Cyber Security im Rechnungswesen (Präsenz)

Cyber-Angriffe erkennen und richtig handeln: Sicherheitsstrategien und praxisnahe Lösungen

Cyber-Angriffe sind ein Risiko, das exponentiell an Bedeutung gewinnt. Werden unternehmensrelevante Daten gehackt, sind Unternehmen oft schlagartig handlungsunfähig. Dieses Seminar gibt einen Einblick in das Thema Cyber Security und einen Überblick über die größten Gefahrenpotenziale und vermittelt dabei proaktive Sicherheitsstrategien. Du erfährst, wie moderne Technologien wie Künstliche Intelligenz und Automatisierung eingesetzt werden, um Angriffe frühzeitig zu erkennen und zu verhindern. Darüber hinaus wird erläutert, wie eine starke Sicherheitskultur im Unternehmen etabliert werden kann. In einer interaktiven Fallstudie wird eine realitätsnahe Bedrohung simuliert und erste Lösungsansätze für den Ernstfall erarbeitet.

Inhalte

Weiterbildung nach KI-VO Art. 4 für die Nachweispflicht von KI-Kompetenz

Einführung in Cyber Security
- Überblick über aktuelle Bedrohungen und Herausforderungen in der Cyber Security.
- Wichtige Begriffe und Konzepte: Bedrohungslandschaft, Schwachstellen, Risiken.

Prinzipien der proaktiven Sicherheit
- Definition und Bedeutung proaktiver Sicherheitsmaßnahmen.
- Vergleich: proaktive vs. reaktive Sicherheitsstrategien.

Entwicklung einer effizienten Sicherheitskultur
- Aufbau einer Sicherheitskultur innerhalb der Organisation.
- Schulungs- und Sensibilisierungsprogramme für Mitarbeitende.

Technologische Lösungen für proaktive Sicherheit
- Einsatz moderner Technologien: KI, maschinelles Lernen und Automatisierung.
- Tools und Plattformen zur Bedrohungserkennung und -prävention.
- Was steckt hinter ISMS, TISAX, DORA, NIS-2?

Case Study: Erfolgreiche Implementierung proaktiver Sicherheitsmaßnahmen
- Präsentation unterschiedlicher aktueller Angriffs- und Betrugsszenarien.
- Diskussion von Herausforderungen und Lösungsansätzen im Unternehmen.

Management von Cyber-Security-Risiken
- Identifizierung und Bewertung von Risiken.
- Strategien zur Risikominderung und -überwachung.

Interaktive Gruppenarbeit „Fallstudie Ransomware-Angriff“
- Arbeiten an einem fiktiven Szenario für einen Angriff auf das Unternehmen.
- Präsentation der Ergebnisse und Diskussion.

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

- Lerne aktuelle Cyber-Bedrohungen zu verstehen und Risiken kompetent einzuschätzen.
- Erfahre, wie proaktive Sicherheitsstrategien helfen, Angriffe frühzeitig zu erkennen und zu verhindern.

- Erfahre, wie man moderne Technologien wie KI und Automatisierung gezielt einsetzt, um mit IT-Expert:innen auf Augenhöhe zu diskutieren.
- Lerne durch die Simulation eines Cyber-Angriffs, wie man sich im Ernstfall professionell verhält.

Methoden

Impulsvortag, Diskussionen und direkter Austausch mit dem Experten und im Kreis der Teilnehmenden, Best-Practice-Beispiele und Handlungsempfehlungen.

Teilnehmer:innenkreis

Leiter Rechnungswesen und CFO, Geschäftsleitung, Finanzverantwortliche, leitende Angestellte und Expert:innen insbesondere aus dem Rechnungswesen und dem Controlling oder der IT.

Diese Veranstaltung ist auch als Modul buchbar von:

Expertenprogramm für Digitalisierung und KI im Rechnungswesen

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:
https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges

Trainer:in

Peter Kestner
Unabhängiger Sicherheitsberater
Firmengründer
Aufsichtsrat
Keynote Speaker
Trainer
Bestseller Autor

Beruflicher Werdegang:
- Ex Hacker / Blackhat
- Dipl. Informatiker
- Oracle, Director Cyber Security EMEA
- Deloitte Partner, Cyber Security Government & Defence

- KPMG Partner, Cyber Security,
Global Rep. DE

Schwerpunkte:
Cyber Security, Cyber Crime, Cyber Terrorismus, Betriebssysteme, Netzwerke, Datenbanken, KI
Social Engineering, Kryptographie, Steganographie, Strategie & Taktik für Angri und Verteidigung

Details zur Weiterbildung

Seminar | Präsenz

1 Tag

Termine

06.11.2026
München/Feldkirchen
Veranstaltungsort
Hotel Bauer Feldkirchen

Tage & Uhrzeit
Freitag, 06.11.2026
09:00 Uhr - 17:00 Uhr

09.02.2027
Berlin
Veranstaltungsort
Hotel Berlin, Berlin

Tage & Uhrzeit
Dienstag, 09.02.2027
09:00 Uhr - 17:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41300

Teilnahmegebühr

€ 790,- zzgl. MwSt.
€ 940,10 inkl. MwSt.
Die angegebene Teilnahmegebühr beinhaltet

- ein gemeinsames Mittagessen pro vollem Seminartag,
- Pausenverpflegung und
- umfangreiche Arbeitsunterlagen.

Die Übernachtungskosten im Hotel werden von den Teilnehmenden direkt mit dem Hotel abgerechnet. Für die Hotelbuchung findest du in deiner Lernumgebung ein Reservierungsformular.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41300
E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:
https://www.haufe-akademie.de/faqs

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.
Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.

Haufe Akademie GmbH & Co. KG
Munzinger Straße 9, 79111 Freiburg, www.haufe-akademie.de, Beratung: Tel.: +49 761 595339-00, service@haufe-akademie.de

Cyber Security im Rechnungswesen (Live-Online)

Cyber-Angriffe erkennen und richtig handeln: Sicherheitsstrategien und praxisnahe Lösungen

Cyber-Angriffe sind ein Risiko, das exponentiell an Bedeutung gewinnt. Werden unternehmensrelevante Daten gehackt, sind Unternehmen oft schlagartig handlungsunfähig. Dieses Seminar gibt einen Einblick in das Thema Cyber Security und einen Überblick über die größten Gefahrenpotenziale und vermittelt dabei proaktive Sicherheitsstrategien. Du erfährst, wie moderne Technologien wie Künstliche Intelligenz und Automatisierung eingesetzt werden, um Angriffe frühzeitig zu erkennen und zu verhindern. Darüber hinaus wird erläutert, wie eine starke Sicherheitskultur im Unternehmen etabliert werden kann. In einer interaktiven Fallstudie wird eine realitätsnahe Bedrohung simuliert und erste Lösungsansätze für den Ernstfall erarbeitet.

Inhalte

Einführung in Cyber Security
- Überblick über aktuelle Bedrohungen und Herausforderungen in der Cyber Security.
- Wichtige Begriffe und Konzepte: Bedrohungslandschaft, Schwachstellen, Risiken.

Prinzipien der proaktiven Sicherheit
- Definition und Bedeutung proaktiver Sicherheitsmaßnahmen.
- Vergleich: proaktive vs. reaktive Sicherheitsstrategien.

Entwicklung einer effizienten Sicherheitskultur
- Aufbau einer Sicherheitskultur innerhalb der Organisation.
- Schulungs- und Sensibilisierungsprogramme für Mitarbeitende.

Technologische Lösungen für proaktive Sicherheit
- Einsatz moderner Technologien: KI, maschinelles Lernen und Automatisierung.
- Tools und Plattformen zur Bedrohungserkennung und -prävention.
- Was steckt hinter ISMS, TISAX, DORA, NIS-2?

Case Study: Erfolgreiche Implementierung proaktiver Sicherheitsmaßnahmen
- Präsentation unterschiedlicher aktueller Angriffs- und Betrugsszenarien.
- Diskussion von Herausforderungen und Lösungsansätzen im Unternehmen.

Management von Cyber-Security-Risiken
- Identifizierung und Bewertung von Risiken.
- Strategien zur Risikominderung und -überwachung.

Interaktive Gruppenarbeit „Fallstudie Ransomware-Angriff“
- Arbeiten an einem fiktiven Szenario für einen Angriff auf das Unternehmen.
- Präsentation der Ergebnisse und Diskussion.

Weiterbildung nach KI-VO Art. 4 für die Nachweispflicht von KI-Kompetenz

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

- Lerne aktuelle Cyber-Bedrohungen zu verstehen und Risiken kompetent einzuschätzen.
- Erfahre, wie proaktive Sicherheitsstrategien helfen, Angriffe frühzeitig zu erkennen und zu verhindern.

- Erfahre, wie man moderne Technologien wie KI und Automatisierung gezielt einsetzt, um mit IT-Expert:innen auf Augenhöhe zu diskutieren.
- Lerne durch die Simulation eines Cyber-Angriffs, wie man sich im Ernstfall professionell verhält.

Methoden

Impulsvortag, Diskussionen und direkter Austausch mit dem Experten und im Kreis der Teilnehmenden, Best-Practice-Beispiele und Handlungsempfehlungen.

Teilnehmer:innenkreis

Leiter Rechnungswesen und CFO, Geschäftsleitung, Finanzverantwortliche, leitende Angestellte und Expert:innen insbesondere aus dem Rechnungswesen und dem Controlling oder der IT.

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:
https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges

Trainer:in

Peter Kestner
Unabhängiger Sicherheitsberater
Firmengründer
Aufsichtsrat
Keynote Speaker
Trainer
Bestseller Autor

Beruflicher Werdegang:
- Ex Hacker / Blackhat
- Dipl. Informatiker
- Oracle, Director Cyber Security EMEA
- Deloitte Partner, Cyber Security Government & Defence
- KPMG Partner, Cyber Security, Global Rep. DE

Schwerpunkte:
Cyber Security, Cyber Crime, Cyber Terrorismus, Betriebssysteme, Netzwerke, Datenbanken, KI

Social Engineering, Kryptographie, Steganographie, Strategie & Taktik für Angri und Verteidigung

Details zur Weiterbildung

Seminar | Online

1 Tag

Starttermine

16.09.2026
Live-Online
Durchführung
zoom

Modulzeiten
Mittwoch, 16.09.2026
09:00 Uhr - 17:00 Uhr

11.03.2027
Live-Online
Durchführung
zoom

Modulzeiten
Donnerstag, 11.03.2027
09:00 Uhr - 17:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41302

Teilnahmegebühr

€ 790,- zzgl. MwSt.
€ 940,10 inkl. MwSt.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41300
E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:
https://www.haufe-akademie.de/faqs

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.
Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.