

Workshop IT-Forensik

IT-Forensik (3 Tage)

Sowohl im Internet als auch im Firmennetz werden Systeme täglich Opfer von Hackerangriffen.

Wenn nun der Ernstfall eines solchen Angriffs eintritt, stellt sich die Frage nach den Ursachen der Angriffe und der Vorgehensweise und Identität des Täters. Dabei wird der Angriff forensisch untersucht, was bedeutet, dass Spuren identifiziert und diese (gerichtsverwertbar) gesichert werden. Danach erfolgt ihre Auswertung und Aufbereitung als Beweismittel.

Inhalt des Workshops:

- **Definition**
Forensik, IT-Forensik
- **Auftreten von Spuren**
Festplatte, Hauptspeicher (Prozesse, Netzwerkverbindungen, offene Dateien, etc.)
Mobiltelefon, SIM-Karte, PDA
versteckte Spuren (z.B. Steganografie)
- **Sicherung von Spuren, lokal und über das Netzwerk**
- **Sicherstellung der Authentizität von Spuren, Gerichtsverwertbarkeit**
- **Analyse der erhobenen Daten**
Werkzeuge unter Windows und Linux
Ursachenforschung
Rückschlussmöglichkeiten auf Ziele und Kenntnisstand des Täters
- **Verfassen von gerichtskonformen Berichten**
- **Projektmanagement: IT-Forensik**
Zusammenarbeit mit Strafverfolgungsbehörden
rechtliche Situation

Zielgruppe:	Administratoren, IT-Sicherheitsverantwortliche, betriebliche Ermittler
Lernziel:	Behandlung grundlegender Fragestellungen der IT-Forensik und Standardtechniken
Nützliche Vorkenntnisse	Grundkenntnisse über Netzwerke, Grundkenntnisse in WINDOWS, LINUX oder UNIX
Dauer:	3 Tage
Teilnehmerzahl:	4-6