22. Januar 2026 · 13:00–16:30 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

Cyberrisiken – Aktuelle Sicherheitslücken und wirksame (Gegen-)Maßnahmen

Banken-Praxis-Seminar

- Cyberrisiken: Sicherheitslücken, Gefahren, wirksame Maßnahmen
- Krisenmanagement, Schadensminimierung, Forensische Aufklärung
- Schnelligkeit als entscheidender Erfolgsfaktor bei IKT-Vorfällen
- Haftungsfragen bei Cyber-Angriffen – Wer haftet?
- Unterschätzte Angriffsvektoren für Cyber-Angriffe
- DORA-konforme Schwachstellenanalyse und PenTestings
- Maßnahmen bei Industriespionage in Banken (APT-Abwehr)

Referenten

Jan Spittka
Partner, Rechtsanwalt
Clyde & Co Europe LLP, Düsseldorf

Helmut Brechtken
Partner, Head of Digital Forensic Incidence Response (DFIR), Deloitte GmbH WPG, Köln

Christian Horn
Senior Managing Consultant, Experte für Penetration Testing & Cyber Security, ProSec GmbH

Gordon Shepherd
Managing Consultant, Experte für IT-Management & ITSM
ProSec GmbH

Programm

Jan Spittka, Clyde & Co · **13:00-14:00 Uhr**

Aktuelle Bedrohungslage durch Cyberangriffe und Ransomware

- Aktuelle Lage der IT-Sicherheit und Cyber-Sicherheit in Deutschland sowie im deutschen Finanzwesen
- Identifikation kritischer Geschäftsprozesse
- Typischer Ablauf eines Cyber-Incidents anhand eines konkreten Fallbeispiels aus der Praxis
- Wirksames Schwachstellen-Management
- Haftung für Datenschutzverstöße

Helmut Brechtken, Deloitte · **14:15-15:15 Uhr**

Cybercrime und Cyber-Angriffe: Aktuelle Sicherheitslücken, Gefahren und wirksame (Gegen-)Maßnahmen

- Deutliche Zunahme der Cyber-Angriffe (Cybercrime, eSpionage und eSabotage) auf Unternehmen, Organisationen und kritische Infrastrukturen
- Cyberkriminalität im Dreiklang »Krisenmanagement – Schadensminimierung/Abwehr – digital-forensische Aufklärung«
- Fallbeispiele aus der Cyber-Abwehr und der digital-forensischen Untersuchungspraxis
- Schnelligkeit als entscheidender Erfolgsfaktor bei Sicherheitsvorfällen
- Ansätze zur Cybercrime-Prävention

Christian Horn und **Gordon Shepherd, ProSec**
15:30-16:30 Uhr

Penetrationstests, Physical-Tests und DORA-konforme Schwachstellen-Analysen – Ethical Hacking für digitale Resilienz

- Realistische IT-Sicherheitsanalysen
- Effiziente IT-Sicherheit trotz hoher Aufsichts-Anforderungen
- IT-Sicherheit als Strategie – klare Entscheidungen, Richtung und Ziele der IT-Sicherheit
- Messung des Reifegrads der IT-Sicherheit und der Schutzbedarfsanalyse
- Ausgestaltung institutsindividueller, angemessener PenTests und Schwachstellen-Analysen
- Maßnahmen bei Industriespionage in Banken und Unternehmen (APT-Abwehr)

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Anforderungen an den Umgang mit Cyber-Risiken sowie deren Erkennung, Abwehr oder Vermeidung
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut und Ihren Bereich
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit den Referenten
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit anderen Praktiker*innen

Seminarziel

Die Bedrohungslage durch Cyber-Risiken nimmt weiter zu. Supply-Chain-Attacken, KI-basiertes Phishing und hybrides Arbeiten werden zunehmend zur Bedrohung für Banken, Versicherungen und Unternehmen. Cybercrime-as-a-Service wird dabei zum gängigen Geschäftsmodell und die Angriffstaktiken von Hackern und Angreifern werden kontinuierlich weiterentwickelt und »verbessert«.

Täglich werden mehrere Millionen Cyber-Angriffe registriert – alleine in Deutschland! Der Umgang mit Schwachstellen und Sicherheitslücken ist und bleibt daher eine der größten Herausforderungen der Informationssicherheit und des Cyber-Security-Managements. Die »Schnittstelle« zwischen Mensch und Cyberraum bleibt Einfallstor Nummer 1 – mehr als 85% aller Angriffe haben beim Faktor Mensch ihren Ursprung, da Mitarbeitende sich über emotionale Manipulation und Social Engineering in der Regel immer mit der gleichen Methode angreifen lassen.

Die erfahrenen Referenten beschäftigen sich mit der Frage, welche Vorgehensweisen und Maßnahmen bei der Prävention, Erkennung, Aufdeckung, Behebung oder sogar Vermeidung und Versicherbarkeit von Cyberrisiken sinnvoll und wirksam sein können und geben wertvolle und direkt anwendbare Umsetzungs- und Praxistipps.

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- Cyber-Security, Cyber-Response und IT-Forensik
- Informationssicherheit (ISB) und Datenschutz
- IT und Organisation, IT-Compliance und IT-Governance
- Interne Revision und IT-Revision, IT-Notfallmanagement (BCM/ITSCM)

sowie andere interessierte Fach- bzw. Grundsatzbereiche, Vorstandsmitglieder/Geschäftsleitung, externe Prüfer*innen sowie Bankdienstleister.

Unsere Referenten

Jan Spittka
Partner, Rechtsanwalt, Clyde & Co Europe LLP, Düsseldorf

Jan Spittka leitet die deutsche »Data Protection and Privacy«-Praxis bei Clyde & Co Deutschland. Er berät umfassend zu Datenschutz und Cybersecurity und vertritt Unternehmen regelmäßig gegenüber Behörden und vor Gericht.

Helmut Brechtken
Partner, Head of Digital Forensic Incidence Response (DFIR)
Deloitte GmbH Wirtschaftsprüfungsgesellschaft, Köln

Als Head of Digital Forensic Incident Response (DFIR) ist er verantwortlich für Projekte zur forensischen Aufklärung von Cybercrime-Attacken (wie Ransomware, Bankdatenbetrug, Datendiebstahl etc.). Zudem berät er Mandanten zur Cyber-Security Prävention (wie aktuell NIS-2) und der Vermeidung bzw. Abwehr von Cybercrime-Attacken.

Christian Horn
Senior Managing Consultant, Experte für Penetration Testing & Cyber Security, ProSec GmbH

Christian Horn ist Head of Solution Service bei der ProSec GmbH und verfügt über langjährige Erfahrung in der IT-Sicherheit. Nach über elf Jahren als Soldat auf Zeit bei der Bundeswehr wechselte er 2020 zu ProSec, wo er vom Penetrationstester zur Führungskraft aufstieg. Mit IHK-Zertifikaten als Specialist for Cyber Attack und Technical IT Security Specialist vereint er technisches Know-how und Praxis.

Gordon Shepherd
Managing Consultant, Experte für IT-Management & ITSM, ProSec GmbH

Gordon Shepherd ist als Managing Consultant bei der ProSec GmbH tätig und verfügt über mehr als 25 Jahre Erfahrung im IT-Management und in der Cyber Security. Zuvor war er in verschiedenen Stationen als Verantwortlicher für die operative IT mit Schwerpunkt Cybersecurity & Awareness tätig und leitete dort mehrere Jahre IT-Organisationen.

1 Jahr DORA – Umsetzungsstand, Erfahrungen, Erkenntnisse
19. Januar 2026, Online-Veranstaltung

Überprüfung der DORA-Konformität von (IKT-)Dienstleistern und Cloud Service Providern
21. Januar 2026, Online-Veranstaltung

DORA Spezial: Informationssicherheit & IKT-Risikomanagement
22. Januar 2026, Online-Veranstaltung

MaRisk Spezial: Risikoberichtswesen & Vorstands-Reporting
27. Januar 2026, Online-Veranstaltung

Praxis-Umsetzung aktueller DORA- und Aufsichts-Anforderungen in der DL-Steuerung
27. Januar 2026, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM
28. Januar 2026, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
4./5. Februar 2026, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.

Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

Anmeldeformular

Cyberrisiken – Aktuelle Sicherheitslücken und wirksame (Gegen-)Maßnahmen

Name

Vorname

Position

Firma

Straße / Nr.

PLZ / Ort

Telefon

E-Mail

Name der Assistenz

Datum / Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

Termin und Seminarzeiten

Donnerstag, 22. Januar 2026
13:00–16:30 Uhr
Online-Zugang ab 12:45 Uhr

Seminar-Nr. 26 01 BA084 W

Teilnahmegebühr

Die Teilnahme ist kostenfrei.
Die Anmeldung berechtigt zur Teilnahme am Online-Seminar sowie zum Erhalt der Präsentation als PDF-Datei.

Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: www.akademie-heidelberg.de/agb

Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

11.25 / 2601 BA084