



# Cyber-Vorstand – Exklusivseminar für das C-Level

Vorsorge, Notfallmanagement  
und Haftung in der IT-Sicherheit

# Cyber-Vorstand – Exklusivseminar für das C-Level

## Vorsorge, Notfallmanagement und Haftung in der IT-Sicherheit

### Kurzbeschreibung

Cyber-Attacks häufen sich. Alle Unternehmen sind potentiell bedroht. Dies erkennt auch der Gesetzgeber und verschärft die Anforderungen an die Informationssicherheit und zugleich die persönliche Verantwortung des Managements, unter anderem in der NIS 2-Richtlinie. Kurzum: Cyber-Security wird zur Chefsache, eine Delegation in wichtigen Einrichtungen unzulässig und die persönliche Haftung für Unternehmensschäden festgeschrieben.

Das Management-Seminar versetzt Sie auf Leitungsebene in die Lage, eine angemessene **Cyber-Sicherheit in Ihrem Unternehmen korrekt zu steuern und zu überwachen** und persönliche Haftungsansprüche zu vermeiden. Dazu wird im geschützten Rahmen das Know-how vermittelt, das für die Implementierung eines wirksamen Cyber-Security-Riskmanagements erforderlich ist. Am Ende der Veranstaltung wird der Ernstfall einer Cyber-Attacke trainiert.



### Inhalt

- Haftungsrisiken für die Unternehmensleitung
- Ressourcen: Verantwortung und Riskmanagement
- Trainieren: Anforderungen an die Cyber-Security
- Awareness: Sensibilität, Motivation und Haftungsrisiken
- Notfallplan: Prozesse und Kommunikation

### Was lernen Sie in diesem Exklusivseminar?

Die Teilnehmenden werden fit gemacht, die Cyber-Security in ihrem Unternehmen wirksam zu etablieren und zu steuern. So können Verantwortliche Cyber-Attacks vorbeugen und im Ernstfall richtig reagieren. Damit ist der Wissensgrundstein gelegt, um Cyber-Vorfälle möglichst zu vermeiden und im Ernstfall die Schäden zu reduzieren. Das gilt sowohl für kommerzielle Schadensersatzansprüche, etwa wegen Datenpannen oder Lieferverzögerungen, als auch für Produktionsausfälle, genauso wie im Kontext der Reputation und persönlichen Haftung der Leitungsebene.

# Cyber-Vorstand – Exklusivseminar für das C-Level

## Vorsorge, Notfallmanagement und Haftung in der IT-Sicherheit

### Zielgruppe

Das Exklusivseminar richtet sich an das Management von Unternehmen, Geschäftsleiterinnen und –leiter sowie Vorstände und Aufsichtsgremien als auch Leitungspersonen von Kernbereichen im Unternehmen. Das Seminar verfolgt einen ganzheitlichen Ansatz der Wissensvermittlung und erfordert weder juristische noch IT-Vorkenntnisse. Das Seminar eignet sich nicht für Fachkräfte aus der IT-Sicherheit (CISOs, IT-Sicherheitsbeauftragte o. Ä.).

Zielgruppe des Management-Seminar ist explizit die Unternehmensführung, da der Gesetzgeber die persönliche Haftung für die Leitungsebene im Umsetzungsgesetz zur NIS 2-Richtlinie fest schreibt. Die Verantwortung für diese Kontrollfunktion darf nach dem Gesetzesvorschlag nicht delegiert werden.

Das Seminar eignet sich auch für Geschäftsführende aus dem **Finanzsektor**, für die die persönliche Haftung auch durch die DORA-Verordnung vorgeschrieben ist.

### Didaktischer Aufbau

Im engsten Teilnehmerkreis erhalten die Teilnehmende einen Überblick über die Anforderungen an eine angemessene Cyber-Security. Die Referenten arbeiten mit Beispielen, kombiniert mit Checklisten und der Simulation von konkreten Vorfällen. Die Umsetzung wird praktisch angewandt und geübt.



### Zusatzinformationen

- Die Durchführung des Workshops kann erst ab einer **Mindestteilnehmerzahl von fünf** garantiert werden. Die **Maximalteilnehmerzahl beträgt 15**.
- Der 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) finden Sie [hier](#) einen zusätzlichen Vergleich zu den jeweiligen Eigenschaften.
- 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 auch Anträge auf Anerkennung unserer Veranstaltungen in anderen Bundesländern.
- 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.

# Seminarprogramm

## Cyber-Vorstand – Exklusivseminar für das C-Level

### Agenda

#### Ressourcen

- **Risikomanagement:** Richtlinien als Compliance-Anforderung und Informations-Management-Systeme (ISMS) im Unternehmen umsetzen
- **Zuständigkeiten:** Verteilung der Verantwortlichkeiten, Ressourcen bereitstellen und (auch künftig noch) zulässiger Delegationsumfang
- **Sicherheitslevel:** Relevanz der Sicherheitslevel und wie sie bestimmt werden

Sie lernen, welche Ressourcen im Unternehmen für die IT-Sicherheit rechtlich notwendig sind, um Haftungsrisiken zu vermeiden, und wie Sie diese dokumentiert schaffen und erhalten.

#### Trainieren

- **Know-how der rechtlichen Anforderungen an die Sicherheit mit Trainingsfällen:** Konziser Überblick über die rechtlichen Anforderungen der Datenschutzgrundverordnung über BSI- und NIS-2-Umsetzungsgesetz bis hin zu Sondervorgaben, etwa im Energierecht
  - **Besonderheit für den Finanzsektor:** DORA-Verordnung
- **Checklisten mit BSI IT-Grundschutz und ISO27001:** Handreichung für das C-Level, welche Checklisten und Tools bei der Kontrolle vorgeschlagener Maßnahmen, ihrer Billigung und der Überprüfung fortlaufender Einhaltung helfen
- **Dokumentation und Meldepflichten:** Entwicklung der Anforderungen an eine rechtlich sichere Dokumentation der Maßnahmen und Vorgänge sowie Überblick über die Meldepflichten, um im Ernstfall vorbereitet zu sein

Sie lernen die rechtlichen Anforderungen an die IT-Sicherheit praxisnah kennen und wie Sie diese in Ihrem Unternehmen implementieren (lassen), billigen und fortlaufend überprüfen und dokumentieren.

# Seminarprogramm

## Cyber-Vorstand – Exklusivseminar für das C-Level

### Agenda

#### Awareness

- **Auswirkungen auf den Unternehmensbetrieb:** Überblick über die regelmäßigen Auswirkungen auf den Unternehmensbetrieb und ihre rechtliche Relevanz sowie Steuerungsoptionen: von Lieferverzögerungen über den Datenschutz bis hin zu Erpressungsforderungen
- **Rechtliche Risiken bei unzureichender Sicherheit - Haftungsrisiken für das Unternehmen und das Management:** Wann sind Cyber-Vorfälle „höhere Gewalt“ und unverschuldet, wann muss ein Unternehmen für Verzögerungen haften, wann drohen Vertragsstrafen und Schadensersatzansprüche von Betroffenen und wie kann ein Unternehmen diese Risiken minimieren? Zudem: Schäden des Unternehmens können zu Schäden des Managements werden, insbesondere nach Umsetzung der NIS-2-Richtlinie. Wie können diese persönlichen Haftungsrisiken minimiert werden?
- **Mitarbeitende schulen mit Trainingsfällen:** Welche Mitarbeiterschulungen sind unabdingbar, um die Awareness zur Risikoreduktion im gesamten Unternehmen zu verankern?

Sie lernen, welche (rechtlichen) Risiken ein Cyber-Vorfall mit sich bringt und wie Sie diese über eine optimierte Steuerung auf dem C-Level minimieren können.

#### Notfallplan

- **Detecting:** Anforderungen und rechtlich zulässige Möglichkeiten an eine fortlaufende Überwachung der Datenflüsse, um Hackerzugriffe frühestmöglich zu vermeiden
- **Reaktion planen und richtig durchführen mit Trainingsfällen:** Wie Sie einen an Ihr Unternehmen angepassten Notfallplan erstellen und erfolgreich implementieren
- **Folgen erfolgreicher Angriffe: vom Umgang mit Erpressungsforderungen bis zum Handling von Schadensersatz- und Regressansprüchen mit Praxisbeispielen:** wie Sie nach einer Cyber-Attacke systematisch und schnell vorgehen, um Schäden zu minimieren: von der forensischen Aufklärung über die Formulierung von Behördenmeldungen über Betroffeneninformationen bis hin zum Umgang mit Erpressungsforderungen und dem Handling von Folgeansprüchen von Geschäftspartnern und Betroffenen

Richtig handeln im Ernstfall: Sie lernen, welche Anforderungen schon vorab verfestigt sein sollen und wie Sie diese umsetzen.

# Ihre Referenten



## Dr. Eren Basar

**Partner, Fachanwalt für Strafrecht, CIPP/E  
Wessing & Partner, Düsseldorf**

Eren Basar ist Fachanwalt für Strafrecht. Er berät im Wirtschaftsstrafrecht, übernimmt Individualverteidigungen von Unternehmen und Führungskräften und verteidigt in Hauptverhandlungen. Unternehmen in Straf- und Ordnungswidrigkeitenverfahren sind seine Mandanten. Ihnen hilft er auch, präventive Aufstellungen solcher Verfahren zu gestalten. Eren Basar ist Spezialist im IT- und Datenschutzstrafrecht. Sein Steckenpferd ist die digitale Beweisgewinnung. Er ist zertifizierter Compliance Officer (TÜV), Certified Information Privacy Professional Europe (CIPP/E) sowie IT-Sicherheitsbeauftragter nach ISO 27001/BSI Grundschutz (Bitkom).



## Dr. Kristina Schreiber

**Partnerin, Fachwältin für Verwaltungsrecht, CIPP/E  
Loschelder Rechtsanwälte, Köln**

Kristina Schreiber berät und vertritt Unternehmen im IT- und Datenrecht. Sie ist spezialisiert auf die Begleitung von Digitalisierungsprozessen, u.a. auch der Etablierung rechtskonformer Cyber-Security-Prozesse, und berät und vertritt Unternehmen nach Cyber-Attacken auch gegenüber den zuständigen Aufsichtsbehörden und in Gerichtsverfahren. Zu ihren Mandanten zählen sowohl mittelständische Unternehmen als auch große Konzerne, u. a. aus dem eHealth-Segment und den regulierten Industrien. Kristina Schreiber bloggt unter [www.digitalisierungsrecht.eu](http://www.digitalisierungsrecht.eu), publiziert regelmäßig in Fachzeitschriften und hält Vorträge.

# Shortfacts



## Termine, Veranstaltungsorte & 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](mailto:info@bitkom-akademie.de)  
Weitere Seminare finden Sie unter [www.bitkom-akademie.de](http://www.bitkom-akademie.de)

**bitkom**  
akademie