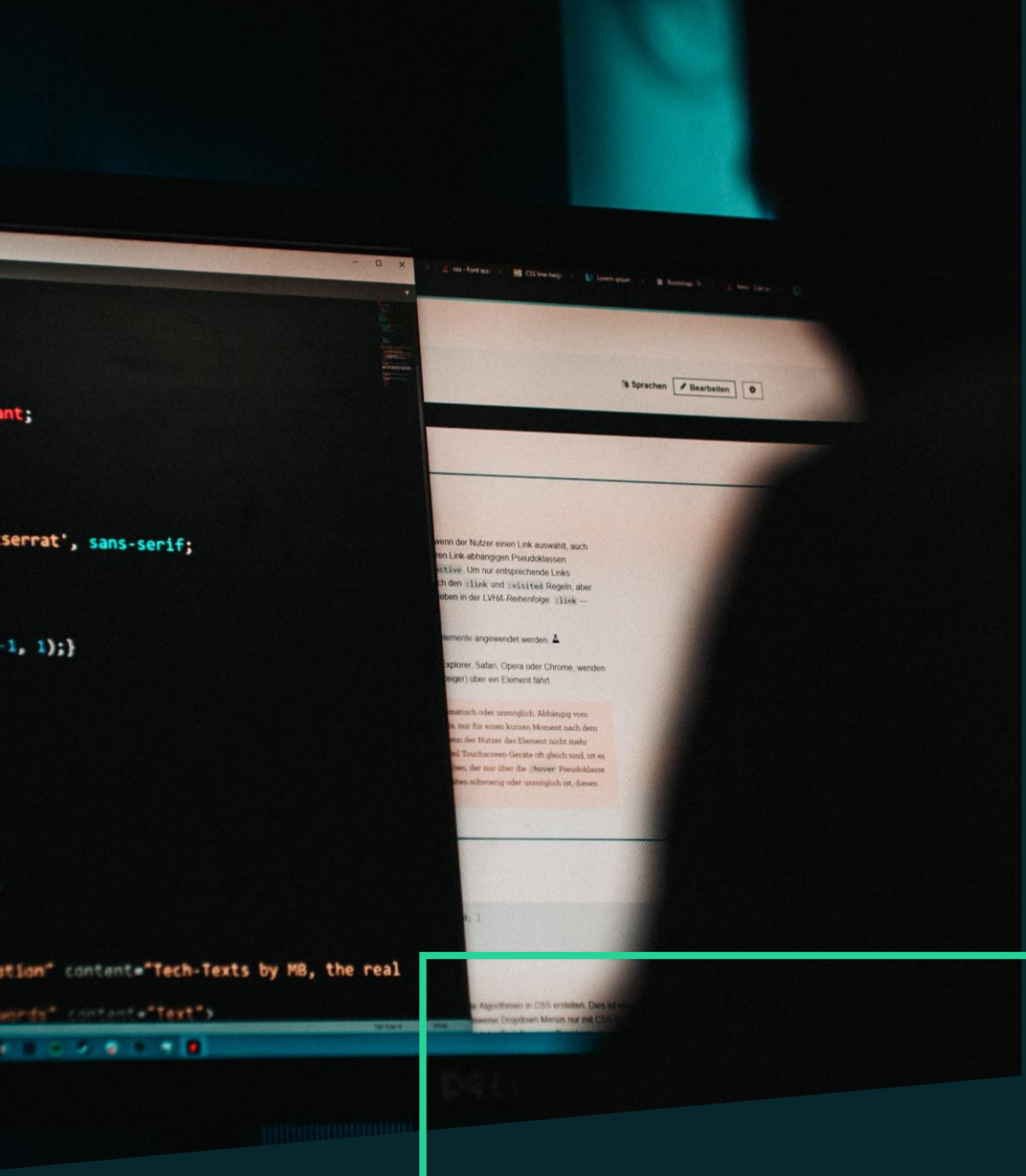
bitkom
akademie



Ethical Hacking & Pentesting

Praxiseinstieg in die digitale offensive Sicherheit

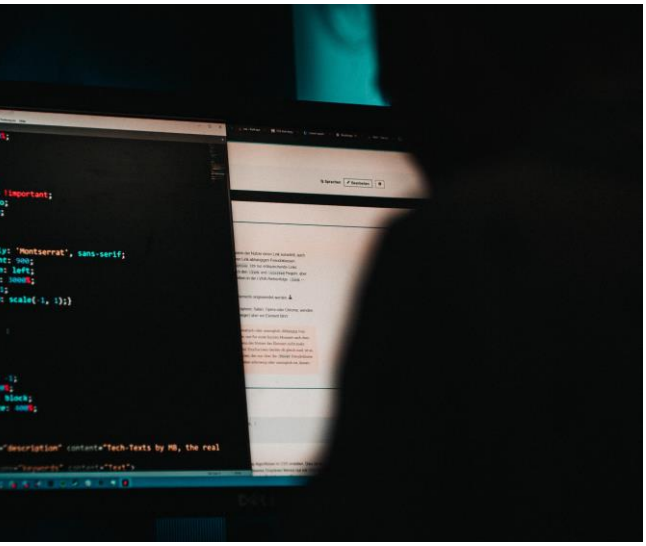
Ethical Hacking & Pentesting

Praxiseinstieg in die digitale offensive Sicherheit

Kurzbeschreibung

Um die IT-Sicherheit in Organisationen zu erhöhen und Cyberangriffe abzuwehren, ist es von erheblichem Vorteil, die Denkweise und Techniken von Hackern nachvollziehen zu können. In diesem Zusammenhang hat sich in der IT-Security das „Ethical Hacking“ als Methode etabliert, um im Auftrag des eigenen Unternehmens böswillige Angreifer zu imitieren. Auf diese Weise lassen sich zielgerichtet Schwachstellen in den eigenen Netzwerken und Systemen identifizieren.

Der dreitägige Workshop „Ethical Hacking & Pentesting" bieten Ihnen eine fundierte **Einführung in die Grundlagen des Hacking und Penetration-Testing**. Sie lernen wesentliche Techniken und Konzepte der offensiven IT-Sicherheit kennen. Durch eine Kombination aus theoretischen Grundlagen und praktischen Übungen werden Sie in die Lage versetzt, Sicherheitslücken zu erkennen und geeignete Gegenmaßnahmen für Ihr Unternehmen zu entwickeln.



Inhalt

- Einführung in die Grundlagen des Hacking und ethische Richtlinien
- Übersicht über gängige Hacking-Methoden und -Tools
- Netzwerksicherheit und Schwachstellenanalyse
- Praktische Hacking-Übungen
- Praktische Übungen zu Penetrationstests
- Methoden zur Erkennung und Abwehr von Cyberangriffen
- Grundlagen der Kryptographie und sichere Kommunikation
- Rechtliche Aspekte und Verantwortung im Bereich IT-Sicherheit
- Abschlussübung: Durchführung eines simulierten Penetrationstests

Was lernen Sie in diesem Workshop?

In diesem Workshop erwerben Sie grundlegende Kenntnisse im Bereich des **ethischen Hacking und Pentesting**. Anhand von praktischen Übungen vertiefen Sie Ihr Verständnis für typische Hacking-Angriffe und entwickeln Fähigkeiten, diese effektiv abzuwehren. Darüber hinaus erhalten Sie Einblicke in die rechtlichen Rahmenbedingungen und ethischen Verpflichtungen im Bereich der IT-Sicherheit. Außerdem wird Ihnen der Umgang mit **Penetration-Testing-Tools** wie Wireshark, NMAP, Metasploit und vielen weiteren näher gebracht.

BREDEX

bitkom akademie

Ethical Hacking & Pentesting

Praxiseinstieg in die digitale offensive Sicherheit

Zielgruppe

Der dreitägige Workshop ist maßgeschneidert für IT-Profis, die ihre Kenntnisse im Bereich der offensiven IT-Sicherheit vertiefen und das eigene Unternehmen proaktiv schützen möchten. Das Seminar eignet sich für alle, die das **ethische Hacking verstehen und in ersten Übungen praktisch anwenden** möchten. Grundkenntnisse in der IT-Sicherheit sind von Vorteil.

Sie sind IT-Sicherheitsbeauftragte/r, Systemadministrator/in oder in einer ähnlichen Position und möchten:

- Ihre Kompetenzen im Bereich ethisches Hacking ausbauen.
- Netzwerk- und Systemangriffe nicht nur abwehren, sondern auch vorhersagen und verhindern.
- Sicherheitslücken erkennen und schließen, bevor sie ausgenutzt werden.
- Die Sicherheitsarchitektur Ihres Unternehmens verstärken und optimieren.

Didaktischer Aufbau

In praktischen Einheiten vertiefen wir uns ins ethische Hacking und Pentesting. Nach einer theoretischen Einführung wenden Sie die Inhalte in **praktischen Hacking-Übungen und Simulationen** an. Sie erhalten Einblicke in Tools und Methoden, die zur Erkennung und Bewertung von Cyberrisiken notwendig sind.

Zusatzinformationen

- Der Praxis-Workshop findet in einer kleinen Gruppe von maximal **16 Personen statt**. Die Mindestteilnehmerzahl beträgt 5.
- Die Bitkom Akademie ist anerkannter Bildungsträger in Baden-Württemberg und Nordrhein-Westfalen. Teilnehmende haben im Rahmen des Bildungszeitgesetzes die Möglichkeit, Bildungsurlaub bzw. eine Bildungsfreistellung zu beantragen. Auf Anfrage erstellen wir Anträge auf Anerkennung unserer Seminar-Veranstaltungen auch in anderen Bundesländern.
- Dieser Online-Workshop wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie hier einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) bietet Ihnen diese Tabelle einen zusätzlichen Vergleich zu den jeweiligen Eigenschaften.
- Wir erklären ausdrücklich, dass beim Bitkom – Unterzeichner der Charta der Vielfalt – jede Person, unabhängig von Geschlecht, Nationalität, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung und Identität willkommen ist.

BREDEX

bitkom akademie

Seminarprogramm

Ethical Hacking & Pentesting

Tag 1

Einführung in das ethische Hacking

- Definition von ethischem Hacking
- Abgrenzung zu illegalen Aktivitäten
- Übersicht über gängige Hacking-Methoden und -Tools
- Bedeutung für die Unternehmenssicherheit

Grundlagen der IT-Sicherheit

- Vertraulichkeit, Integrität, Verfügbarkeit
- Sicherheitsrisiken und Bedrohungsmodelle
- Sicherheitsrichtlinien und Best Practices

Ethische und rechtliche Grundlagen

- Berufsethik des Pentesters
- Gesetzliche Rahmenbedingungen und Compliance
- Verantwortungsbewusster Umgang mit Sicherheitslücken

Tag 2

Netzwerksicherheit

- Grundlagen der Netzwerktechnologien
- Schwachstellen in Netzwerken
- Tools zur Netzwerkanalyse

Betriebssystem-Sicherheit

- Sicherheitsmechanismen von Betriebssystemen
- Häufige Schwachstellen und Angriffsszenarien
- Tools und Techniken zur Systemabsicherung

Anwendungssicherheit

- Sicherheitsprobleme in Webanwendungen
- SQL-Injection, Cross-Site Scripting, andere Angriffe
- Tools zur Erkennung von Anwendungsschwachstellen

BREDEX

bitkom akademie

Seminarprogramm

Ethical Hacking & Pentesting

Tag 3

Penetration Testing
- Ablauf eines Penetrationstests
- Erkennung und Ausnutzung von Schwachstellen
- Dokumentation und Reporting
- Einblick in Penetration-Testing-Tools wie Wireshark, NMAP, Metasploit

Social Engineering
- Psychologische Grundlagen
- Häufige Social-Engineering-Techniken
- Abwehrmaßnahmen und Schulung von Mitarbeitenden

Wireless Security
- Sicherheitsprobleme in Wireless-Netzwerken
- Angriffe auf WLAN-Strukturen
- Sicherheitskonzepte für Wireless-Netzwerke

Tag 4

Praktische Hacking-Übungen
- Setup der Testumgebung
- Durchführung von Angriffsszenarien
- Auswertung und Analyse der Ergebnisse

Kryptographie in der Praxis
- Grundlagen und Anwendungsgebiete
- Verschlüsselungswerkzeuge und -methoden
- Sichere Konfiguration von Verschlüsselungstechniken

Abschlussübung: Simulierter Penetrationstest
- Planung und Vorbereitung
- Durchführung des simulierten Angriffs
- Analyse und Präsentation der Ergebnisse

BREDEX

bitkom akademie

Ihr Referent

Ron Kneffel

Head of Data Privacy & IT Security
Bredex GmbH

Ron Kneffel ist seit über 20 Jahren Berater für Informationssicherheit und Informations- und Kommunikationstechnologien. Nach 15 Jahre Leitung eines inhabergeführten ITK-Beratungsunternehmen wechselte er vollständig in die Bereiche Digitalisierung und leitet heute bei der Bredex unter anderen den Bereich Informationssicherheit und nachhaltige Digitalisierung bei der Firma Bredex in Braunschweig.

Shortfacts

Termine, Veranstaltungsort und Preise

Die aktuellen Informationen entnehmen Sie bitte der ↗ Website der Bitkom Akademie.

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie