SC450 Digitale Forensik für Fachexperten

Kurzbeschreibung:

Cyberkriminelle stellen durch Phishing, Hacking oder Scamming eine hohe Gefahr für Unternehmen und deren sensible Daten dar. Um den Gefahren eines Angriffs vorzubeugen bzw. im Falle eines Angriffs die von Tätern hinterlassenen Spuren aufzuspüren und gerichtsverwertbar zu sichern, bedarf es IT-forensischer Kenntnisse.

Der Fokus des Workshops **SC450 Digitale Forensik für Fachexperten** liegt auf der praktischen Analyse von Windows- und Linuxsystemen unter Berücksichtigung IT-forensischer Prinzipien.

Hierbei wird sowohl auf die Grundlagen digitaler Forensik als auch detailliert auf einzelne IT-forensische Artefakte eingegangen. Die Inhalte werden in überschaubarer Runde in Form von Präsentationen, praktischen Übungen und Gruppendiskussionen interaktiv erarbeitet.

Das Seminar schließt am letzten Seminartag mit einer Prüfung sowie einem Zertifikat ab.

Für die Prüfung, die am Nachmittag stattfindet, haben die Teilnehmer 90 Minuten Zeit. Es handelt sich um 40 Multiple Choice-Fragen. Um die Prüfung erfolgreich zu bestehen, müssen 70 % davon richtig beantwortet werden.

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

◆ ◊