SC450 Digitale Forensik für Fachexperten

Kurzbeschreibung:

IT-Sicherheitsfachkräfte und Administratoren erhalten eine praxisnahe Einführung in digitale Forensik. Vermittelt wird die Analyse von Windows- und Linuxsystemen nach forensischen Prinzipien sowie der Umgang mit typischen Artefakten. Behandelt werden Methoden zur Spurensicherung, praktische Übungen und Diskussionen. Das Training schließt mit einer Prüfung ab.

Zielgruppe:

- Praktiker, insbesondere der Informatik und verwandter Fächer
- IT-Administratoren
- Angehende IT-Forensiker

Voraussetzungen:

Ein gutes Verständnis von IT-Systemen und -Begriffen wird erwartet.

Sonstiges:

Dauer: 5 Tage

Preis: 2850 Euro plus Mwst.

Ziele:

Die Beweissicherung und der Nachweis strafbarer Handlungen bei IT-Sicherheitsvorfällen stellt Unternehmen häufig vor große Herausforderungen.

In diesem Workshop vermitteln wir Ihnen das nötige Insider-Wissen, wie Sie bei IT-Sicherheitsvorfällen forensische Analysen von Windows- und Linux-Systemen durchführen und gerichtsverwertbare Beweise sichern und auswerten können. Der Schwerpunkt des Workshops liegt auf der **praxisorientierten** Vermittlung grundlegender Kenntnisse IT-forensischer Arbeit.

Am Ende des Workshops werden Sie fähig sein:

- Sicherheitsvorfällen sicherer und richtig zu begegnen
- gerichtsverwertbar Spuren zu sichern
- eigenständig Schritte einer forensischen Analyse von Windows-Systemen durchzuführen
- einen erheblichen Beitrag zur beweissicheren Aufklärung von Cyberangriffen zu leisten, um Tätern auf die Spur zu kommen

Inhalte/Agenda:

- ♦ **Begrüßung, Kennenlernen, Orga**

- ♦ **Einführung**
- ♦ ◊ Kontext: Informationssicherheit, IT-Sicherheit und Datenschutz
  ◊ Bedeutung Forensik
  ◊ Einführung in Incident Response
  ◊ · Definition, Zielsetzung
  · Problemfelder und Empfehlungen
  ◊ Einführung in die digitale Forensik (Erster Einblick: Definition, Zielsetzung)
  ◊ Exkurs: Strafrecht

- ♦ **Angriffe verstehen**
- ♦ ◊ Angreifer und deren Motivationen
  ◊ Häufige Angriffstechniken & Angriffsziele
  ◊ CTF: live Pentest

- ♦ **Incident Response (Theorie und Grundlagen)**
- ♦ ◊ Incident Response (BlueTeam)
  ◊ Windows Forensik
  ◊ Übung: digitale Spurensuche
  ◊ Gerichtsverwertbare Dokumentation

- ♦ **Praxis: Handlungsempfehlungen und Werkzeuge**
- ♦ ◊ Diskussion zu Maßnahmen nach Erkenntnisgewinn aus der IT-Forensik
  ◊ Welche Tools werden zwingend benötigt?
  ◊ Welche Tools sind "nice to have"?

- ♦ **Praxisschwerpunkt: Windows Forensik**
- ♦ ◊ Windows Registry
  ◊ · Registry Hives online und offline
  · Tools zur Datenerfassung
  · Tools zur Registry-Auswertung
  ◊ Systeminformationen
  ◊ · OS-Version
  · Current Control Set
  · Computer Name
  · Zeitzone
  · Netzwerkinterfaces
  · Autostart
  · SAM Hive und User Informationen
  ◊ Systemanmeldungen
  ◊ Event Logs
  ◊ Netzwerkverbindungen
  ◊ Fernzugriffe
  ◊ USB-Geräte
  ◊ · Geräte Identifikation
  · First/Last Times
  ◊ Dateizugriffe
  ◊ · Recent Files
  · Office Recent Files
  · ShellBags
  · Open/Save and LastVisited Dialog MRUs
  · Windows Explorer Address/Search Bars
  ◊ Dateiausführungen
  ◊ · User Assist
  · ShimCache
  · AmCache
  · BAM/DAM
  ◊ Gelöschte Dateien

- ♦ **Kompakt: Linux-Forensik**
- ♦ ◊ Systeminformationen
  ◊ ·

- User Account
- User Groups
- Sudoers List
- Systemanmeldungen

◊ System-Konfiguration
- Hostname
- Zeitzone
- Netzwerk-Konfiguration
- Prozesse
- DNS-Informationen

◊ Persistence mechanism
- Cron jobs
- Services
- Bash/shell startup

◊ Log-Dateien
- Syslogs
- Authentication logs
- Third-party logs

◊ Gelöschte Dateien

♦ **Wiederholung und Abschlussprüfung**

◊ Quiz
◊ Beantwortung von Fragen und Diskussion
◊ Prüfung

♦ ◊