

Cyber Risiken – Aktuelle Sicherheitslücken und wirksame (Gegen-)Maßnahmen



Praxis-Seminar · 4 CPE-Punkte

- **Cybercrime und Cyber-Angriffe: aktuelle Sicherheitslücken, Gefahren und wirksame (Gegen-)Maßnahmen**
- **Krisenmanagement/Schadensminimierung/Forensische Aufklärung**
- **Schnelligkeit als entscheidender Erfolgsfaktor bei (IKT-)Sicherheitsvorfällen**
- **Haftungsfragen bei Cyber-Angriffen – Wer haftet?**
- **Smart Devices und mobile Endgeräte als unterschätzter Angriffsvektor von Cyber-Angriffen**

20 Jahre
AKADEMIE
HEIDELBERG.

Referenten



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



Helmut Brechtken
Partner, Head of Digital Forensic Incident
Response (DFIR), Deloitte GmbH
Wirtschaftsprüfungs-gesellschaft, Köln



Elmar Jilka
CEO, Experte für Cyber Risk &
Cyber Security, GENOA
International GmbH, Linz

Programm

Jan Spittka, Clyde & Co · 14:00–15:00 Uhr

Aktuelle Bedrohungslage durch Cyberangriffe und Ransomware

- Aktuelle Lage der IT-Sicherheit und Cyber-Sicherheit in Deutschland sowie im deutschen Finanzwesen
- Identifikation kritischer Geschäftsprozesse
- Wirksames Schwachstellen-Management
- Typischer Ablauf eines Datenschutzvorfalls
- Haftung für Datenschutzverstöße

Helmut Brechtken, Deloitte GmbH · 15:10–16:00 Uhr

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

- Deutliche Zunahme der Cyber-Angriffe 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

Elmar Jilka, GENOA net works · 16:10–17:00 Uhr

Smart Devices und mobile Endgeräte als unterschätzter Angriffsvektor von Cyber-Angriffen – Live-Daten, Wirksamkeit und Ad-hoc-Information

- Welche Bedrohungen begleiten die Digitalisierung für mobiles Arbeiten?
- Herausforderungen von Cyber-Risiken im Risikomanagement
- Geltende Mindeststandards (z. B. BSI, GDPR)
- Was versteht man unter Cyber-Risiko für mobile Endgeräte?
- Systematische Ansprüche zur Identifikation, Analyse und Priorisierung von Cyberrisiken
- Ableitung konkreter Maßnahmen für die ICT-Security von Smart Devices
- Welche Zahlenbasis dient zur Kommunikation zwischen CIO, Head of IT, CISO und IT?
- Welche Live-Daten verändern Cyber-Risiken?

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 Unternehmen und Ihren Bereich
- Sie klären offene Fragen für Ihren Bereich mit den erfahrenen Praxis-Referenten
- Sie erhalten wertvolle Praxis- und Prüfungstipps 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 Nutzung mobiler Endgeräte und Smart Devices als »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 Cyber-Risiken sinnvoll und wirksam sein können und geben wertvolle und direkt anwendbare Umsetzungs- und Praxistipps.

Wissenswertes

Aus der Praxis für die Praxis!

Wir wenden uns insbesondere an die Mitarbeitenden folgender Bereiche:

- Cyber-Security, Cyber-Response und IT-Forensik
- Informationssicherheit (ISB) und Datenschutz
- IT und Organisation
- Interne Revision und IT-Revision
- IT-Compliance und IT-Governance
- IT-Notfallmanagement (BCM/ITSCM)
- sowie andere interessierte Fachbereiche bzw. Grundsatzbereiche, Vorstandsmitglieder und Geschäftsleitung, externe Prüferinnen und Prüfer 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, Forensic Technology
Head of Digital Forensic Incident 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 und der Vermeidung bzw. Abwehr von Cybercrime-Attacken.



Elmar Jilka

CEO, Mitglied des Cyber Security Boards
GENOA net works IT-Beratungs GmbH, Linz

Elmar Jilka ist spezialisiert auf den vollautomatischen Rundum-Service für Cyber Security zum Schutz der Unternehmens-Assets mit Hilfe von hoch digitalisierten Prozessen, einem präventiven IT-Security-Konzept und technologischen Vorteilen aus künstlicher Intelligenz (AI) und Machine Learning (ML). So bietet er seinen Kunden einen modernen und wirksamen Schutz gegen bekannte und zukünftige Bedrohungen.

Seminar-Vorschläge

Überprüfung der DORA Konformität von (IKT-)Dienstleistern und Cloud Service Providern

21. Januar 2025, Online-Veranstaltung

Modulreihe zur sicheren Nutzung von KI & ChatGPT

Ab 22. Januar 2025, Online-Veranstaltung

DORA Spezial:

Informationssicherheit & IKT-Risikomanagement

23. Januar 2025, Online-Veranstaltung

Neue DORA- und Aufsichts-Anforderungen an (IKT-)Notfallmanagement & BCM

29. Januar 2025, Online-Veranstaltung

Nutzung von Robotic (RPA) und Echtzeitreporting zur Prozessoptimierung in Banken

13. Februar 2025, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)

17. Februar 2025, Online-Veranstaltung

Mobile-Work-Risiken im Fokus von DORA, IKT-Risikomanagement & IT-Revision

18. Februar 2025, 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

Cyber-Risiken – aktuelle Sicherheitslücken und direkt wirksame (Gegen-)Maßnahmen

Name _____

Vorname _____

Position _____

Firma _____

Straße _____

PLZ / Ort _____

Tel./Fax _____

E-Mail _____

Name der Assistenz _____

Datum Unterschrift _____

An anmeldung@akademie-heidelberg.de oder per Fax an: **06221/65033-29**

Termin + Seminarzeiten

Mittwoch, 22. Januar 2025
14:00 – 17:00 Uhr
Online-Zugang ab 13:45 Uhr
Seminar-Nr. 25 01 BA084 W

Ohne Teilnahmegebühr!

€ 0,-

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, wenn gewünscht, 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 Internet-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.



AH AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0 · Fax 06221/65033-69
info@akademie-heidelberg.de
www.akademie-heidelberg.de