SC430 Digitale Forensik

Kurzbeschreibung:

Cyberkriminelle stellen durch Phishing, Hacking oder Scamming eine hohe Gefahr für Unternehmen und deren hoch sensiblen 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.

Profitieren Sie in diesem Seminar von den Erfahrungen und Kenntnissen einer Kriminalkommissarin und erfahren Sie die grundlegenden Kenntnisse IT-forensischer Arbeit. Der Fokus liegt auf der praktischen Anwendung IT-forensischer Vorgehensweisen, Prozessen und Analysen. Hierzu gehören alle Leistungen im Bereich der Digital Forensics

- Digitale Forensik und Incident Response (DFIR)
- Bearbeitung von IT-Sicherheitsvorfällen in der IT-Forensik (Reaktion)
- Vorbeugung von IT-Sicherheitsvorfällen (Prävention)
- Erkennung und Einschätzung von Sicherheitslücken (Detektion)

Hierbei wird sowohl auf die Grundlagen im Bereich DFIR als auch detailliert auf einzelne Ermittlungsphasen- und Schritte eingegangen

Anhand von expliziten Fallbeispielen werden z. B. die Phasen des Incident Response Prozesses nähergebracht sowie die einzelnen Schritte einer IT-forensischen Analyse von Windowssystemen durchgeführt, um umfassend Benutzerinteraktionen nachweisen und interpretieren zu können.

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
- Verantwortliche im Bereich Informationssicherheit
- IT-Sicherheitsmanager
- Informationssicherheitsbeauftragte / IT-Sicherheitsbeauftragte
- CISO / CIO

Voraussetzungen:

Ein grundlegendes 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 durchführen und gerichtsverwertbare Beweise sichern und auswerten können. Sie lernen eine neue Sichtweise kennen, um diesen Angriffen vorbereitet begegnen zu können Der Schwerpunkt des Workshops liegt auf der **praxisorientierten** Vermittlung grundlegender Kenntnisse IT-forensischer Arbeit. Sie werden alle Leistungen im Bereich Digital Forensics and Incident Response (DFIR) kennenlernen.

Am Ende des Workshops werden Sie fähig sein:

- Sicherheitsvorfälle besser einschätzen zu können
- Eigenständig Schritte für eine forensischen Analyse zur gerichtsverwertbaren Sicherung von Spuren durchzuführen
- reaktive Maßnahmen einzuleiten
- Maßnahmen zur Vorbeugung von IT-Sicherheitsvorfällen einzuleiten
- Sie erhalten Handlungsempfehlungen für den Umgang mit Ermittlungsbehörden

Inhalte/Agenda:

- Vorstellen und Kennenlernen

- Digitale Forensik und Incident Response (DFIR)
    - ♦ Von der Allgemeinen zur Digitalen Forensik
    - ♦ Grundbegriffe DFIR
    - ♦ Spurentheorie
    - ♦ Chain of Custody
    - ♦ Prinzipien
    - ♦ Herausforderungen

- Datenträgerforensik
    - ♦ Datensammlung und -sicherung
    - ♦ IT-Forensische Analyse
        - ◊ Windows Registry
        - ◊ USB-Nutzung
        - ◊ Shell Items
        - ◊ E-Mail-Artefakte
        - ◊ Eventlogs
        - ◊ Browsernutzung
        - ◊ Relevanz des Arbeitsspeichers
    - ♦ Dokumentation
    - ♦ Der forensische Bericht

- Incident Response (IR)
    - ♦ IR Prozess (IRP)
        - ◊ Vor einem IR
            - · Incident Response Plan (IR)
        - ◊ Währenddessen
            - · Klassische forensische Rolle im IRP
            - · Ganzheitlicher Ansatz IR
            - · Kill Chain
        - ◊ Nach einem IR
            - · Nachbereitung, Lessons Learned
    - ♦ Umgang mit Ermittlungsbehörden

- Präventive Forensik
    - ♦ Was ist präventive Forensik?
    - ♦ Rahmenverträge
    - ♦ Workshops, Trainings, Schulungen
    - ♦ Szenario
    - ♦ Nutzen

- Detektive Forensik
    - ♦ Schnittstelle zur IT-Sicherheit
    - ♦ IT-Schwachstellenanalyse
    - ♦ Penetrationstest
    - ♦ Erkenntnisse für IT-Forensiker

- Weitere forensische Felder und Ausblick