IT-Sicherheitstrainings

2. Halbjahr 2026

cirosec

Herzlich willkommen bei den Trainings von 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.

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.

Sowohl unser neues Training **„IR-Sofortmaßnahmen“** als auch die Schulung **„IT-Sicherheit für Entwickler“** bieten wir Ihnen ausschließlich als Inhouse-Schulungen an.

Weitere Informationen finden Sie unter training.cirosec.de

23.09.-24.09.2026 online
09.12.-10.12.2026 online

Malware und Ransomware — Hintergründe, Erkennung, Schutz und Reaktion

Malware und Ransomware haben sich zu einer allgegenwärtigen Bedrohung entwickelt. Immer mehr Unternehmen sind betroffen, werden erpresst und ihre Betriebsabläufe massiv gestört.

Die Schulung vermittelt das nötige Wissen über die Angreifer, ihre Techniken und Vorgehensweisen. Zudem werden sinnvolle Sicherheitsmaßnahmen vorgestellt, um sich wirksam vor Angriffen zu schützen, sie im Ernstfall 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.

Anschließend 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 näher beleuchtet und voneinander abgegrenzt.

Weitere Themen sind die richtige Reaktion auf Vorfälle, die nötige Vorbereitung für das Incident Management und die Wiederherstellung sowie Möglichkeiten zur Analyse.

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

Zielgruppe: Sicherheitsverantwortliche, Administratoren, CERTs und SOC-Mitglieder

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

Dauer: 2 Tage **Preis: 1.995,- €**

08.12.-09.12.2026 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 weiteren Verlauf 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,- €**

22.09.2026 online
01.12.2026 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 gehen wir auch darauf ein, welche ergänzenden Anforforderungen für KRITIS-relevante Unternehmen bestehen.

Darauf aufbauend erörtern wir detailliert anhand von Fallbeispielen ein angemessenes Vorgehen bei einem Verdacht auf einen Hackerangriff, auf Datenmissbrauch, auf Datendiebstahl, auf Datenlöschung oder auch bei unberechtigter Nutzung firmeneigener Kommunikationsmöglichkeiten.

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,- €**

10.11.-13.11.2026 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.

Das Gelernte wird in mehreren Laborübungen in die Praxis umgesetzt. Dabei stehen jedem Teilnehmer zahlreiche Werkzeugen und Exploits zur Verfügung, die weit über die üblichen Scanner hinausgehen. Neben einigen Aha-Erlebnissen können die Teilnehmer auf diese Weise sicherheitsrelevante Fragen realistisch einschätzen und bewerten.

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, des TCP/IP-Stacks und der Funktionsweise gängiger Protokolle sind von Vorteil.

Dauer: 4 Tage **Preis: 3.140,- €**

29.09.-01.10.2026 Ludwigsburg

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 Webfrontends oder Webservices anbieten, sondern auch, weil diese Systeme stets mit neuen Methoden angegriffen und manipuliert werden können.

Das Intensivtraining vermittelt Ihnen die Vorgehensweise der Angreifer sowie bekannte und weniger bekannte Angriffstechniken auf Webapplikationen mit den dahinter liegenden Datenbanken und Backends.

Der ausgesprochen praxisorientierte Stil ist durch zahlreiche Laborübungen angereichert. Dabei stehen jedem Teilnehmer zahlreiche Werkzeugen und Exploits zur Verfügung, die weit über die üblichen Scanner hinausgehen. Neben einigen Aha-Erlebnissen können die Teilnehmer auf diese Weise sicherheitsrelevante Fragen realistisch einschätzen und bewerten.

Die Schulung deckt alle Schwachstellenarten der OWASP Top Ten ab.

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

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

Zielgruppe: Administratoren und Sicherheitsverantwortliche, die die Sicherheit auch durch die Brille des Angreifers betrachten und dabei sehr tief in dessen Welt eintauchen möchten, aber auch Entwickler von Webanwendungen sowie Administratoren von Webservern und E-Business-Systemen

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

Dauer: 3 Tage **Preis: 2.490,- €**

22.09.-24.09.2026 in Köln
08.12.-10.12.2026 in München

Hacking und Härtung von Windows-Betriebssystemen

Diese dreitägige Schulung widmet sich vollständig der Sicherheit der aktuellen Windows-Betriebssysteme Windows 10/11 und Server 2016/2019/2022.

Unsere erfahrenen Trainer stellen Ihnen sicherheitsrelevante Funktionen, deren Anforderungen und Konfigurationsmöglichkeiten sowie die Herausforderungen bei der Verwaltung und Administration dieser Systeme vor. Ausgehend von typischen Bedrohungsszenarien für Clients und Server lernen Sie mithilfe von Hands-on-Übungen und Demonstrationen, wie Sie die neuen Technologien und Möglichkeiten zur Absicherung dieser Systeme nutzen können.

Im Rahmen dieser Schulung diskutieren wir mit Ihnen zunächst typische Bedrohungsszenarien und zeigen beispielhafte Angriffe auf Windows-Maschinen in den unterschiedlichen Einsatzszenarien, zum Beispiel auf Laptops im Außendienst, Tower-PCs in der zentralen Verwaltung oder Server im internen Netzwerk.

Diesen Bedrohungsszenarien stellen wir im Verlauf der Schulung sinnvolle Härtungs- und Schutzmaßnahmen gegenüber.

Dadurch erhalten Windows-Administratoren ein tieferes Verständnis für mögliche Bedrohungen und IT-Sicherheitsverantwortliche können die Schutzfunktionen der Windows-Betriebssysteme kennenlernen.

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 sind mehrstufig aufgebaut, sodass einerseits erfahrene Windows-Administratoren noch gefordert werden und andererseits Einsteiger stets in der Lage sind, die vermittelten Inhalte nachzuvollziehen.

Dauer: 3 Tage **Preis: 2.490,- €**

20.10.-22.10.2026 in München
01.12.-03.12.2026 in Ludwigsburg

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 Entra ID.

Zunächst behandeln unsere erfahrenen Trainer wichtige Grundlagen zur Funktionsweise der Verzeichnisdienste (wie z. B. Protokollgrundlagen), anschließend werden ausgewählte Angriffsvektoren besprochen, demonstriert und in Hands-on-Übungen von den Teilnehmern praktisch ausgenutzt. Hierbei lernen die Teilnehmer unter anderem den Einsatz von Open-Source-Hacking-Werkzeugen kennen. Ziel ist es, Sicherheitslücken in der eigenen Infrastruktur zu finden und sie 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 (auch Enterprise Access Model genannt), 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. Die Auswirkungen einzelner Härtungsmaßnahmen und Funktionen demonstrieren wir Ihnen mithilfe gängiger, frei verfügbarer Angriffswerkzeuge.

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 Entra ID sowie Vorwissen zu gängigen Angriffswerkzeugen und -vektoren sind von Vorteil, um den größten Schulungseffekt zu erzielen.

Dauer: 3 Tage **Preis: 2.490,- €**

11.11.-12.11.2026 online

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,- € online / 2.090,- € vor Ort**

26.11.2026, 9-13 Uhr online

NIS-2-Schulung für die Geschäftsleitung

entspricht den BSI-Vorgaben

Mit dem NIS-2-Umsetzungsgesetz sind Unternehmen verpflichtet, ein systematisches Risikomanagement einzuführen, um Sicherheitsrisiken zu erkennen, geeignete Maßnahmen abzuleiten und deren Umsetzung sicherzustellen.

Besonders die Geschäftsleitung steht in der Verantwortung: Sie ist gesetzlich verpflichtet, ein wirksames Risikomanagement zu etablieren, dessen Umsetzung und Wirksamkeit zu überwachen und regelmäßig an Schulungen teilzunehmen.

In der Schulung vermitteln wir die zentralen Inhalte, die die Geschäftsleitung benötigt, um ihren gesetzlichen Pflichten nachzukommen.

Die Schulung folgt den Vorgaben der BSI-Handreichung für NIS-2-Geschäftsleitungsschulungen und bietet eine klare Orientierung im komplexen NIS-2-Regelwerk.

Die Schulung umfasst u. a. folgende Themen:

- Einordnung der NIS-2-Richtlinie und Abgrenzung zu anderen EU-Regelwerken wie CRA, DORA, DSGVO
- Betroffene Organisationen: „wesentliche“ und „wichtige“ Einrichtungen
- Zentrale Pflichten: Risikomanagement, Meldepflichten, Registrierung, Leitungsverantwortung
- Abhängigkeiten zwischen IT-Systemen, Prozessen und Diensten
- Grundlagen des Risikomanagements und typische Gefährdungen
- Auswirkungen von Risiken auf Geschäftsabläufe, Kunden und Compliance
- Strategien zur Risikobehandlung und Umgang mit Zielkonflikten
- Schnittstellen zum unternehmensweiten Risikomanagement
- Mindestanforderungen NIS-2-Richtlinie an Sicherheitsmaßnahmen
- Einhaltung des „Stands der Technik“, Überblick über wichtigste Sicherheitsmaßnahmen
- Dokumentationspflichten im Rahmen des Risikomanagements

Für Inhouse-Schulungen kann diese Schulung optional mit unserem Training „IT-Sicherheit für Strategen und Manager“ kombiniert werden.

Dauer: 4 Stunden **Preis: 490,- €**

17.11.-18.11.2026 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, ihrer Konfiguration und ihrem Betrieb beachtet werden sollten.

Zunächst erörtern wir mit Ihnen typische Bedrohungsszenarien und Risiken in Cloud-Umgebungen. Des Weiteren werden die spezifischen Risiken in Azure-Cloud-Umgebungen diskutiert und Maßnahmen vorgestellt, um diese 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: Von Vorteil sind Grundkenntnisse zur allgemeinen Arbeit auf der Kommandozeile und zu netzwerktechnischen Grundlagen.

Dauer: 2 Tage **Preis: 1.995,- €**

Inhouse-Schulung auf Anfrage

IR-Sofortmaßnahmen

Im Rahmen der eintägigen, praxisnahen Schulung vermitteln wir Ihren zuständigen Mitarbeitern Grundlagen der Incident Response und forensischer Analysen, sodass diese im Falle eines Sicherheitsvorfalls in kurzer Zeit selbstständig die richtigen Sofortmaßnahmen einleiten können.

Vor der eigentlichen Reaktion auf einen Vorfall und einer forensischen Untersuchung steht zunächst die Erkennung eines Vorfalls sowie die Bewertung, ob es sich dabei überhaupt um einen IT-Sicherheitsvorfall handelt, bei dem externe Unterstützung benötigt wird. Beim Hinzuziehen externer Spezialisten vergeht weitere Zeit, bis diese aktiv werden oder vor Ort sein können.

Während dieser Zeit ist es sinnvoll, bereits mit eigenem Personal erste Maßnahmen zu ergreifen, um Spuren zu sichern oder eine weitere Ausbreitung des Vorfalls zu stoppen. Zudem sind für die effektive Analyse, Bearbeitung und Eindämmung eines Vorfalls zahlreiche Vorbereitungen Ihrerseits notwendig, damit die erforderlichen Informationen bei Bedarf überhaupt zur Verfügung stehen und nötige Eingriffe in die IT-Infrastruktur schnell erfolgen können. Auch die erfolgreiche Wiederherstellung von IT-Systemen nach einem Vorfall hängt stark von einer guten Vorbereitung ab.

Grundlagen von IR und Forensik für Ihre Mitarbeiter:

- Richtige Durchführung erster Maßnahmen
- Bewertung verschiedener Situationen und passende Reaktionen
- Hilfe zur Selbsthilfe
- Übungen zur praktischen Vorgehensweise

Bei diesem Training stehen den Teilnehmern Notebooks mit diversen Werkzeugen zur Verfügung, um die erlernten Inhalte in Übungen selbst nachvollziehen zu können. Diese werden für die Dauer des Lehrgangs von cirosec bereitgestellt.

Zielgruppe: internes Incident-Response-Team und Administratoren, die bei einem Vorfall mitwirken

Dauer: 1 Tag **Preis: Nach Vereinbarung**

Inhouse-Schulung auf Anfrage

IT-Sicherheit für Entwickler

Sensibilisierung und sichere Entwicklung von Webapplikationen

Um Entwickler für Schwachstellen in Webapplikationen 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 ausgehend vom Application Security Verification Standard (ASVS) des Open Web Application Security Project (OWASP) 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 Quelltextbeispiele von Ihnen diskutieren. Auf Wunsch können auch wesentliche Maßnahmen zur Härtung von Web- und Applikationsservern behandelt werden.

Zielgruppe: Entwickler, Architekten und Sicherheitsverantwortliche

Dauer: 2-3 Tage **Preis: Nach Vereinbarung**

cirosec GmbH

Wir sind ein spezialisiertes Unternehmen mit Fokus auf Informationssicherheit, führen Penetrationstests und Red Teamings durch, unterstützen unsere Kunden bei der Incident Response und beraten sie im deutschsprachigen Raum bei Fragen der Informations- und IT-Sicherheit.

Gegründet wurde cirosec im Jahr 2002 von einem erfahrenen Team aus der IT-Sicherheitsbranche. Heute beschäftigt das Unternehmen über 80 festangestellte Mitarbeiter.

Die exzellent ausgebildeten Berater sind als Buchautoren oder Referenten internationaler Kongresse bekannt, verfügen über einen breiten Erfahrungsschatz aus einer teilweise mehr als 25-jährigen Tätigkeit im IT-Sicherheitsbereich und haben sich durch erfolgreiche Researchtätigkeiten einen Namen gemacht: Immer wieder entdecken sie neue, zuvor noch nicht veröffentlichte Schwachstellen in Standard-Software-Produkten.

Bei der Incident Response und Forensik bieten wir deutschlandweit eine 24/7-Erreichbarkeit inklusive garantierter Reaktionszeiten sowie einen umfassenden Leistungskatalog für gezielte Angriffe und IT-Sicherheitsvorfälle.

Darüber hinaus ist cirosec Veranstalter einer der größten IT-Sicherheitskonferenzen in Deutschland – der jährlich stattfindenden IT-Defense.

Teilnahmebedingungen

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

Frühbucherrabatt: Bei einer Anmeldung bis acht Wochen vor Beginn des Trainings erhalten Sie einen Frühbucherrabatt von 5 %.

Teilnahmebedingungen: Die Teilnahmegebühr ist nach Rechnungserhalt zu entrichten. Bei Stornierung einer Anmeldung bis zwei Wochen vor Seminarbeginn wird eine Bearbeitungsgebühr von 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.

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.

cirosec GmbH
Ferdinand-Braun-Straße 4
74074 Heilbronn
T +49 7131 59455-0
info@cirosec.de
www.cirosec.de

cirosec