>> IT Forensik

Workshop zur Umsetzung

Unter IT Forensik versteht man die Verfolgung von Spuren auf einem System. Sei es die Nachverfolgung eines Einbruchversuchs in ein Netzwerk oder die Beweissicherung in strittigen Fällen.

Ihr Nutzen

Dieses Seminar gibt Ihnen einen Überblick über die Konzepte der Forensik und Aktionen die in einem Notfall (Einbruch, Diebstahl, DOS Attacke) durchzuführen sind. Nach dem Seminar können Sie mit Forensic Case Tools umgehen und Beweise und Vorgänge auf IT-Systemen entsprechend sichern.

Preis pro Teilnehmer

EUR 2850,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Seminarinhalte

1. Tag
* Einführung in Computer-Forensik
- Unterscheidung Netzwerk/System-Forensik

* Ansatzpunkte für forensische Untersuchungen im Netzwerk

* Strukturierung einer forensischen Untersuchung

* Beweissicherung für gerichtliche Zwecke

* Netzwerkforensik
- Sammeln von relevanten Daten
- Datenauswertung
- Datenarchivierung

* Forensische Untersuchungen
- Ablaufpläne
- Checklisten

2. Tag
* Konzepte in der IT Forensik
- Kodierung
- Dateierweiterungen und Header
- Speicher und Hauptspeicher
- Flüchtige / Nicht flüchtige Speicher
- Computer / Netzwerke / Mainframe / Cloud
- Arten von Daten
- Dateisystem
- Belegter / Freier Speicher
- File Carving

* Das Forensische Labor einrichten

* Auswahl von Tools
- Sichern der Daten
- Dokumentation

3. Tag
* Methoden in der Forensik
- Dokumentieren der Umgebung
- Spurensicherung
- Forensisches Clonen der Datenträger
- Live System versus Dead System

Voraussetzungen

Grundkenntnisse der PC und Netzwerksicherheit.

Hinweise

Version: N/A

- Hashing
- Berichterstellung

* Windows System Artifakte
- Gelöschte Daten
- Hibernate/Page-Files
- Die Registry
- Print Spooler
- Metadaten
- Prefetch,Link Files,Shadow Copies, Recent Files

* Interessante Spuren
- Eventlogs
- Applikations-Installationen erkennen
- Seltsame Services erkennen
- Database Mystery (ESE, Thumbs.DB, Index)
- USB/BYOD Forensik auf Windows Systemen

4. Tag
* Antiforensik
- Das Konzept der Antiforensik
- Daten verstecken
- Daten vernichten

* Browser und E-Mail
- Cookies
- Web Cache
- History
- E-Mail Spuren

* Übersicht über Forensik im Netzwerk

* Übersicht über Mobile Device Forensik

Unsere BildungsberaterInnen stehen Ihnen gerne zur Verfügung. Innsbruck +43 (0)512 36 47 77.