



# Incident Response Management

Effektive Reaktion auf  
Cybersicherheitsvorfälle

# Incident Response Management

## Effektive Reaktion auf Cybersicherheitsvorfälle

### Kurzbeschreibung

IT-Sicherheitsprofis wissen: Die Frage, ist nicht ob ein Cyberangriff passiert, sondern wann. Laut einer Studie des Bitkom aus 2023 sind 84 Prozent der Unternehmen im vergangenen Jahr Opfer von Datendiebstahl, Spionage oder Sabotage geworden, weitere 9 Prozent gehen davon aus. Ist der Ernstfall eingetreten, kommt es darauf an, wie IT-Sicherheitsexpertinnen und -experten auf den Vorfall reagieren. Eine **zielgerichtete, schnelle und durchdachte Reaktion** ist von entscheidender Bedeutung, um die Schäden so gering wie möglich zu halten.

Der zweitägige Workshop „Incident Response Management“ schult Sie intensiv in der **proaktiven Bewältigung von Sicherheitsvorfällen**, dem Vorfallreaktionsmanagement. Sie werden mit bewährten Methoden und Strategien vertraut gemacht, um effektiv auf Sicherheitsbedrohungen zu reagieren. Das Ziel ist es, Ausfallzeiten zu minimieren und den Geschäftsbetrieb so schnell wie möglich wieder aufnehmen zu können. Dafür lernen Sie in diesem Workshop die entsprechenden praktischen Ansätze kennen.



### Inhalte

- Grundlagen des Incident Management
- Erkennung und Analyse von Vorfällen
- Einschätzung der Bedrohungsstufe
- Effektive Reaktionsstrategien: Entwicklung von Reaktionsplänen & Maßnahmen zur schnellen Eindämmung von Sicherheitsvorfällen
- Post-Incident-Analyse
- Kontinuierliche Verbesserungsstrategien
- Aufbau eines Incident Response Teams

### Was lernen Sie in diesem Seminar?

Im Workshop lernen Sie, wie Sie eine wirksame Verteidigungslinie gegenüber Sicherheitsvorfällen aufbauen. Nach dem Workshop haben Sie ein grundlegendes Verständnis zu den Incident-Management-Phasen und zum Ablauf entwickelt. Sie sind im Anschluss in der Lage, Strategien zur Verbesserung des Incident Managements in der eigenen Organisation zu implementieren. Dazu gehört auch die eigenständige Entwicklung von Reaktionsplänen und Wiederherstellungsmaßnahmen sowie deren Bewertung und kontinuierliche Anpassung.

# Incident Response Management

## Effektive Reaktion auf Cybersicherheitsvorfälle

### Zielgruppe

Der Workshop eignet sich für alle Fach- und Führungskräfte, die mit der Überwachung und Reaktion auf Cybervorfälle beauftragt sind. Dazu zählen u. a. Mitarbeitende in der IT-Sicherheit, IT-Sicherheitsbeauftragte, Leitungsfunktionen im IT-Bereich, IT-Administratoren, Mitarbeitende in IT-Operations sowie Incident Manager und Prozessverantwortliche. Grundkenntnisse in der IT-Sicherheit werden vorausgesetzt.

### Didaktischer Aufbau

Der Workshop vermittelt Techniken und Methoden zur zielgerichteten Reaktion auf Sicherheitsvorfälle und deren Auswirkungen. Es werden erste praktische Ansätze zur Implementierung von Frühwarnsystemen erlernt und Methoden zur Identifizierung von Angriffen veranschaulicht. Das Seminar findet in einer kleinen Gruppe statt, damit auf individuelle Fragen eingegangen werden kann.



### Zusatzinformationen

- Das Seminar hat eine begrenzte **Teilnehmerzahl von 16 Personen**. Die Mindestteilnehmerzahl beträgt 5.
- 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 Anträge auf Anerkennung unserer Seminar-Veranstaltungen auch in anderen Bundesländern.
- Dieser 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) bietet Ihnen [diese Tabelle](#) einen zusätzlichen Vergleich zu den jeweiligen Eigenschaften.
- 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

## Incident Response Management

### Grundlagen des Information Security Incident Managements

- Definition und Kategorisierung von Sicherheitsvorfällen
- Bedeutung eines proaktiven Incident Management Ansatzes

### Erkennung und Analyse von Vorfällen

- Implementierung von Frühwarnsystemen
- Forensische Methoden zur Identifizierung von Angriffen

### Klassifizierung und Priorisierung

- Taxonomie von Sicherheitsvorfällen
- Schnelle Einschätzung der Bedrohungsstufe

### Aufbau eines Incident Response Teams

- Rollen und Verantwortlichkeiten
- Teamzusammensetzung und -training

### Effektive Reaktionsstrategien

- Entwicklung von Reaktionsplänen
- Koordination von Maßnahmen während eines Vorfalls

### Eindämmung und Wiederherstellung

- Strategien zur schnellen Eindämmung von Sicherheitsvorfällen
- Wiederherstellungsmaßnahmen und Business Continuity

### Post-Incident-Analyse und Berichterstattung

- Bewertung der Incident-Response-Effektivität
- Erstellung von Berichten für Stakeholder und Behörden

### Kontinuierliche Verbesserung

- Identifikation von Lektionen aus vergangenen Vorfällen
- Anpassung von Richtlinien und Verfahren zur ständigen Verbesserung

Tag  
1

Tag  
2

# Ihr Referent

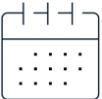


## Thorsten Rödel

**Berater für Informationssicherheit  
Bredex GmbH**

Thorsten Rödel ist Experte für Informationssicherheit und zuständig für Beratung und Implementierung - Informationssicherheit gem. ISO / IEC 27001 sowie BSI IT-Grundschutz. Er ist Dozent und Trainer für ISO 27001 und BSI Grundschutz Kompendium (Praktiker und Experte) sowie BSI Sicherheitskonzepte Erstellung auf 100-x Standard und 200-x Standard / Migration Risikomanagement gem. ISO / IEC 31000.

## Shortfact



### **Termine, Veranstaltungsort und 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)

