IT-Sicherheitstrainings

2. Halbjahr 2020

cirosec

cirosec GmbH

Die **erfahrenen IT-Sicherheitsspezialisten** von cirosec führen Penetrationstests durch, beraten ihre Kunden herstellerneutral und setzen Lösungen kompetent um.

Das cirosec-Team zeichnet sich durch seine zahlreichen Experten aus, die als Buchautoren oder Referenten bekannt sind und die Kunden mit technischem und strategischem Sachverstand individuell beraten. Darüber hinaus verfügt das Team über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen.

Das **Angebotsspektrum** umfasst:

- Beratung, Konzepte, Reviews und Analysen
- Durchführung von Audits und Penetrationstests
- Incident Response und Forensik
- Konzeption, Evaluation und Implementierung von Lösungen
- Trainings & Awareness

Die Themenschwerpunkte der cirosec GmbH liegen auf modernen Schutzmaßnahmen für Unternehmen. Dazu gehören zum Beispiel:

- Schutz vor gezielten Angriffen (APTs), moderner Malware und Denial-of-Service-Angriffen
- Sicherheit von (mobilen) Endgeräten, Apps, Webapplikationen, Portalen und Webservices
- Nachvollziehbarkeit und Kontrolle administrativer Zugriffe
- Informationssicherheitsmanagement (ISMS)
- Cloud Security
- Windows-10-Sicherheit & Office 365
- IoT und Industrie 4.0
- Verwundbarkeits- und Risikomanagement

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

Je nach aktueller Situation finden unsere Trainings im vorgesehenen Tagungshotel oder alternativ online statt. Aktuelle Informationen hierzu finden Sie auf unserer Website.

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.

13.10.-16.10.2020 Ludwigsburg/online
01.12.-04.12.2020 Köln/online

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

Termine

07.07.-09.07.2020 online
10.11.-12.11.2020 Hamburg/online
15.12.-17.12.2020 München/online

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

15.09.-17.09.2020 München/online
03.11.-05.11.2020 Ludwigsburg/online

Hacking und Härtung von Windows-Systemen

In dieser Schulung zeigen unsere praxiserfahrenen Trainer, wie Hacker heute vorgehen, um Windows-Umgebungen zu übernehmen, und wie Sie sich dagegen schützen können.

In diversen Demonstrationen und praktischen Übungen zeigen wir typische Angriffe auf Windows-Clients und Windows-Server sowie auf die darauf betriebenen Dienste wie Microsoft IIS oder Microsoft SQL Server. Anhand dieser konkreten und für alle Teilnehmer nachvollziehbaren Angriffsszenarien präsentieren wir anschließend Möglichkeiten zur Härtung der Systeme mit (wenig) bekannten Bordmitteln oder frei verfügbaren Werkzeugen, um derartige Angriffe zu erschweren oder gar zu verhindern.

Um Ihre Infrastruktur zu schützen, müssen Sie gängige Techniken sowie die Ziele und das Vorgehen unterschiedlicher Angreifer kennen und verstehen. In der Schulung lernen Sie die dafür typischen Hacker-Werkzeuge kennen, die zur Grundausstattung eines jeden „Red Teams“ oder Hackers gehören. Die Verwendung ist primär darauf ausgelegt, die Ausnutzung unsicherer Konfigurationen zu demonstrieren sowie generelle Probleme in Windows-Umgebungen nachzuvollziehen. Unsere Schulungsumgebung sowie die gezeigten Angriffs- und Abwehrmöglichkeiten basieren auf den aktuellen Funktionen von Windows 10 Enterprise bzw. Windows Server 2016.

Zielgruppe: Sicherheitsverantwortliche, Administratoren, SOC-Mitglieder, „Blue Team“- oder „Red Team“-Mitglieder sowie (Projekt-)Verantwortliche im Bereich Windows oder Windows-Sicherheit, die nach Wegen zur Absicherung oder Prüfung ihrer Windows-Umgebung suchen

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

17.11.-19.11.2020 München/online

Sicherheit von Windows 10 im Unternehmen

Diese Schulung widmet sich vollständig der Sicherheit des aktuellen Client-Betriebssystems Windows 10. 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-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 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

24.11.-26.11.2020 Ludwigsburg/online

Forensik Extrem

Incident Handling & IT-Forensik im Unternehmen

In diesem Training werden aktuelle Methoden der Incident Response, des Incident Handling und der IT-Forensik vorgestellt.

Vor einer forensischen Untersuchung steht zunächst der Vorfall, der als solcher erkannt werden muss. Ihm folgt die unmittelbare Reaktion in Form der Incident Response. Sie versucht, den Vorfall zu erfassen und ihn für eine nachfolgende forensische Untersuchung aufzubereiten. Der ISO-27035-Standard dient als Leitfaden zur Erkennung und Behandlung von Sicherheitsvorfällen.

Im Rahmen der Schulung gehen wir zunächst auf die Möglichkeiten zur Erkennung von Sicherheitsvorfällen ein. Anschließend zeigen wir, wie anhand des ISO-27035-Standards eine systematische Vorgehensweise gewährleistet werden kann.

Darauf aufbauend wird anhand von Fallbeispielen das richtige Vorgehen bei einem Verdacht auf Hacker-Einbruch, Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung von firmeneigenen Kommunikationsmöglichkeiten detailliert erörtert. Auf einem zur Verfügung gestellten Laptop lernt jeder Teilnehmer anhand von Übungen, Spuren in IT-Systemen zu suchen, sie richtig zu sichern und zu interpretieren.

Nach Abschluss des Trainings können die Teilnehmer die Wege eines Einbrechers nachvollziehen. Sie wissen, wie sie einen Incident-Response-Prozess etablieren können und welche Anforderungen an die gerichtsfeste Sammlung, Speicherung und Auswertung digitaler Spuren als Beweismittel erfüllt werden müssen.

Behandelte Systeme: Windows, Linux und Unix

Zielgruppe: Administratoren, Sicherheitsverantwortliche, CERTs und betriebliche Ermittler

Voraussetzung: Grundlegende Kenntnisse in Windows, Linux und Unix. Von Vorteil sind Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern.

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

Termin

29./30.09.2020 Köln/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,- Euro

Termin

29./30.09.2020 Ludwigsburg/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

Termin

09./10.12.2020 Ludwigsburg/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

Termin

16.11.-20.11.2020 Ludwigsburg/online

Certified ISO 27001 Lead Auditor

(Das Training findet in englischer Sprache statt.)

Dieser Intensivkurs vermittelt Ihnen die nötigen Fachkenntnisse, um durch die Anwendung anerkannter Auditierungsprinzipien, -prozeduren und -techniken ein Informationssicherheitsmanagementsystem (ISMS) zu auditieren.

Im Laufe des Trainings erwerben Sie das Wissen und die Fertigkeiten, um interne und externe Audits konform zum Zertifizierungsprozess der Standards ISO 19011 und 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.

Sobald Sie die notwendigen Fachkenntnisse zur Durchführung eines solchen Audits erworben haben, können Sie an der Prüfung teilnehmen und das Zertifikat „PECB Certified ISO/IEC 27001 Lead Auditor“ beantragen. Das Zertifikat des PECB Lead Auditor ist der Nachweis dafür, dass Sie über die Fähigkeiten und Kompetenzen verfügen, Unternehmen anhand von Best Practices zu auditieren.

Das Training basiert auf Theorien und Best Practices, die bei ISMS-Audits Anwendung finden. Zur Veranschaulichung werden im Kurs Beispiele aus Fallstudien herangezogen. Die praktischen Übungen basieren auf einer Fallstudie mit Rollenspiel und Diskussion. Die Praxistests ähneln der Zertifizierungsprüfung.

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

Voraussetzung: Kenntnisse im Bereich Informationssicherheit und Managementprozesse

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

Termin

12.10.-16.10.2020 Ludwigsburg/online

Certified ISO 27001 Lead Implementer

(Das Training findet in englischer Sprache statt.)

Dieser Intensivkurs vermittelt Ihnen die nötigen Fachkenntnisse, um ein Unternehmen beim Aufbau, der Implementierung, dem Management und der Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 zu unterstützen.

Zusätzlich zu den genannten Fachkenntnissen erwerben Sie umfassendes Wissen über die Best Practices im Bereich ISMS zur Sicherung der sensiblen Informationen eines Unternehmens und zur Steigerung der allgemeinen Leistung und Wirksamkeit.

Sobald Sie alle wichtigen Konzepte von Informationssicherheitsmanagementsystemen verinnerlicht haben, können Sie an der Prüfung teilnehmen und das Zertifikat „PECB Certified ISO/IEC 27001 Lead Implementer“ beantragen. Das Zertifikat des PECB Lead Implementer ist der Nachweis dafür, dass Sie sowohl über die praktische Erfahrung als auch über die fachliche Fähigkeit verfügen, in einem Unternehmen ein ISMS nach ISO/IEC 27001 zu implementieren.

Das Training basiert auf Theorien und Best Practices, die bei der Implementierung eines ISMS Anwendung finden. Zur Veranschaulichung werden im Kurs Beispiele aus Fallstudien herangezogen. Die praktischen Übungen basieren auf einer Fallstudie mit Rollenspiel und Diskussion. Die Praxistests ähneln der Zertifizierungsprüfung.

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: Kenntnisse im Bereich Informationssicherheit und Managementprozesse

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