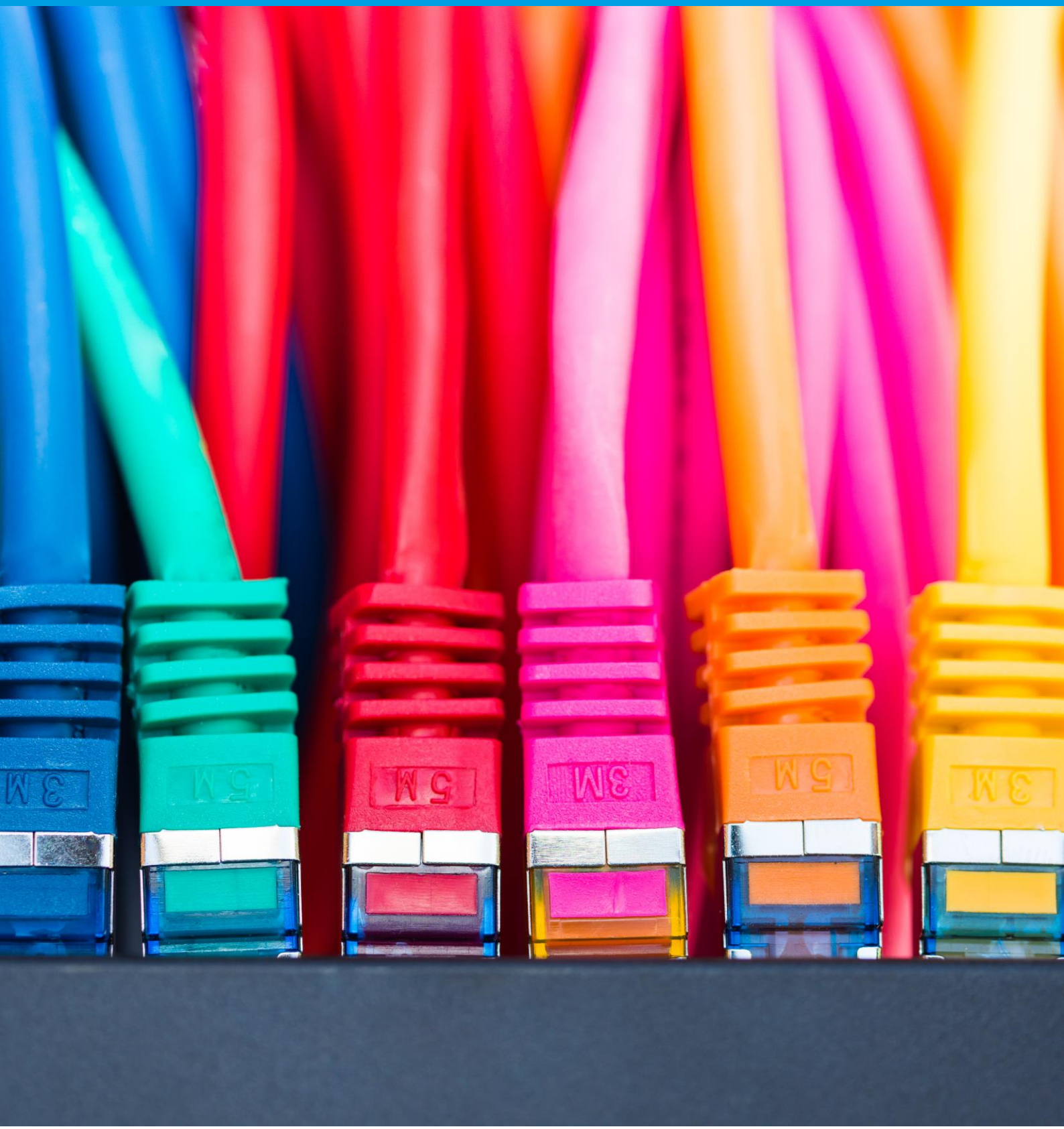

IT-Forensik im betrieblichen Umfeld – Zertifikatslehrgang

Theorie und Praxis zur gerichtsfesten Beweissicherung und ersten Datensichtung nach IT-Sicherheitsvorfällen

bitkom akademie

IT-Forensik im betrieblichen Umfeld – Zertifikatslehrgang

Theorie und Praxis zur gerichtsfesten Beweissicherung und ersten Datensichtung nach IT-Sicherheitsvorfällen

Erweiterte Fachliche Kompetenzen für IT-Sicherheitsverantwortliche

IT-Sicherheitsvorfälle sind branchenübergreifend zum Dauerproblem für Unternehmen geworden. Mit der Datenschutz-Grundverordnung (DSGVO) sind nicht nur neue Meldepflichten an die Aufsichtsbehörden verbunden, sondern darüber hinaus auch umfangreiche Maßnahmen, die erhebliche Kosten verursachen können. Nach IT-Sicherheitsvorfällen ist eine rasche und professionelle Aufarbeitung notwendig, um größeren Schaden zu vermeiden.

In diesem Lehrgang lernen Sie einerseits die aktuelle Rechtsgrundlagen sowie Strategien zur erfolgreichen Ermittlung und gutachterlichen Aufbereitung von IT-Sicherheitsvorällen kennen. Anschließend werden konkrete Maßnahmen vorgestellt, um flüchtige Daten, bspw. aus Arbeitsspeichern (RAM), gerichtsfest zu sichern, noch bevor die (externen) forensischen Spezialisten eintreffen und die weiteren internen Ermittlungen übernehmen. Anhand von realen Cases und praktischen Übungen erhalten Sie die strategischen Grundlagen, um im Sinne der “Forensic Readiness” in Ihrem Unternehmensumfeld zu handeln.

Inhalt des Lehrgangs

- Rechtsgrundlagen: StGB, UrhG, DSGVO
- Beweiskette & Dokumentation, Forensiche Sonderuntersuchungen
- IT-Forensik – technische Grundlagen
- Ermittlungsstrategien
- Sicherung flüchtiger Daten aus Arbeitsspeichern
- Auswertungsmethoden und Berichtswesen
- „Forensic Readiness“ in Unternehmen
- Praktische Übungen und Anwendungsszenarien

An wen richtet sich der Lehrgang?

Die Schulung richtet sich hauptsächlich an alle Verantwortlichen im Informationssicherheitsbereich, IT-Sicherheitsbeauftragte, Datenschutzbeauftragte, IT-Risk Manager, BSI IT-Grundschutzexperten sowie generell an operative Entscheidungsträger im Unternehmen.

bitkom akademie

Welche Vorkenntnisse sollten Teilnehmer mitbringen?

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

Zertifikat

Bei bestandener Prüfung erhalten die Teilnehmer ein Zertifikat.

Didaktischer Aufbau des Lehrgangs

Der Lehrgang ist ein Grundlagenkurs zur Vermittlung von Inhalten gemäß anerkannter internationaler Standards. Aufgrund der Aktualität und Neuigkeit des Themas basiert der Lehrgang mehrheitlich auf Vermittlung von theoretischem Fachwissen unterstützt durch praktische Übungen. Der dreitägige Lehrgang besteht aus theoretischen und praktischen Lehreinheiten (Workshop-Charakter). Die Seminarunterlagen dienen dem Teilnehmer im Bedarfsfall auch als Handbuch um IT-Sicherheitsvorfälle von der ersten Stunde an zu meistern.

Was ist an Technik mitzubringen?

- Teilnehmer sollten vorzugsweise ein Notebook mit Windows Betriebssystem zum Lehrgang mitbringen, da viele Demonstrationen auf dem Windows Betriebssystem basieren. Jedoch besteht hier kein Zwang.
- Bitte achten Sie darauf, dass USB-Anschlüsse nicht gesperrt sind.

Zusatzinformationen

- **Die Prüfung besteht aus einem Multiple Choice Test und findet am dritten Veranstaltungstag statt (45min). Teilnehmer erhalten einen Nachweis zur bestandenen Prüfung.**
- Die Durchführung des Seminars kann erst ab einer Mindestteilnehmerzahl von 5 garantiert werden. Die maximale Teilnehmerzahl beträgt 15.
- 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.
- Lunch und Getränke sind im Seminarpreis enthalten.
- Anmeldeschluss ist 2 Wochen vor Seminarbeginn.
- Tipp: Nutzen Sie für Ihre Anreise zu unseren Akademie-Seminaren die Sonderkonditionen unserer Partner.

bitkom akademie

IT-Forensik im betrieblichen Umfeld

TAG 1

09.30-10.00
Begrüßung durch den Seminarleiter
- Vorstellungsrunde & Erwartungshaltung der Teilnehmer

10.30-11.30
Einführung
- Entwicklung der forensischen Wissenschaften
- Computerkriminalität im engeren und weiteren Sinne
- Digitale Forensik und Untergruppen

11.30-11.45
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

11.45-13.15
Rechtsgrundlagen I
- Grundbegriffe
- Beweiskette und Dokumentation

13.15-14.15
Mittagspause

14.15-15.45
Rechtsgrundlagen II
- StGB / stopp, UrhG (Urheberrechtsgesetz)
- EU-DSGVO und betrieblicher Datenschutz
- Forensische Sonderuntersuchungen im betrieblichen Umfeld (was geht-was nicht!)

15.45-16.00
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

16.00-17.30
Datenakquirierung I
- Allgemeines zur Datenakquirierung
- Grundsätze der Sicherung und Varianten

17.30
Ende des ersten Seminartages

bitkom akademie

IT-Forensik im betrieblichen Umfeld

TAG 2

09.00-09.30
Begrüßung durch den Seminarleiter und Rückblick auf Tag 1

09.30-10.30
Datenakquirierung II
- Datensicherung an Einzelplatzrechnern
- Datensicherung in Netzwerken
- Fallstrick Erfahrung

10.30-11.00
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

11.00-12.30
Werkzeuge für Sicherung und Auswertung I
- FTK Imager
- Durchsuchungskonzept 2.0
- Sicherung von Arbeitsspeicherinhalten

12.30-13.30
Mittagspause

13.30-15.00
Werkzeuge für Sicherung und Auswertung II
- RAM-Auswertungstools

15.00-15.30
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

15.30-17.00
Fallbeispiele
- Arbeitszeitbetrug
- Datenabfluss durch Mitarbeiter
- CEO Fraud und andere Varianten
- Kassenmanipulation (Umsatzverkürzung)

17.00
Ende des zweiten Seminartages

bitkom akademie

IT-Forensik im betrieblichen Umfeld

TAG 3

09.00-09.30
Begrüßung durch den Seminarleiter und Rückblick auf Tag 2

09.30-10.30
Praktischer Teil I
- Sicherstellungskonzept in der Praxis
- Dokumentationsverfahren
- Vermeiden von Fehlern

10.30-11.00
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

11.00-12.30
Praktischer Teil II
- Vorführung einer Auswertung mit forensischer Auswertesoftware
- Die Alarmkette bei einem Sicherheitsvorfall
- „Forensic Readiness“ in Unternehmen aus praktischer Sicht

12.30-13.30
Mittagspause

13.30-15.30
Prüfung
- Wiederholung und Prüfungsvorbereitung
- Klärung auftretender Fragen
- Schriftliche Prüfung

15.30-15.45
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

15.45-16.30
- Bekanntgabe Ergebnisse
- Ausgabe der Teilnahmebescheinigungen
- Abschlussbesprechung

16.30
Ende des Seminars

bitkom akademie

Ihre Referenten

Peter Meyer

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

Peter Meyer ist seit über 10 Jahren IT-Forensiker und dabei u.a. auf die digital-forensische Bearbeitung von Wirtschaftsdelikten wie Datensabotage, Datenabfluss, Bilanzfälschung sowie die Analyse von Datenbanken in ERP Systemen bei Verdachtsmomenten auf Betrug und Verschleierung von Finanzströmen (Geldwäsche) spezialisiert. Er ist zudem Mitglied in folgenden Verbänden: (1) Deutsche Gesellschaft für Kriminalistik e.V (DGfK) AGs Computerkriminalität und Wirtschaftskriminalität, (2) im Deutscher EDV-Gerichtstag e.V. sowie (3) dem Soforthilfe nach gravierenden Unfällen - Zoll - e.V.

Thomas Schmalz

IT-Forensiker

Thomas Schmalz hat den Bachelor of Engineering in IT-Forensik und ist aktuell als angestellter IT-Forensiker tätig. Er startete seine berufliche Laufbahn als Software-Entwickler und hat sich seit einigen Jahren auf die IT-Forensik spezialisiert, insbesondere auf die Auswertung von Hauptspeichern (RAM-Forensik). Er ist Mitglied in der Deutschen Gesellschaft für Kriminalistik e.V (DGfK) und Teilnehmer der Allianz für Cyber-Sicherheit vom BSI.

Shortfacts

Preise

1.950 €* Regulär

1.750 €* für Bitkom-Mitglieder

120 € Zertifizierung (optional)

**Die angegebenen Preise sind in Netto-Beträgen ausgewiesen.*

Termine und Veranstaltungsort

Die Termine entnehmen Sie bitte der Website der Bitkom Akademie. hier ↗

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