S E M I N A R E

Microsoft

2174

Online – IT-Forensik Praxis-Workshop (MS IT Boot-Camp)

Die Fälle von Computer- und Internetkriminalität nehmen weiterhin zu. Dabei sind es nicht nur externe Angriffe, welche Schäden verursachen, sondern auch bestehende oder ehemalige Mitarbeiter.

Besteht der Verdacht einer kriminellen Handlung, dann kommt es auf ein methodisches und sorgfältiges Vorgehen an.

Dabei trägt die IT-Forensik nicht nur zur Schadenaufklärung und Identifikation des Täters bei, sondern unterstützt in der Ermittlung und Beseitigung von Schwachstellen in einer Organisation.

o Zielgruppe

Der Workshop richtet sich an Leiter und Mitarbeiter aus den Bereichen:
Informationssicherheit / IT-Sicherheit / CERT
Die Fälle von Computer- und Internetkriminalität nehmen weiterhin zu. Dabei sind es nicht nur externe Angriffe, welche Schäden verursachen, sondern auch bestehende oder ehemalige Mitarbeiter.
Besteht der Verdacht einer kriminellen Handlung, dann kommt es auf ein methodisches und sorgfältiges Vorgehen an.
Dabei trägt die IT-Forensik nicht nur zur Schadenaufklärung und Identifikation des Täters bei, sondern unterstützt in der Ermittlung und Beseitigung von Schwachstellen in einer Organisation.

o Voraussetzungen

Die Teilnehmer sollten über detaillierte Kenntnisse in den Bereichen Netzwerktechnologien und Betriebssysteme (Fokus Microsoft Windows) verfügen

Software:
-TeamViewer 15 als Meeting-Client (Freie Version)
Hardware:
-Headset oder Lautsprecher/Mikrofon für die Kommunikation
-Für eine Sichtverbindung ist der Einsatz einer Kamera hilfreich (nicht verpflichtend)
-Wünschenswert ist ein 2. Monitor
-Bildschirmauflösung: 1600x900

o Seminarziel

Dieses 3-tägige IT-Bootcamp bietet eine Einführung in die IT-Forensik (z. B. technische Begriffe, rechtliche Aspekte, Organisation, Vorgehensweisen) an Windows-Systemen und vermittelt das Grundlagenwissen, um
• Vorfälle auf der Datenträgerebene und relevanter Komponenten zu erkennen,
• Vorgehensweise zur gerichtsverwertbaren Spurensicherung,
• Analyse der verschiedenen Datenträgerarten, wie z. B. Festplatten usw.,
• Gebräuchliche Werkzeuge der IT-Forensik zur Sicherung und Analyse von Daten auf Datenträgern.
Im Seminar werden Erfahrungsberichte aus der Ermittlungspraxis gegeben und die praktischen Anwendungen der IT-forensischen Methoden und Werkzeuge anschaulich demonstriert und geübt.

o Seminarinhalt

Einführung
- Überblick über die IT-Forensik
- Aktuelle Herausforderungen an die IT-Forensik
- Ziele einer IT-forensischen Untersuchung
- Grundsätze forensischer Arbeitsweise
- Rechtliche Aspekte (Datenschutz und Telekommunikationsgesetz)
- Beispiele aus der Ermittlungspraxis

Identifizierung von relevanten Datenquellen
Forensische Datensicherung von relevanten Datenquellen
- Laptop / Desktop
- E-Mail-Server
- File-Server

CONSULTING & INFORMATIONSDIENSTE GMBH

München
Berghamer Straße 14
85435 Erding
Tel.: 0 81 22 / 97 40 - 0
Fax: 0 81 22 / 97 40 - 10

Erfurt
Michaelisstraße 13a
99084 Erfurt
Tel.: 03 61 / 5 65 93 - 0
Fax: 03 61 / 5 65 93 - 10

Internet
www.md-consulting.de

E-Mail
info@md-consulting.de

Bankverbindung
HypoVereinsbank
Erfurt

IBAN:
DE84 8202 0086
0003 9840 95

SWIFT/BIC:
HYVEDEMM 498

Geschäftsführer
Dr. Martin Diestelmann

HRB München 289362

USt.Id Nr.:
DE 150 108 446

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2174

- Mobile Geräte (Smartphones, Tablets, etc.)
- Daten in der Cloud
- Hauptspeicher

Technische Grundlagen

- Aufbau einer Festplatte
- Partitionstabellen
- Dateisysteme

Wiederherstellung von gelöschten bzw. geänderten Dateien

- Gelöschte Dateien und deren Rekonstruktion
- File Carving
- Volume Shadow Copy

Vorgehensweise bei verschlüsselten Daten/Datenträgern

- Festplattenverschlüsselung
- Dateiverschlüsselung

Dateianalyse

- Keyword-Suche
- Metadaten

Windows-Systemanalyse

- Systeminformationen
- Registry
- Log Files
- User-Aktivitäten
- Internet Forensic (Webbrowser, E-Mails)

Hauptspeicher-Analyse

- Laufende Prozesse
- Netzwerkaktivitäten
- Anhaltspunkte für Malware

o **Seminardauer: 3 Tage a 2 x 3 Stunden,** jeweils von 9-12 Uhr und 13-16 Uhr
Im Preis enthalten sind kursbegleitende Seminarunterlagen.

o **Preis pro Person: 1.990 EUR netto**