser: Firefox oder Google Chrome

Management, öffentlich wirksame Personen, Fachkräfte, Anwender und Selbstständige

3 Stunden

199,–

Online

Veranstaltet durch

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Referent:

Martin Klöden, seit 2018 Trainer im Lernlabor für Cybersicherheit Hochschule Mittweida

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/security-awareness

Informationen im Überblick

Keine Voraussetzungen

Anwendende, Einsteiger*innen

1 Tag Präsenz

600,–

Weiden/Bonn

Veranstaltet durch

Fraunhofer FKIE

Fraunhofer AISEC

Referenten:

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

Dr. Michael Rademacher, IT-Sicherheitsforscher Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/it-sicherheit-praevention-reaktion

Grundlagen der IT-Sicherheit – Von Prävention bis Reaktion

Wo fängt IT-Sicherheit eigentlich an?

Die Welt der IT-Sicherheit birgt viele Facetten und ist komplex. IT-Sicherheit dringt in alle Lebensbereiche ein, sei es im Job oder zu Hause, im Smartphone oder auf dem Firmenlaptop: Die Erfordernisse nach Grundkenntnissen der IT-Sicherheit wachsen zunehmend an! Doch was verbirgt sich hinter dem Begriff? Dieses Seminar bietet Ihnen einen leichten Einstieg in diesen Themenkomplex. Sie lernen Grundbegriffe kennen, und welche Anforderung von der Prävention bis zur Reaktion auf Sie zu kommen. In praktischen Übungen lernen Sie damit umzugehen!

Ihr Nutzen

- Nach dem Seminar können Sie das deutsche Zertifizierungsschema des BSI nachvollziehen.
- Sie können die zentralen Konzepte der Common Criteria anwenden und notwendige Aktivitäten auf Herstellerseite abschätzen.
- Sie können die Anwendbarkeit von CC bzgl. Ihres Portfolios abschätzen und eigens eine CC-Zertifizierung initiieren.
- Sie wissen, wie man IT-sicherheitskonformes Verhalten im privaten und beruflichen Bereich anwendet und Bedrohungen der IT-Sicherheit erkennt.
- Sie wissen, wie man Schutzmechanismen für die IT-Sicherheit anwendet und im Falle eines Sicherheitsvorfalls konform handelt.

Inhalte des Seminars

Kennenlernen der Grundbegriffe der IT-Sicherheit

Identifizieren von Sicherheitszielen

Angriffsmethoden und Bedrohungen

Gegenmaßnahmen

Physical Security und Social Engineering

Organisatorische IT-Sicherheit | **Präsenz**

IT-Sicherheitsorganisation im Unternehmen

IT-Sicherheitsmaßnahmen im Unternehmen etablieren

IT-Sicherheit muss in jedem Unternehmen etabliert werden – doch häufig hapert es in der Sicherheitsorganisation. Die Folgen können gravierend sein: Wettbewerbsvorteile gehen verloren, Kunden wenden sich durch Vorkommnisse ab, rechtliche Konsequenzen und finanzielle Einbußen! Dieses Seminar hilft Ihnen, in Ihrem Unternehmen eine passende IT- Sicherheitsorganisation aufzubauen. Ziele sind die Förderung von Mitarbeiter-Awareness und das Etablieren von Sicherheitsmaßnahmen.

Inhalte des Seminars

IT-Sicherheit – Grundlagen und Motivation

Wirtschaftsspionage

Google Hacking

Rechtliche Grundlagen, insbesondere EU-DSGVO

Live Hacking

IT-Sicherheitsmanagement

Workshop: Fallbeispiele aus der Praxis

Ihr Nutzen

- Nach dem Seminar können Sie wichtige Bedrohungen für Unternehmensdaten einschätzen und Vorkehrungen zu deren Abwehr treffen.
- Sie wissen, wie Sie den Aufbau eines IT-Sicherheitsmanagements durchführen.
- Sie haben Einblick in die Vorgehensweise von Hackern und Wirtschaftsspionen anhand von Live Hacking und Google Hacking.
- Sie können die Schritte zur Umsetzung wesentlicher rechtlicher Randbedingungen vornehmen.

Informationen im Überblick

Keine Voraussetzungen

Führungskräfte, Fachkräfte und Spezialist*innen, Anwendende

1 Tag Präsenz

600,–

Weiden

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/it-sicherheitsorganisation-im-unternehmen

Informationen im Überblick

Keine Voraussetzungen

Mitarbeiterinnen und Mitarbeiter aus dem Management, IT-Sicherheitsverantwortliche, Führungskräfte, Mitglieder des Vorstands

4 Stunden online

210,–

online

Veranstaltet durch

Fraunhofer FKIE

Referent:

Prof. Dr. Michael Meier, Lehrstuhlinhaber IT-Sicherheit, Universität Bonn, Abteilungsleiter Cyber Security, Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/it-sicherheitsstrategie-unternehmen-online

Crashkurs IT-Sicherheitsstrategie im Unternehmen

Optional auch mit erweiterten Inhalten als Inhouse Seminar. Fragen Sie uns an!

Ganzheitliche IT-Sicherheit etablieren

Die Herausforderung: Stetig wachsende IT-Sicherheitsanforderungen und eine unübersichtliche Lage der Informationssicherheit. Je mehr automatisiert wird, desto mehr Informationen (auch sensibler Art) sind potenziell angreifbar. An erster Stelle benötigt man deshalb ein Bewusstsein für IT-Sicherheit und dafür nötige Kompetenzen. In unserem Crashkurs lernen Sie, wie Sie aktuelle Bedrohungen erkennen und einschätzen können. Die Förderung des Sicherheitsbewusstseins steht im Mittelpunkt des Seminars. Zudem können Sie nach dem Seminar, die Auswirkungen von IT-Sicherheits- und Datenschutzgesetzen auf Ihr Unternehmen einschätzen.

Inhalte des Seminars

- Aktuelle Angriffstechniken und Gegenmaßnahmen – Ausnutzung von Programmverwundbarkeiten
- Angreifer – Typen, Motivationen, Vorgehensweise
- Gegenmaßnahmen und Abwehrstrategien
- Aktuelle Bedrohungen im Umfeld Cybercrime
- Aktuelles Thema: Identitätsdiebstahl
- Ein Blick in den Werkzeugkasten der NSA

Ihr Nutzen

- Nach dem Seminar können Sie typische Fehler im Umgang mit Sicherheitsmechanismen vermeiden.
- Sie können wesentliche Sicherheitsmaßnahmen unterscheiden.
- Sie können die Anforderungen des Datenschutzes und der Anwender sinnvoll technisch umsetzen und Auswirkungen der neuen IT-Sicherheits- und Datenschutzgesetze auf Ihr Unternehmen einschätzen.
- Sie wissen, welche Schritte bei der Einführung eines Risikomanagements anstehen.
- Sie können interne Kampagnen zur Mitarbeitersensibilisierung für Sicherheitsfragen verbessern.

BSI-Vorfall-Expert*in

Aufbauschulung mit optionalem Personenzertifikat des BSI

Unser Zusatzangebot: Auffrischung der Seminarinhalte vor dem Prüfungstermin

Aufgrund der starken Abhängigkeit von einer funktionierenden Informationstechnik ist es essenziell, angemessen auf IT-Sicherheitsvorfälle zu reagieren und somit das Schadensausmaß möglichst auf ein Minimum zu reduzieren. Insbesondere soll es kleinen und mittelständischen Unternehmen und regionalen Behörden ermöglicht werden, IT-Sicherheitsvorfälle schnell und effektiv zu beheben. Dazu bedarf es geschulte Expert*innen, welche bei Bedarf auch vor Ort unterstützen können.

Diese Schulung stellt das Einstiegsmodul hinsichtlich der Qualifizierung zum Vorfall-Expert*in innerhalb des Cyber-Sicherheitsnetzwerks des Bundesamt für Sicherheit in der Informationstechnik (BSI) dar.

Inhalte des Seminars

- Rahmenbedingungen kennenlernen
- Ablauf des Standardvorgehens erproben
- Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen kennen
- Remote-Unterstützung erproben
- Praktizieren der »Vor-Ort-Unterstützung«
- Präventive Maßnahmen einleiten

Ihr Nutzen

- Nach dem Seminar können Sie den Betroffenen bei einem IT-Sicherheitsvorfall prozessorientiert, schnell und effektiv Unterstützung leisten.
- Sie können Angriffswege und -formen erkennen und geeignete Maßnahmen einleiten.
- Sie können den Betroffenen vor Ort oder, per remote Unterstützung leisten und bei der Prävention behilflich sein.

Organisatorische IT-Sicherheit | Online oder Präsenz

Informationen im Überblick

Grundlegende Kenntnisse zur Informationssicherheit und -technik.

IT-Sicherheitsbeauftragte, Notfallbeauftragte, Einzelexpert*innen, die mit einem Zertifikat den Status »Vorfall-Experte« des BSI anstreben.

3 Tage Präsenz, online oder on Demand-Kurs

1800,–

Bonn/ Mittweida/ Mönchengladbach/ Online

Referenten:

Prof. Dr. Matthias Mehrtens, Professor der Hochschule Niederrhein

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Martin Klöden, Trainer im Lernlabor für Cybersicherheit Hochschule Mittweida

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/bsi-vorfall-experte

Datenschutz

Die Anforderungen an den Datenschutz nehmen zu!

Datenschutz wird von Unternehmen nicht selten als lästiges Thema empfunden. Doch der Anspruch an die Integrität und Vertraulichkeit im Umgang mit den persönlichen, personengebundenen Daten nimmt gesellschaftlich einen hohen Stellenwert ein.

Durch die gewaltige Nutzung des Internets ist der Datenverkehr und damit auch die Datenerhebung enorm gestiegen. Diese Daten ermöglichen jedoch Einblicke in vertrauliche und persönliche Informationen von Personen. Da jede Person die Verfügungsgewalt über die eigenen Informationen besitzt, kann mit diesen Daten nicht einfach frei und sorglos verfahren werden. EU-Richtlinien wie die EU-DSGVO oder Bundesgesetze wie das BDSG stellen sicher, dass Unternehmen nur die Daten erheben und verwenden, die Ihnen explizit dafür zur Verfügung gestellt wurden.

Die EU-DSGVO und das BDSG sind rechtlich bindend! Bei Verstoß drohen empfindliche Bußgelder bis zu 20 Millionen Euro oder 4% des weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres!

Im Lernlabor Cybersicherheit werden Sie darauf geschult, Datenschutzverordnungen sachgemäß umzusetzen. In unseren Seminaren lernen Sie, welche Herausforderungen dabei auftreten können, und wie diese im Unternehmen umgesetzt werden können. Mit den Fraunhofer-Expertinnen und -Experten bekommen Sie ein Spezialistenteam an Ihre Seite, das sowohl wissenschaftliche Expertise als auch Branchenkenntnis miteinbringt.

Mit EU-Richtlinien und Bundesgesetzen ist Datenschutz kein individualspezifisches Kriterium mehr, sondern eine Herausforderung, der sich jedes Unternehmen stellen muss.

Datenschutz am Arbeitsplatz

Grundlagenwissen für Mitarbeitende

Die Herausforderung: Neue Datenschutzanforderungen benötigen Sensibilisierung – auch bei den Mitarbeitenden. Mit den Neuerungen der DSGVO und des BDSG seit Mai 2018 steigen die Anforderungen in jeglichen Bereichen eines Unternehmens. Werden diese unzureichend umgesetzt, drohen sogar Abmahnungen und Bußgelder. Datenschutz wird deshalb zur Verantwortung aller Mitarbeitenden. Die Voraussetzung: Know-how und Awareness. Dieses Seminar bietet eine unternehmensgerechte Einführung in den rechtskonformen Datenschutz.

Inhalte des Seminars

Personenbezogenen Daten

Besondere Kategorie und damit Pflicht zur Datenschutz-Folgeabschätzung

Sicherstellung der Betroffenen-Rechte

Weitergabe von Daten an Externe

Datenschutzverstoß erkennen und melden

Dokumentation der Verarbeitungstätigkeiten und Aufstellen der technischen und organisatorischen Maßnahmen

Datenschutz-Folgeabschätzung selbstständig durchführen

Ihr Nutzen

- Nach dem Seminar können Sie die Ziele und Grundsätze des deutschen und europäischen Datenschutzes nachvollziehen und erklären.
- Sie kennen die Zulässigkeitsvoraussetzung und Betroffenenrechte des Datenschutzes.
- Sie wissen, wie sie mit Datenschutzverletzungen umgehen.
- Sie können die Grundlagen der aktuellen Datenschutzregelungen an Ihre Mitarbeitenden weitergeben.

Informationen im Überblick

Keine Voraussetzungen

Mitarbeitende, die mit personenbezogenen Daten beschäftigt sind

2 Stunden
on Demand-Kurs

50,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu,
wiss. Mitarbeiter
Fraunhofer FOKUS

Michael Holzhüter,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/datenschutz-am-arbeitsplatz

Informationen im Überblick

Keine Voraussetzungen

(Angehende) Datenschutzverantwortliche, Datenschutzbeauftragte, Unternehmensleitung, Management, Projektleitung, Product Owner

12 Stunden on Demand-Kurs

1000,– auf Wunsch Online Zertifizierung: 180,– zzgl. MwSt.

online

Veranstaltet durch

Fraunhofer FOKUS

Referent:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/eu-datenschutz-online

EU-Datenschutz-Spezialist*in

Rechtskonform im Unternehmen

Die Herausforderung: Datenschutz wird immer komplexer. Durch die Erweiterung des DSGVO und des BDSG seit dem 25.05.2018 entstehen immer mehr Handlungsfelder für Unternehmen. Eine korrekte und rechtzeitige Umsetzung ist dabei unverzichtbar, denn ist das nicht der Fall, können hohe Bußgelder und Strafen bis zu 20 Mio. € oder 4% des gesamten Jahresumsatzes auf ein Unternehmen zukommen. Dieses Seminar stattet Sie in praxisorientierten Einheiten mit dem nötigen Wissen aus, um ihr Unternehmen nach außen hin richtig abzusichern.

Inhalte des Seminars

Einführung in den Datenschutz
- Gesetze und Verordnungen
- Grundbegriffe des Datenschutzes

Verarbeitung personenbezogener Daten und Zulässigkeitsvoraussetzungen
- Prozesse für Betroffenenrechte gestalten
- Notfallplanung bei Datenschutzverletzungen
- Personenbezogene Daten im Ausland verarbeiten

Dokumentation im Unternehmen
- Anforderungen an die Datenschutzbeauftragten
- Verzeichnis für Verarbeitungstätigkeiten rechtssicher gestalten

Technische und organisatorische Maßnahmen rechtssicher gestalten
- Datenschutz-Folgeabschätzung durchführen
- Anforderungen in der Softwareentwicklung kennen und umsetzen

Sensibilisierung, Schulung und interne Beratung im Unternehmen durchführen
- Durchführung von Audits
- Auftragsverarbeitung

Ihr Nutzen

- Nach dem Seminar verstehen sie die Aufgaben, Ziele und Grundprinzipien der Datenschutzgesetze: Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG), Landesdatenschutz- und weitere Gesetze.
- Sie kennen aktuelle Rechtbegriffe und wissen mit ihnen umzugehen.
- Sie können den Stand des Datenschutzes schnell im Unternehmen erfassen, gezielt Risiken begegnen und Sanktionen vermeiden.

Zertifizierte*r EU-Datenschutz-Spezialist*in (DSGVO/GDPR)

Datenschutz im Unternehmen festigen

DIe Herausforderung: Datenschutz braucht starkes Management. Am 25.05.2018 traten die EU-Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz in Kraft. Auch jetzt haben viele Unternehmen diese noch nicht umgesetzt. Ein Grund: die anspruchsvolle und zeitaufwendige Umsetzung der entsprechenden Regelungen. Wo soll man anfangen? Wie kann man den Stand des Datenschutzes im Unternehmen praktisch erfassen? Für eine rechtskonforme Umsetzung empfiehlt es sich deshalb, im Unternehmen eigene Spezialisten einzusetzen.

Inhalte des Seminars

Einführung in den Datenschutz
- Gesetze und Verordnungen
- Grundbegriffe des Datenschutzes

Verarbeitung personenbezogener Daten und Zulässigkeitsvoraussetzungen
- Prozesse für Betroffenenrechte gestalten
- Notfallplanung bei Datenschutzverletzungen
- Personenbezogene Daten im Ausland verarbeiten

Dokumentation im Unternehmen
- Anforderungen an den Datenschutzbeauftragten
- Verzeichnis für Verarbeitungstätigkeiten rechtssicher gestalten

Technische und organisatorische Maßnahmen rechtssicher gestalten
- Datenschutz-Folgeabschätzung durchführen
- Anforderungen in der Softwareentwicklung kennen und umsetzen

Sensibilisierung, Schulung und interne Beratung im Unternehmen durchführen
- Durchführung von Audits
- Auftragsverarbeitung

Ihr Nutzen

- Nach dem Seminar können Sie die Vorschriften der Datenschutzgesetze umsetzen: Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG), Landesdatenschutz- und weitere Gesetze.
- Sie kennen aktuelle Rechtsbegriffe und wissen mit ihnen umzugehen.
- Sie können die Relevanz des Datenschutzes nachvollziehen, gezielt Risiken begegnen und Sanktionen vermeiden.

Informationen im Überblick

Keine Voraussetzungen

(Angehende) Datenschutzverantwortliche, Datenschutzbeauftragte, Unternehmensleitung, Management, Projektleitung, Product Owner

2 Tage Präsenz

1200,– Zertifizierung: 180,– zzgl. MwSt.

Berlin

Veranstaltet durch

Fraunhofer FOKUS

Referenten:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/eu-datenschutz

Informationen im Überblick

Zertifikat für EU-Datenschutzspezialist*in oder Grundkenntnisse im Datenschutz

Datenschutzbeauftragte, Unternehmensleitung, Mitarbeiter*innen und Führungskräfte aus Marketing und Sales, welche mit personenbezogenen Daten arbeiten (Vertrieb/ Marketingexperten)

3 Stunden on Demand-Kurs

400,–

online

Veranstaltet durch

Fraunhofer FOKUS

Referent:

Sebastian Breu, wiss. Mitarbeiter Fraunhofer FOKUS

Michael Holzhüter, wiss. Mitarbeiter Fraunhofer FOKUS

Weitere Infos und Anmeldung unter:

www.cybersicherheit.fraunhofer.de/eu-datenschutz-vermarktung

Datenschutzkonform in der Vermarktung

Aufbaukurs für EU-Datenschutzspezialist*in

Die Herausforderung: Personenbezogene Daten sind für das Marketing hoch relevant. Arbeiten Sie in diesem Bereich, tragen Sie die Verantwortung, dass rechtskonform gehandelt wird und vorrangig mit personenbezogenen Daten der richtige Umgang herrscht. Damit ersparen Sie Ihrem Unternehmen Abmahnungen und Bußgelder. In der Verarbeitung solcher Daten benötigt man deshalb Know-how und Sensibilität. Mitarbeitende im Bereich Marketing und Sales müssen daher stets mit den aktuellen Datenschutzbestimmungen vertraut sein. Erfahren Sie, wie Sie mit Bild- und Videoaufnahmen rechtskonform umgehen, und worauf bei der Kundenakquise besonders zu achten ist.

Inhalte des Seminars

Überblick zu den wichtigsten Datenschutzbestimmungen
- Bundesland, Deutschland, EU

Umgang mit Bild-und Videoaufnahmen
- Insbesondere bei Veranstaltungen
- Betroffenenrechte bei Bildern sicherstellen

Kundenakquise
- Kaltakquise per Telefon
- Kaltakquise per Mail
- E-Mail Tracking

Auftragsdatenverarbeitung
- Datenberechtigung
- Datenzugriff
- Datenfokus

Personenbezogene Daten in CRM-Systemen verwalten

Ihr Nutzen

- Nach dem Seminar können Sie die Umsetzung der Vorschriften von EU-Datenschutzgrundverordnung und Bundesdatenschutzgesetz in Marketing und Sales planen und für Ihren Organisationskontext anwenden.
- Sie können aktuelle Rechtsbegriffe besser verstehen.
- Sie sind in der Lage, die entsprechende Aufmerksamkeit für dieses wichtige Aufgabenfeld und die dafür notwendige Sensibilisierung im Unternehmen zu erlangen.
- Sie kennen die wichtigen Bereiche, die Sie als Marketing- und Sales-Mitarbeitende im Blick haben müssen.

Datenschutz |
Online oder Präsenz

Technischer Datenschutz in Unternehmen und Behörden

Anonymisierung und Pseudonymisierung effektiv anwenden

Die Herausforderung: Personenbezogene Daten zu schützen und datenschutzkonform zu verarbeiten. Ein Weg ist die Anonymisierung und die Pseudonymisierung der persönlichen Daten. Auf diese Weise kann der Schutz der Privatsphäre sichergestellt werden. Häufig ist aber unklar, wie die Daten am besten anonymisiert bzw. pseudonymisiert werden können. Dieses Seminar zeigt Ihnen, welche grundlegenden Techniken angewendet werden können. Anhand praktischer Beispiele lernen Sie, wie sich Anonymisierungs- und Pseudonymisierungsverfahren anwenden lassen.

Inhalte des Seminars

Motivation und Einordnung der Funktion von Verfahren für die Pseudonymisierung und Anonymisierung von Daten

Grundlegendes zur angewandten Kryptographie mit Praxisbeispielen

Privacy Enhancing Technologies

Anonymisierung mit Praxisbeispielen

Pseudonymisierung mit Praxisbeispielen

Ihr Nutzen

- Nach dem Seminar können Sie wesentliche Pseudonymisierungs- und Anonymisierungstechniken unterscheiden und anwenden.
- Sie können gängige Fehler beim Einsatz von Pseudonymisierungs- und Anonymisierungstechniken vermeiden.
- Sie können Anforderungen des Datenschutzes und der Anwender sinnvoll technisch umsetzen.
- Sie kennen praktikable Lösungsansätze zur Etablierung effektiver Pseudonymisierungen und Anonymisierungen.

Informationen im Überblick

Grundlegendes technisches Verständnis, z.B. aus einem Informatikstudium auf Bachelor-Niveau oder aus entsprechender Berufserfahrung

Fachkräfte mit grundlegendem technischen Verständnis und Interesse an technischem Datenschutz

1 Tag Präsenz

600,–

Bonn oder online

Veranstaltet durch

Fraunhofer FKIE

Referentin:

Saffija Kasem-Madani,
wiss. Mitarbeiterin
Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/technischer-datenschutz

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:


Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Sicherheit in Software-Entwicklung & Netzwerken
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
Energie- & Wasserversorgung und Public Safety
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

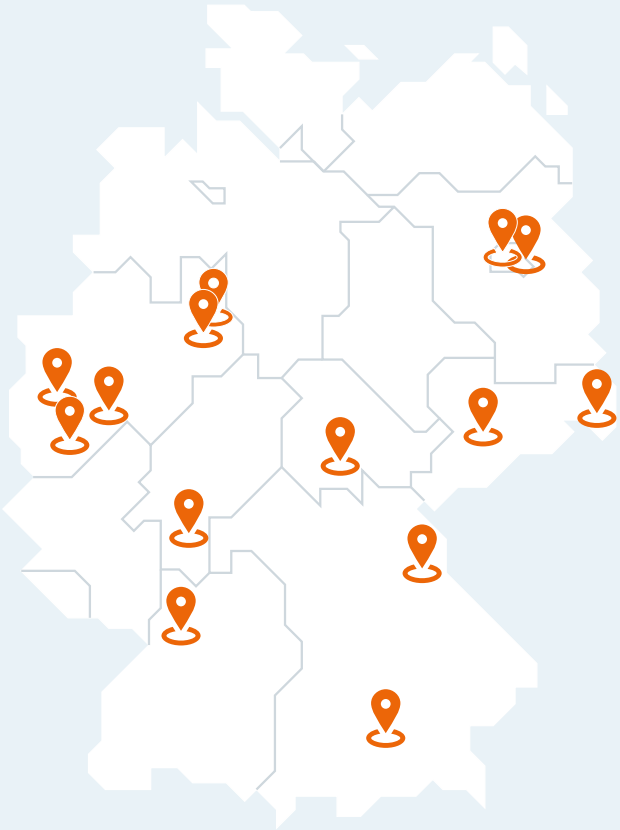
Aktuelle Qualifizierung aus der angewandten Forschung

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 Mai 2022

Sie erreichen uns

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

www.cybersicherheit.fraunhofer.de