IT-Sicherheitstrainings

Termine 2024

cirosec

Trainings bei cirosec

Wir bieten Ihnen individuell gestaltete Seminare und Trainings, in denen Ihnen unsere langjährig erfahrenen Berater den richtigen Umgang mit modernen Technologien und neuen Sicherheitsthemen vermitteln.

Die Vorteile eines Trainings bei cirosec liegen auf der Hand:

- Erfahrene, als Berater tätige Trainer mit aktuellem Praxisbezug
- Ständig aktualisierte Inhalte
- Lösungsorientierte Vorgehensweise
- Tiefes Eintauchen in die Sichtweise eines Angreifers nach dem Prinzip „Know your Enemy“ bei unseren Hacking-Extrem-Trainings
- Learning by Doing: Bei vielen Trainings steht jedem Teilnehmer ein Notebook für praxisnahe Übungsaufgaben zur Verfügung.

Hinweis zu den Online-Schulungen

Unsere Trainings finden sowohl in Tagungshotels als auch alternativ online statt.

Bei den Online-Schulungen können die Teilnehmer nicht nur die Folien und die Trainer per Video-Übertragung in Microsoft Teams sehen, sondern auch die Kontrolle über einen eigenen virtuellen Übungsarbeitsplatz übernehmen, der von cirosec bereitgestellt wird und mit zahlreichen Werkzeugen und Exploits ausgestattet ist.

Die Schulungsteilnehmer können somit auch bei der Online-Variante der Schulung alle Übungsaufgaben interaktiv und mit individueller Betreuung der Trainer durchführen.

Termine

14.05.2024 Frankfurt
17.10.2024 Ludwigsburg
11.12.2024 Ludwigsburg

Malware und Ransomware — Hintergründe, Erkennung, Schutz

Malware und Ransomware haben sich zu einer allgegenwärtigen Bedrohung entwickelt. Immer mehr Unternehmen sind betroffen, werden erpresst und können nicht mehr arbeiten.

Die Schulung vermittelt das nötige Wissen über die Angreifer, ihre Techniken und Vorgehensweisen sowie sinnvolle Sicherheitsmaßnahmen, um sich wirksam schützen, Angriffe frühzeitig erkennen und richtig reagieren zu können.

In einem Rückblick auf die wichtigsten Vorfälle der vergangenen Jahre werden die verschiedenen Infektionsmechanismen, die Schritte zur Weiterverbreitung und Umgehung von Schutzmaßnahmen sowie die Hintergründe und Tätergruppen erläutert.

Danach werden Strategien und Techniken zur Prävention von Vorfällen dargestellt und bewertet. Diese beinhalten sowohl die sinnvolle Nutzung der vorhandenen Bordmittel von Windows und der typischen Gateways als auch moderne Trends wie EDR, XDR und SASE sowie Strategien wie Zero Trust. Ebenso werden Konzepte und Techniken zur frühzeitigen Erkennung von Angriffen und Infektionen erläutert und die Rolle von CERTs, SOCs und SIEM-Lösungen zusammen mit den heute relevanten Betriebsmodellen und Outsourcing-Optionen abgegrenzt.

Auch die richtige Reaktion auf Vorfälle, nötige Vorbereitung für das Incident Management und die Wiederherstellung sowie Möglichkeiten zur Analyse von Malware werden dargestellt.

In dieser Schulung erlernen die Teilnehmer nicht nur konkrete technische und organisatorische Maßnahmen, sondern auch die Herangehensweise zur Erstellung von Malwareschutzkonzepten.

Zielgruppe: Sicherheitsverantwortliche, Administratoren, SOC-Mitglieder, CERTs

Voraussetzung: Grundlegende Kenntnisse in der IT; von Vorteil sind Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern.

Dauer: 1 Tag **Preis:** 995,- Euro

Termin

25.06.-26.06.2024 online
24.09.-25.09.2024 online
10.12.-11.12.2024 online

Sicherheit in Microsoft Office 365

Unser Trainer stellt Ihnen in diesem Training sicherheitsrelevante Aspekte und Funktionen von Microsoft Office 365 vor. Des Weiteren werden Konfigurationsmöglichkeiten sowie Maßnahmen für die Administration und den sicheren Betrieb einer O365-Umgebung präsentiert.

Im Rahmen dieser Schulung erörtern wir mit Ihnen zunächst typische Bedrohungsszenarien und Risiken für Cloud-Umgebungen im Allgemeinen und Office 365 im Speziellen.
Themen dieses Teils sind unter anderem:

- Datensicherheit vs. Datenverlust
- Missbrauch von Accounts bzw. Identitätsdiebstahl
- Unzureichende Strategie für Cloud-Migration und -Betrieb
- Notfallkonzepte
- Angriffe auf die Verfügbarkeit

Im zweiten Teil der Schulung werden spezifische Risiken in Office 365 diskutiert und Maßnahmen vorgestellt, um die erörterten Risiken zu minimieren. Hierbei geht es um folgende Aspekte:

- Sicherer Aufbau und sichere Konfiguration eines Office-365-Tenants
- Absicherung von Office 365
- Sichere Konfiguration von Client-Komponenten
- Berechtigungs- und Nutzermanagement
- Integration einer O365-Umgebung in eine bestehende Unternehmensinfrastruktur

Darüber hinaus zeigen wir typische organisatorische und technische Herausforderungen des sicheren Betriebs einer Office-365-Umgebung auf und diskutieren mögliche Lösungsansätze.
Die Teilnehmer haben am Ende der Schulung ein tieferes Verständnis sowohl von der Funktionsweise von Office 365 als auch von möglichen Bedrohungen und können Maßnahmen zur Absicherung einer O365-Umgebung zukünftig effizient umsetzen.

Zielgruppe: Sicherheitsverantwortliche, Administratoren, IT-Architekten, Verantwortliche im Bereich Cloud

Dauer: 2 Tage **Preis:** 1.995,- Euro

16.05.2024 Frankfurt
16.10.2024 online

Incident Handling & Response

In diesem ganztägigen Seminar werden aktuelle Methoden des Incident Handling und der Incident Response als Vorbereitung auf mögliche zukünftige Vorfälle behandelt.

Zunächst gehen wir darauf ein, wie sich ein Sicherheitsvorfall erkennen lässt. Dabei werden sowohl technische Möglichkeiten zur Erkennung etwaiger Sicherheitsvorfälle auf Endgeräten und im Netzwerk erörtert als auch organisatorische Maßnahmen dargestellt. Anschließend zeigen wir, wie mithilfe des ISO-27035-Standards eine systematische Vorgehensweise bei der Bearbeitung eines Vorfalls gewährleistet werden kann. Dabei betrachten wir ebenfalls, welche ergänzenden Anforderungen für KRITIS-relevante Unternehmen bestehen.

Darauf aufbauend wird anhand von Fallbeispielen exemplarisch das richtige Vorgehen bei einem Verdacht auf Hacker-Einbruch, Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung firmeneigener Kommunikationsmöglichkeiten detailliert erörtert.

Nach Abschluss des Seminars wissen die Teilnehmenden nicht nur, wie sie einen Incident-Response-Prozess im Unternehmen etablieren und weiterentwickeln können, sondern auch welche Anforderungen an die Sammlung, Speicherung und Auswertung digitaler Spuren als Beweismittel zu erfüllen sind.

Zielgruppe: Sicherheitsverantwortliche, CERTs, betriebliche Ermittler

Voraussetzung: Grundlegende Kenntnisse in der IT; von Vorteil sind Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern.

Dauer: 1 Tag **Preis:** 995,- Euro

10.09.-13.09.2024 Frankfurt
03.12.-06.12.2024 Ludwigsburg

Hacking Extrem

Die größtmögliche Sicherheit kann nur dann erreicht werden, wenn man die Methoden und Vorgehensweise der Angreifer kennt und ihre Denkweise und Motive nachvollziehen kann.

Häufig werden Sicherheitsmechanismen lediglich aus der Sicht eines Administrators oder Netzwerkspezialisten geplant und aufgebaut. Die Betrachtungsweise eines Angreifers unterscheidet sich in der Regel jedoch grundlegend davon. Nicht zuletzt deshalb kommt es immer wieder zu erfolgreichen Angriffen auf Firmennetze.

Dieses Intensivtraining vermittelt die Vorgehensweise von Angreifern jenseits von Web-Applikationen. Beginnend mit der Informationsgewinnung geht es in zahlreichen Schritten über Linux-Server und Windows-Clients bis in die Domäne. Es wird auf bekannte und weniger bekannte Angriffstechniken eingegangen – von den grundlegenden Klassikern bis hin zur Umgehung aktueller Schutzmechanismen, von konzeptionellen Problemen bis hin zu Vorgängen in der Hardware. In zahlreichen Demonstrationen werden Beispiele aus der Praxis beleuchtet.

Die Trainer führen selbst regelmäßig Sicherheitsüberprüfungen durch und geben eigene Praxiserfahrung sowie Insider-Wissen aus der „Szene“ ungefiltert weiter.

Behandelte Betriebssysteme: Linux/Unix-Umfeld und Windows

Zielgruppe: Administratoren, Netzwerkspezialisten, Sicherheitsverantwortliche und Mitarbeiter auf Management-Ebene, die sich nicht scheuen, (Un-)Sicherheit auch durch die Brille des Angreifers zu betrachten, und dabei sehr tief in eine technische Welt eintauchen möchten.

Voraussetzung: Kenntnisse der grundlegenden Vorgänge der Benutzung und Administration von Windows- und Linux-Systemen. Kenntnisse des TCP/IP-Stacks und der Funktionsweise gängiger Protokolle sind von Vorteil.

Dauer: 4 Tage **Preis:** 2.995,- Euro

Termin

16.04.-18.04.2024 Frankfurt
24.09.-26.09.2024 Ludwigsburg
10.12.-12.12.2024 München

Hacking Extrem Web-Applikationen

Webbasierte Applikationen haben sich zu bevorzugten Angriffspunkten entwickelt: Nicht nur, weil immer mehr Firmen Onlineshops, Bankanwendungen, Mitarbeiterportale oder andere interaktive Applikationen mit Web-Front-Ends oder Web Services anbieten, sondern auch, weil diese Systeme stets mit neuen Methoden angegriffen und manipuliert werden können.

„Hacking Extrem Web-Applikationen“ ist ein Training, das sich mit Angriffen auf Web-Applikationen und Back-End-Systeme beschäftigt. Die Schulung deckt alle Schwachstellenarten der OWASP Top Ten 2017 ab.

Das Intensivtraining vermittelt Ihnen die Vorgehensweise der Angreifer sowie bekannte und weniger bekannte Angriffstechniken auf Web-Applikationen mit den dahinter liegenden Datenbanken und Back-Ends. Der ausgesprochen praxisorientierte Stil ist durch zahlreiche Laborübungen angereichert.

Jedem Teilnehmer steht bei diesem Training jeweils ein Notebook mit einer Fülle von Werkzeugen zur Verfügung. So kann jeder selbst erfahren, wie ein Angreifer praktisch vorgeht.

Die Trainer führen regelmäßig Sicherheitsüberprüfungen durch und sind als Experten im Bereich der Applikationssicherheit bekannt.

Behandelte Systeme: Unix- und Windows-basierte Webserver, Datenbanken, Applikationsserver, ...

Zielgruppe: Administratoren und Sicherheitsverantwortliche, die die Sicherheit auch durch die Brille des Angreifers betrachten und dabei sehr tief in dessen Welt eintauchen möchten. Ebenso ist das Training interessant für Entwickler von Webanwendungen sowie für Administratoren von Webservern und E-Business-Systemen.

Voraussetzung: Grundkenntnisse in HTTP, HTML sowie im Bereich Webserver und Datenbanken

Dauer: 3 Tage **Preis:** 2.400,- Euro

Termine

04.06.-06.06.2024 online
08.10.-10.10.2024 Köln
19.11.-21.11.2024 München

Hacking und Härtung von Windows-Betriebssystemen

Diese Schulung widmet sich vollständig der Sicherheit des aktuellen Client-Betriebssystems Windows 10/11. Unsere erfahrenen Trainer stellen Ihnen sicherheitsrelevante Neuerungen, deren Anforderungen und Konfigurationsmöglichkeiten sowie neue Herausforderungen für die Verwaltung und Administration dieser Clients vor. Ausgehend von typischen Bedrohungsszenarien für Windows-10/11-Clients lernen Sie mithilfe von Hands-on-Übungen und Demonstrationen, wie Sie die neuen Technologien und Möglichkeiten zur Absicherung der Endgeräte nutzen können.

Im Rahmen dieser Schulung diskutieren wir mit Ihnen zunächst typische Bedrohungsszenarien für Windows-Clients in den unterschiedlichen Einsatzszenarien. Diesen Bedrohungsszenarien stellen wir im Verlauf der Schulung sinnvolle Härtungs- und Schutzmaßnahmen gegenüber. Dadurch erhalten erfahrene Client-Administratoren ein tieferes Verständnis für mögliche Bedrohungen, und IT-Sicherheitsverantwortliche können die Möglichkeiten von Windows 10/11 kennenlernen. Darüber hinaus zeigen wir typische organisatorische und technische Herausforderungen zum sicheren Betrieb einer Windows-Client-Umgebung auf und diskutieren mögliche Lösungsansätze. In unserer Schulungsumgebung lernen Sie relevante Konfigurationseinstellungen und die Handhabung ausgewählter Werkzeuge kennen. Die Auswirkungen einzelner Härtungsmaßnahmen und Funktionen zeigen wir Ihnen mithilfe gängiger, frei verfügbarer Hacker-Tools auf.

Zielgruppe: Sicherheitsverantwortliche, (Client-)Administratoren, SOC-Mitglieder, „Blue Team“- oder „Red Team“-Mitglieder sowie (Projekt-)Verantwortliche im Bereich Windows-Clients oder Windows-Client-Sicherheit

Voraussetzung: Die Teilnehmer sollten über solide Anwendererfahrungen im Windows-Umfeld verfügen. Vorwissen über administrative Werkzeuge oder Angriffs-Tools sind von Vorteil. Die Übungen erfordern den Umgang mit Kommandozeilenwerkzeugen wie PowerShell und gängigen administrativen Werkzeugen aus dem Active-Directory-Umfeld.

Dauer: 3 Tage **Preis:** 2.400,- Euro

Termin

14.05.-16.05.2024 Köln
22.10.-24.10.2024 online
26.11.-28.11.2024 München

Hacking und Härtung von Windows-Infrastrukturen

Diese dreitägige Schulung widmet sich vollständig der Sicherheit von Windows-Infrastrukturen, wie sie heute typischerweise in Unternehmensnetzwerken betrieben werden. Hierbei liegt der Fokus auf der Verwendung der beiden Microsoft-Verzeichnisdienste Active Directory und Azure Active Directory.

Zunächst behandeln unsere erfahrenen Trainer wichtige Grundlagen zur Funktionsweise der Verzeichnisdienste (wie z.B. Protokollgrundlagen), dann werden ausgewählte Angriffsvektoren besprochen, demonstriert oder auch in Hands-on-Übungen von den Teilnehmern praktisch ausgenutzt. Hierbei lernen die Teilnehmer unter anderem den Einsatz von Open-Source-Hacking-Werkzeugen kennen. Das Ziel ist, Sicherheitslücken in der eigenen Infrastruktur zu finden und sie daraufhin zu schließen.

Im Rahmen dieser Schulung diskutieren wir typische Bedrohungsszenarien in Active-Directory-Infrastrukturen. Sie erfahren, wie Sie durch die Einführung des Microsoft-Tiering-Modells (aka Enterprise Access Model), das als Grundlage für ein Konzept zur sicheren Administration der Infrastruktur dient, die vorhandene Angriffsfläche deutlich reduzieren können.

In unserer Schulungsumgebung lernen Sie relevante Konfigurationseinstellungen und die Handhabung ausgewählter Werkzeuge kennen.

Zielgruppe: Administratoren, SOC-Mitglieder, „Blue Team“- oder „Red Team“-Mitglieder sowie (Projekt)Verantwortliche im Bereich Windows-Administration.

Voraussetzung: Die Teilnehmer sollten über solide Administrationserfahrung im Windows-Umfeld verfügen. Grundlegende Erfahrung in der Administration von Active Directory und Azure Active Directory sowie Vorwissen zu gängigen Angriffswerkzeugen und -vektoren sind von Vorteil, um den größten Schulungseffekt zu erzielen.

Dauer: 3 Tage **Preis:** 2.400,- Euro

Termin

05.06.-06.06.2024 online
25.09.-26.09.2024 Ludwigsburg
03.12.-04.12.2024 Köln

Crashkurs IT- und Informationssicherheit

Bedrohungen und Maßnahmen heute

In diesem Training werden theoretische und praktische Grundlagen der IT- und Informationssicherheit durch Vortrag, Diskussion und anhand von Beispielen aus der Praxis vermittelt. Der Trainer ist seit mehr als 20 Jahren als Berater tätig und kann daher umfassende und aktuelle Praxiserfahrungen in die Schulung einbringen.

Nach einer kurzen Einführung werden zunächst Begriffe und Grundlagen der IT- und Informationssicherheit ausführlich erläutert und elementare Zusammenhänge dargestellt. Anschließend erhalten die Teilnehmer anhand ausgewählter Beispiele einen umfassenden Einblick in die aktuell wichtigsten Bedrohungspotenziale und Angriffstechniken.

Daraufhin wird ein sehr ausführlicher Überblick über das gesamte Spektrum an heute zur Verfügung stehenden Maßnahmen zur IT- und Informationssicherheit gegeben.

Zum Abschluss wird der Bereich des Informationssicherheits- und Risikomanagements einschließlich der IT-Grundschutzvorgehensweise des BSI vertiefend betrachtet.

Die Teilnehmer sind nach dem Training in der Lage, die Begrifflichkeiten der IT- und Informationssicherheit richtig einzuordnen. Zudem können sie die Bedrohungslage für ihr Unternehmen einschätzen und passende Maßnahmen ableiten.

Zielgruppe: (Quer-)Einsteiger im Bereich IT- und Informationssicherheit und Manager, die gerne einen groben Überblick über Bedrohungen und Maßnahmen sowie über das Management der IT- und Informationssicherheit erhalten möchten

Voraussetzung: Einfache Grundkenntnisse in der IT

Dauer: 2 Tage **Preis:** 1.995,- Euro

Termine

02.07.-03.07.2024 online
20.11.-21.11.2024 online

Sicherheit in Azure-Cloud-Umgebungen

Unsere erfahrenen Trainer stellen Ihnen in diesem Training sicherheitsrelevante Funktionen der Microsoft-Azure-Cloud vor. Des Weiteren werden Konfigurationsmöglichkeiten sowie Maßnahmen für die Administration und den sicheren Betrieb von Azure-Umgebungen präsentiert.

Ausgehend von typischen Bedrohungsszenarien lernen Sie mithilfe von Hands-on-Übungen und Demonstrationen, welche Sicherheitsaspekte beim Design von Cloud-Architekturen, bei der Konfiguration und dem Betrieb beachtet werden sollten.

Im Rahmen dieser Schulung erörtern wir mit Ihnen zunächst typische Bedrohungsszenarien und Risiken in Cloud-Umgebungen.

Des Weiteren werden die spezifischen Risiken in Azure-Cloud-Umgebungen diskutiert und Maßnahmen vorgestellt, um die erörterten Risiken zu minimieren.

Darüber hinaus zeigen wir typische organisatorische und technische Herausforderungen des sicheren Betriebs einer Azure-Cloud-Umgebung auf und diskutieren mögliche Lösungsansätze.

Jedem Teilnehmer steht für den Verlauf der Schulung eine Übungsumgebung in Azure zur Verfügung, um die vermittelten Inhalte während der Schulung praktisch umzusetzen.

Die Teilnehmer haben am Ende der Schulung ein tieferes Verständnis für mögliche Bedrohungen und können die Maßnahmen und Empfehlungen zur Absicherung von Azure-Cloud-Umgebungen zukünftig effizient umsetzen.

Zielgruppe: Sicherheitsverantwortliche, Administratoren, IT-Architekten, Verantwortliche im Bereich Cloud

Voraussetzung: Grundkenntnisse zu Azure-Funktionen sind von Vorteil.

Dauer: 2 Tage **Preis:** 1.995,- Euro

Termine

11.06.-12.06.2024 online
06.11.-07.11.2024 online

Sicherheit in AWS-Cloud-Umgebungen

Im Rahmen der Schulung stellen wir sicherheitsrelevante Funktionen der AWS-Cloud vor. Des Weiteren werden Konfigurationsmöglichkeiten sowie Maßnahmen für die Administration und den sicheren Betrieb von AWS-Cloud-Umgebungen präsentiert.

Unsere Trainer erörtern die spezifischen Risiken in AWS-Cloud-Umgebungen und stellen Maßnahmen vor, um diese Risiken zu minimieren.

Hierbei geht es um folgende Aspekte:
- Sicherer Aufbau einer AWS-Infrastruktur
- Absicherung der Cloud
- Berechtigungsmanagement
- Logging
- Serverless Computing

Darüber hinaus zeigen wir typische organisatorische und technische Herausforderungen des sicheren Betriebs einer AWS-Cloud-Umgebung auf und diskutieren mögliche Lösungsansätze.

Jedem Teilnehmer steht für den Verlauf der Schulung eine Übungsumgebung in AWS zur Verfügung, um die vermittelten Inhalte während der Schulung praktisch umzusetzen.

Die Teilnehmer haben am Ende der Schulung ein tieferes Verständnis für mögliche Bedrohungen und können die Maßnahmen und Empfehlungen zur Absicherung von AWS-Cloud-Umgebungen zukünftig effizient umsetzen.

Zielgruppe: Sicherheitsverantwortliche, Administratoren, IT-Architekten, Verantwortliche im Bereich Cloud

Voraussetzung: Grundkenntnisse zu AWS-Funktionen sind von Vorteil.

Dauer: 2 Tage **Preis:** 1.995,- Euro

10.06.-13.06.2024 online
11.11.-15.11.2024 Ludwigsburg

ISO/IEC 27001 Lead Auditor

(Das Training findet in englischer Sprache statt.)

Die ISO/IEC 27001-Lead-Auditor-Schulung vermittelt Ihnen das notwendige Fachwissen, um ein Audit des Informationssicherheits-managementssystems (ISMS) auszuführen. Dabei sollen weitgehend anerkannte Auditprinzipien, -verfahren und –techniken angewendet werden. In dieser Schulung erwerben Sie die notwendigen Kenntnisse und Fähigkeiten, um interne und externe Audits in Übereinstimmung mit ISO 19011 und dem Zertifizierungsprozess nach ISO/IEC 17021-1 zu planen und durchzuführen.

Mithilfe praktischer Übungen beherrschen Sie schnell die erforderlichen Auditierungstechniken und können kompetent ein Auditprogramm und ein Auditteam führen sowie die Kommunikation mit Kunden und die Lösung von Konflikten übernehmen.

Am letzten Tag der Schulung können Sie die Prüfung ablegen. Wenn Sie die Prüfung bestanden haben und über das notwendige Fachwissen verfügen, können Sie die Qualifikation des “PECB Certified ISO/IEC 27001 Lead Auditor” beantragen. Dieses Zertifikat bestätigt, dass Sie über die Fähigkeiten und Kompetenzen verfügen, um Organisationen nach Best Practices zu auditieren.

Das Training basiert auf Theorien und Best Practices, die bei ISMS-Audits Anwendung finden. Die praktischen Übungen basieren auf einer Fallstudie mit Rollenspiel und Diskussion. Die Praxistests ähneln der Zertifizierungsprüfung.

Beim Online-Training findet die Prüfung an einem selbst auszuwählenden Termin statt.

Zielgruppe: Auditoren, Manager und Berater; Personen, die für die Einhaltung der ISMS-Anforderungen verantwortlich sind; technische Experten

Voraussetzung: Ein grundlegendes Verständnis von ISO/IEC 27001 und umfassende Kenntnisse der Auditprinzipien

Dauer: 4,5 Tage **Preis:** 2.450,- Euro inkl. Prüfungsgebühr

Termine

15.04.-19.04.2024 Ludwigsburg
07.10.-10.10.2024 online

ISO/IEC 27001 Lead Implementer

(Das Training findet in englischer Sprache statt.)

Das ISO/IEC 27001-Lead-Implementer-Training vermittelt den Teilnehmern das Wissen, wie man eine Organisation bei der effektiven Planung, Implementierung, Verwaltung, Überwachung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS) unterstützt.

Bedrohungen und Angriffe auf die Informationssicherheit nehmen zu und entwickeln sich ständig weiter. Die beste Form der Verteidigung gegen diese Bedrohungen und Angriffe ist die ordnungsgemäße Implementierung und Verwaltung von Informationssicherheitsmaßnahmen und bewährten Verfahren. Informationssicherheit ist auch eine zentrale Erwartung und Forderung von Kunden, Gesetzgebern und anderen Beteiligten.

Dieses Training soll die Teilnehmer auf die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) auf der Grundlage von ISO/IEC 27001 vorbereiten. Er zielt darauf ab, ein umfassendes Verständnis der Best Practice eines ISMS und einen Rahmen für dessen kontinuierliches Management und Verbesserung zu vermitteln.

Nach dem Besuch des Trainingskurses können Sie die Prüfung ablegen. Wenn Sie die Prüfung erfolgreich bestehen, können Sie ein „PECB Certified ISO/IEC 27001 Lead Implementer“-Zertifikat beantragen, das Ihre Fähigkeit und Ihr praktisches Wissen zur Implementierung eines ISMS auf der Grundlage der Anforderungen von ISO/IEC 27001 nachweist.

Beim Online-Training findet die Prüfung an einem selbst auszuwählenden Termin statt.

Zielgruppe: Manager und Berater; IT-Fachberater, die in der Lage sein möchten, ein ISMS zu implementieren; Personen, die für die Einhaltung der ISMS-Anforderungen verantwortlich sind; Mitglieder eines ISMS-Teams

Voraussetzung: Grundlegende Kenntnisse der ISMS-Konzepte und der ISO/IEC 27001

Dauer: 4,5 Tage **Preis:** 2.450,- Euro inkl. Prüfungsgebühr

Inhouse-Trainings

Alle Schulungen bieten wir Ihnen selbstverständlich gerne auch als Inhouse-Trainings an. Die einzelnen Schulungsinhalte können wir bei Interesse speziell an die Wünsche und Anforderungen Ihres Unternehmens anpassen.

Ergänzt wird unser Trainingsangebot durch die Inhouse-Schulungen **„IT-Sicherheit für Strategen & Manager“** und **„IT-Sicherheit für Entwickler“**. Letzere möchten wir Ihnen nachfolgend im Überblick kurz vorstellen.

IT-Sicherheit für Entwickler

Sensibilisierung und sichere Entwicklung von Web-Applikationen

Um Entwickler für Schwachstellen in Web-Applikationen zu sensibilisieren und zugleich wichtige Gegenmaßnahmen aufzuzeigen, bieten wir unseren Kunden eine spezielle Schulung zu diesem Thema an. Sie enthält Elemente aus unserer Schulung Hacking Extrem Web-Applikationen und zusätzlich einen Workshop zur sicheren Entwicklung.

Typischerweise führen wir diese Schulung dreitägig durch: In den ersten beiden Tagen behandeln wir ausgewählte Themen der Schulung Hacking Extrem Web-Applikationen, um die Denkweise und Techniken von Angreifern zu vermitteln. Am dritten Tag stellen wir wesentliche Maßnahmen vor, die beim Design und bei der Entwicklung von Anwendungen berücksichtigt werden sollten, um die zuvor behandelten Schwachstellen zu vermeiden.

Darüber hinaus können wir auf Ihre individuellen Fragen zur sicheren Entwicklung auf den bei Ihnen eingesetzten Plattformen eingehen und Quelltext-Beispiele von Ihnen diskutieren.

Zielgruppe: Entwickler, Architekten und Sicherheitsverantwortliche

Dauer: Üblicherweise 2-3 Tage

Preis: Nach Vereinbarung

Weitere Informationen finden Sie unter training.cirosec.de

Teilnahmebedingungen

Trainingsgebühr: Die Trainingsgebühr versteht sich zzgl. MwSt., einschließlich der Trainingsunterlagen, Tagungsgetränke und Mittagessen.

Frühbucherrabatt: Bei einer Anmeldung bis acht Wochen vor Beginn des Trainings erhalten Sie einen Frühbucherrabatt von 5 %. Ausgenommen davon sind unsere Zertifizierungstrainings.

Teilnahmebedingungen: Die Teilnahmegebühr ist nach Rechnungserhalt zu entrichten. Bei Stornierung einer Anmeldung bis zwei Wochen vor Seminarbeginn wird eine Bearbeitungsgebühr von EUR 120,- zzgl. MwSt. erhoben. Bei Stornierung bis eine Woche vor Beginn wird die halbe, bei späterer Absage oder Fehlen des Teilnehmers die volle Gebühr berechnet.

Mit der Anmeldung werden die Teilnahmebedingungen anerkannt. Es gelten unsere allgemeinen Geschäftsbedingungen.

Anmeldung
Melden Sie sich einfach auf unserer Website **www.cirosec.de** an.

cirosec GmbH
Ferdinand-Braun-Straße 4 | 74074 Heilbronn
T +49 7131 59455-0
F +49 7131 59455-99
www.cirosec.de

cirosec