

IT Forensik - Das Kompaktseminar für den Ernstfall!

- > Wie erkenne ich den Einbruch in mein System?
- > Wie sichert man Beweise gerichtsverwertbar?
- > Welche organisatorischen und technischen Vorbereitungen sind zu treffen? Und wie geht man im Ernstfall strukturiert vor?
- > Welche Fehler gilt es zu vermeiden?
- > Welche straf- und zivilrechtlichen Möglichkeiten gibt es?

[kompaktseminar]

Unser Kompaktseminar bereitet Sie auf den Ernstfall vor
Egal ob externe Angreifer oder interne Spionage!

Das Seminar gliedert sich praxisgerecht in organisatorische und technische Inhalte

Mit Checklisten und Formularen für das Ermittlungsteam

Und zeigt Ihnen was Sie bereits jetzt vorbereiten sollten!

[vorkenntnisse]

Dieses Seminar richtet sich an IT Leiter, IT Security Verantwortliche und Risk Manager

Gute PC Grundkenntnisse werden vorausgesetzt - Forensik Vorkenntnisse sind nicht erforderlich

[inhalte]

[tag 1]

- > **Forensik heute** Zahlen & Fakten
- > **Tätergruppen Analyse** Extern und Intern
- > **Ablauf eines Angriffs** aus der Sicht des Hackers
- > **Incident Detection** Hacker im System?
- > **Response Strategie** Forensik oder System Wiederherstellung?
- > **Incident Response** Vorgehen im Verdachtsfall
- > **Gerichtsverwertbarkeit** Beweissicherungs Formular

[tag 2]

- > **Forensik Tools im Einsatz** Open Source u. Kommerziell
 - > **Analyse laufender Systeme**
 - > **Forensische Duplikate** selbst erstellen
 - > **Post Mortem** Offline Analyse
 - > **Virtuelle Server** und Forensik
 - > **Mobile Devices** Mobiltelefone, PDAs, ...
- > **Wieder Herstellung** gelöschter bzw. veränderter Daten
- > **Anti Forensik** so werden Angriffe verschleiert

[tag 3]

- > **Rechtliche Voraussetzungen und Folgen für Unternehmen**
Gefahren für Administrator und das Unternehmen,
Die Rolle des Betriebsrats,
Eskalationsmechanismen, ...
- > **Incident Response Plan** best Practice mit Checkliste
- > **Zivil- und Strafrechtliche Möglichkeiten**
- > **Fallbeispiel** Mittels des erworbenen Wissens erstellen Sie selbstständig eine forensische Analyse. Setzen Sie dabei organisatorische und technische Anforderungen in der Praxis um!
- > **Abschluss mit Zertifikat**