IT-Forensik Readiness

Theorie und Praxis zur gerichtsfesten Datensichtung im eigenen Unternehmen

bitkom akademie

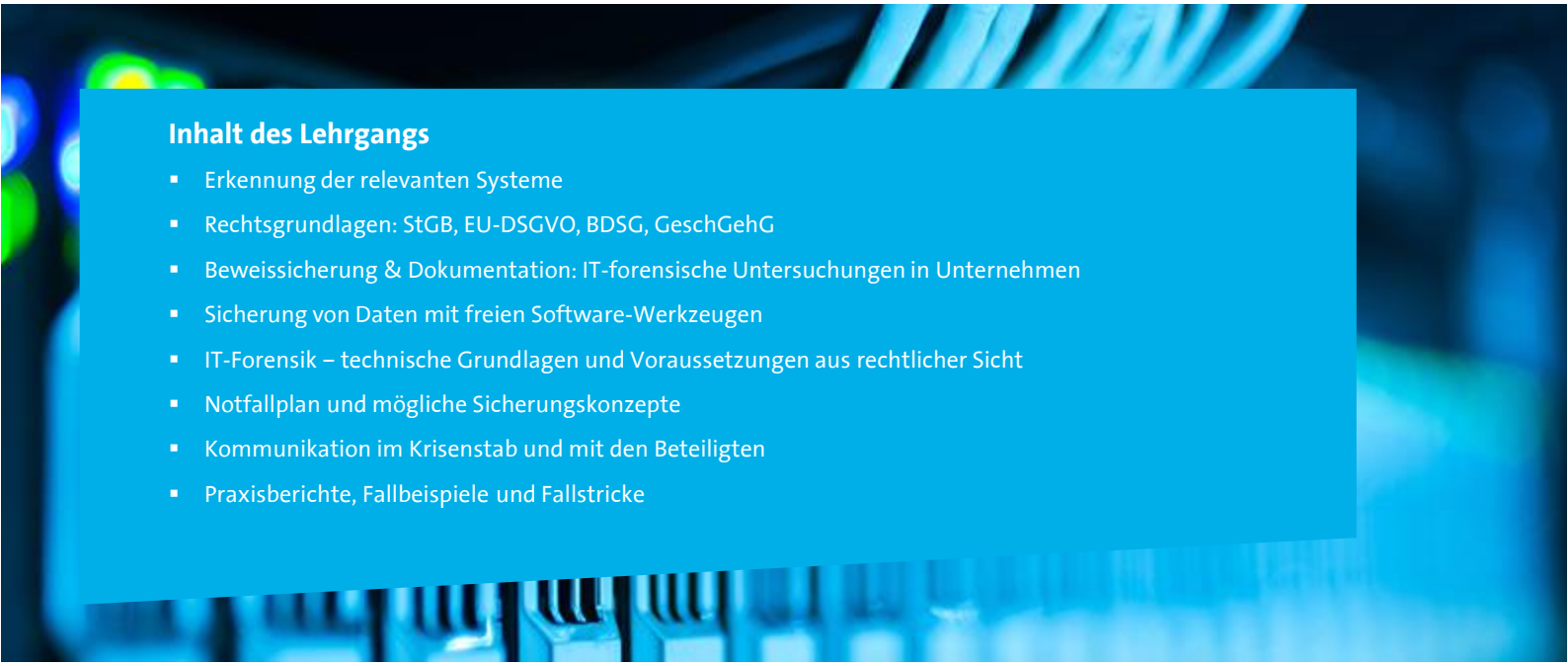
IT-Forensik Readiness

Theorie und Praxis zur gerichtsfesten Datensicherung im eigenen Unternehmen

Erweiterte fachliche Kompetenzen für IT-Sicherheitsverantwortliche

Die Gefährdungslage für Unternehmen und Institutionen verschlechtert sich fortlaufend. Umso wichtiger ist es, für den Ernstfall gut aufgestellt zu sein. Abseits von verlässlichen Schutzkonzepten sollten die Verantwortlichen auch Vorkehrungen zur Beweissicherung im Angriffsfall treffen. Mit den richtigen technischen und organisatorischen Vorbereitungen können Sie in diesem Fall schnell und zielgerichtet reagieren. Schließlich gilt es, eine professionelle Aufarbeitung zu gewährleisten, um größere Schäden zu vermeiden.

Im Online-Workshop lernen Sie, welche Vorkehrungen nötig sind, um die IT-forensische Ersthilfe optimal durchführen zu können. Gemeinsam erarbeiten Sie sich das nötige Fachwissen für den Aufbau IT-forensischer Notfallpläne und Konzepte. Darüber hinaus lernen Sie die Rechtsgrundlagen und mögliche Meldepflichten – etwa mit Blick auf die Datenschutzgrundverordnung – kennen. Nach zwei Workshop-Tagen sind Sie in der Lage, interne Erstmaßnahmen aus technischer Sicht einzuleiten sowie diese auch fachkundig und gerichtsfest durchzuführen.



Inhalt des Lehrgangs

- Erkennung der relevanten Systeme
- Rechtsgrundlagen: StGB, EU-DSGVO, BDSG, GeschGehG
- Beweissicherung & Dokumentation: IT-forensische Untersuchungen in Unternehmen
- Sicherung von Daten mit freien Software-Werkzeugen
- IT-Forensik – technische Grundlagen und Voraussetzungen aus rechtlicher Sicht
- Notfallplan und mögliche Sicherungskonzepte
- Kommunikation im Krisenstab und mit den Beteiligten
- Praxisberichte, Fallbeispiele und Fallstricke

Was Lernen Sie in diesem Workshop?

An zwei Tagen lernen Sie die technischen Grundlagen zur IT-forensischen Datensicherung sowie die aktuellen Rechtsgrundlagen kennen. Es werden Maßnahmen und Systeme vorgestellt, mit denen flüchtige Daten – etwa aus Arbeitsspeichern oder Netzwerken – gerichtsfest gesichert werden können. Anhand von Praxisbeispielen erfahren Sie, wie Sie den Einsatz von forensischen Experten optimal und gerichtswertbar vorbereiten. Anschließend sind Sie in der Lage, die technischen und organisatorischen Maßnahmen einzuleiten, um eine IT-Forensik Readiness in Ihrem Unternehmen zu erreichen.

bitkom akademie

IT-Forensik Readiness

Theorie und Praxis zur gerichtsfesten Datensicherung im eigenen Unternehmen

Zielgruppe

Die Schulung richtet sich an Verantwortliche im Informationssicherheitsbereich, IT-Sicherheitsbeauftragte, IT-Risk Manager, BSI IT-Grundschutzexperten sowie generell an Fach- und Führungskräfte im Unternehmen, die im Rahmen von internen Sicherheitsvorfällen in die Ermittlungen eingebunden werden.

Welche Vorkenntnisse sollten Teilnehmende mitbringen?

Die Teilnehmenden sollten über Grundkenntnisse im Bereich Netzwerktechnik sowie über erweiterte Kenntnisse in der Hardwarestruktur und Virtualisierung von IT-Systemen verfügen. Darüber hinaus wird ein gutes Verständnis über den Aufbau von Dateisystemen und Speichermedien empfohlen.

Was ist an Technik mitzubringen?

Die Teilnehmenden sollten über lokale Admin-Rechte sowie zugängliche USB-Anschlüsse verfügen. Der Einsatz eines Windows-Geräts wird empfohlen, da die praktischen Demonstrationen in diesem Betriebssystem vorgeführt werden.

Didaktischer Aufbau des Workshops

Im Online-Workshop lernen Sie die Grundlagen der IT-Forensik auf der Basis international anerkannter Standards kennen. Der Workshop-Programm verbindet die Vermittlung aktueller Erkenntnisse und neuester Entwicklungen mit dem theoretischen Fachwissen. Das Erlernte wird durch Fallbeispiele illustriert und durch praktische Übungen gefestigt. Im zweitätigen Workshop werden Sie umfangreiche Seminarunterlagen bearbeiten. Sie sind als praxisorientierter Leitfaden gestaltet und dienen Ihnen auch später im Bedarfsfall als Vorlage für einen „roten Faden“ zur ersten Datensicherung. Unterstützt wird dies durch zahlreiche Vorlagen und Checklisten.

Zusatzinformationen

- Der Online-Workshop findet in einer kleinen Gruppe statt. Unser Referenten können dadurch auf individuelle Fragestellungen besser eingehen. Pausen werden zeitlich flexibel gehalten, damit alle fokussiert bleiben können.
- Die Durchführung des Online-Workshops kann erst ab einer Mindestteilnehmerzahl von fünf Personen garantiert werden.
- Die Bitkom Akademie ist anerkannter Bildungsträger in Baden-Württemberg und Nordrhein-Westfalen. Teilnehmer 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.

bitkom akademie

Seminarprogramm

IT-Forensik Readiness

TAG 1

Grundlagen der IT-Forensik
- Computerkriminalität und die Erkennung der relevanten Systeme
- Grundlegende Prinzipien der IT-Forensik
- gerichtsfeste Beweissicherung
- Kommunikation mit Forensikern und Beteiligten

Rechtsgrundlagen I
- Verständnis und Grundbegriffe IT-Forensik Readiness
- Beweiskette und Dokumentationen richtig erstellen

Rechtsgrundlagen II
- EU-DSGVO und besondere Regelungen für den IT-Sicherheitsvorfall
- Erlaubte IT-forensische Maßnahmen im betrieblichen Umfeld

Datenakquirierung I
- Allgemeines zur technischen Datenakquirierung
- technische und organisatorische Einrichtung von Sicherungsprozessen
- Erfahrungsberichte aus der Praxis

Datenakquirierung II
- Grundlagen der Datensicherung im Ernstfall
- Datensicherung an Einzelplatzrechnern
- Datensicherung in Netzwerken
- Fallstricke Erfahrung / Task-Force

TAG 2

Werkzeuge für die forensische Datensicherung
- FTK Imager, DeftZero und weitere freie Software
- Durchsuchungskonzepte und automatisierte Methoden aus der Praxis
- Vorstellung von freier Software für eine IT-forensische Voruntersuchung
- Aufbau einer IT-Forensik Untersuchungsumgebung

Werkzeuge für die forensische Ersthilfe
- Ablauf einer IT-forensischen Sicherstellung und Untersuchung mit freier Software
- Sicherungstools am Beispiel DD, DeftZero, Autopsy von SleuthKit
- Das Datenakquirierungsgerät für die effiziente Datensicherung am Beispiel LogiCube Falcon Neo

Fallbeispiele
- Arbeitszeitbetrug durch Analyse von E-Mail-Systemen aufgedeckt
- Datenabfluss durch Mitarbeiter durch schnelles Handeln aufgedeckt
- CEO Fraud und erforderliche, schnelle Erstreaktionen

Umsetzung der IT-Forensik Readiness in ihrem Unternehmen
- Sicherstellungskonzepte in der Praxis
- Notfallplanung: Alarmkette, Krisenkommunikation, Task-Force
- Dokumentationsverfahren und Dokumentationswerkzeuge

bitkom akademie

Ihr Referent

Volker Wassermann

IT-Forensiker | Computer Forensic Examiner | Expert Witness in Digital Forensics

IT-Forensic-Analyst (DEKRA®)
EDV-Sachverständiger (DEKRA®)
externer Datenschutzbeauftragter (TÜV)
Mehr als 25 Jahre Erfahrung in der IT. Expertisen in der Softwareentwicklung, IT-Software und Hardware, Nachrichtentechnik, Lauschabwehr, Krisenkommunikation

Shortfacts

Termine, Preise und Veranstaltungsorte

Bitte entnehmen Sie aktuelle Informationen hierzu 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
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie