20. Januar 2027 · 13:00–17:00 Uhr
KOSTENFREIE 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**
- **Unterschätzte Angriffsvektoren und Haftung bei Cyber-Angriffen**
- **Proportionale Red Teaming-Möglichkeiten für LSIs in der Praxis**
- **Vorbereitung, Durchführung, Nachbereitung von PenTestings**
- **Maßnahmen zum Erkennen und Schließen von Schwachstellen**

Referenten



Jan Spittka
Partner, Rechtsanwalt
Clyde & Co Europe LLP
Düsseldorf



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



Roman Müller
Teamleiter Red Teaming
Onconsult Deutschland AG
München

Cyberrisiken – Aktuelle Sicherheitslücken und wirksame (Gegen-)Maßnahmen

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
- Cybercrime 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

Roman Müller, Oneconsult · **15:30–17:00 Uhr**
Proportionale Pentesting-Möglichkeiten für LSIs in der Praxis – Vorbereitung, Durchführung, Nachbereitung und Maßnahmen zum Erkennen und Schließen von Schwachstellen

- DieTeilnehmenden werden anhand eines beispielhaften LSI durch den Prozess eines typischen Red Teamings. Vom ersten Gedanken, ob und wann Red Teaming sinnvoll ist, über die konkrete Durchführung bis hin zum strukturierten Umgang mit den Ergebnissen. Jeder Abschnitt wird mit Anekdoten aus realen Engagements, Erfahrungen und insbesondere lehrreichen Fehltritten angereichert

Im Einzelnen werden u. a. die folgenden Themen behandelt:

- Abgrenzung zwischen Penetration Testing und Red Teaming: Wann ist eine Organisation tatsächlich bereit für den nächsten Schritt, und wann ist ein klassischer Penetrationstest die bessere Wahl?
- Scoping und Zieldefinition: Identifikation der kritischen Funktionen, Ableitung relevanter Flags und Festlegung eines realistischen Testumfangs
- Threat-Intelligence: Vorbereitung, Steuerung und Einordnung der Ergebnisse. Was macht einen guten Threat-Intelligence-Bericht aus, und wie fließen die Erkenntnisse in die Testplanung ein?
- Red-Teaming: Definition von Szenarien, Festlegung von Flags und Spielregeln für die operative Durchführung.
- Vorstellung eines beispielhaften Angriffsplans: Der Dozent stellt einen konkreten Angriffsplan vor
- Umgang mit Feststellungen: Priorisierung, Maßnahmenplanung und Nachverfolgung
- Typische Findings bei LSIs: Praxisbeispiele zu den häufigsten Schwachstellen, wiederkehrenden Problemen bei Red-Team-Engagements mit kleineren Instituten und die aus Sicht des Dozenten wirksamsten Gegenmaßnahmen
- Praxis-Hinweise und Umsetzungs-Tipps

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)
- andere interessierte Fach- bzw. Grundsatzbereiche, Vorstandsmitglieder/ Geschäftsleitung, externe Prüfer*innen und 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.



Roman Müller
Teamleiter Red Teaming, Oneconsult Deutschland AG, München

Roman Müller ist Red Teamer und Teamleiter mit langjähriger Erfahrung in der Durchführung von Penetrationstests und Red-Team-Engagements. Sein fachlicher Schwerpunkt liegt auf Red Teaming-Projekten für Kunden aus der Finanz- und Versicherungsbranche. Er war bisher an der Durchführung von vier TIBER-EU-Projekten sowie mehreren Red-Team-Assessments bei LSI-Instituten zentral beteiligt und kennt die besonderen Herausforderungen, denen sich auch kleine und mittlere Institute in der Praxis stellen müssen.

Fachtagung DORA & DORA-Umsetzung
3./4. November 2026, Online-Veranstaltung

Kostenfrei: Durchführung interner Red Teamings
1. Dezember 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer
7. bis 9. Dezember 2026, Online-Veranstaltung

IKT Spezial: Identity- & Access-Management (IAM)
15. Dezember 2026, Online-Veranstaltung

DORA Spezial: Informationssicherheit & IKT-Risikomanagement
21. Januar 2027, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-) Notfallmanagement & BCM
28. Januar 2027, Online-Veranstaltung

DORA-konformes IKT-Risikomanagement
3./4. Februar 2027, Online-Veranstaltung

Verschärfte DORA-Anforderungen an die Prozesse zur Steuerung & Überwachung von IKT-Risiken
22. Februar 2027, 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

Mittwoch, 20. Januar 2027
13:00–17:00 Uhr
Online-Zugang ab 12:45 Uhr

Seminar-Nr. 27 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

10.26 / 27 01 BA084