

Forensic Extrem

Referenten: Tobias Klein, Andreas Kutz, Marco Lorenz und ein Anwalt der Kanzlei Amann

Dauer: 3 Tage

Inhalt:

In diesem Training werden aktuelle technische Methoden der IT-Forensik und des Incident Handling sowie die damit verbundenen rechtlichen Rahmenbedingungen und Möglichkeiten vorgestellt.

Anhand vieler verschiedener Fallbeispiele wird das richtige Vorgehen bei einem Verdacht auf Hacker-Einbruch, Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung von firmeneigenen Kommunikationsmöglichkeiten erörtert.

Die Schulung teilt sich in einen technischen Teil, in dem Werkzeuge für eine forensische Analyse vorgestellt werden und in einen rechtlichen/organisatorischen Teil, in dem die rechtlichen Rahmenbedingungen für Inhouse-Ermittlungen gegen Verdächtige dargestellt werden.

Im **technischen Teil** lernt jeder Teilnehmer anhand vieler Übungen, die er auf einem zur Verfügung gestellten Laptop selbst nachvollzieht, Spuren in IT-Systemen zu suchen, richtig zu sichern und zu interpretieren. Jedem Teilnehmer wird eine Werkzeugsammlung zur Live-Analyse bereit gestellt, die u.a. bisher nicht verfügbare Sammel- und Analysewerkzeuge beinhaltet. Zudem werden im Bereich der Dead-Analyse neben frei verfügbaren Werkzeugen auch etablierte kommerzielle Produkte vorgestellt und eingesetzt.

Bei der Live-Analyse geht es um die Sammlung und Analyse flüchtiger Daten aus laufenden Systemen. Dabei werden Kernel-Komponenten, der Netzwerkstatus und der Hauptspeicher ebenso betrachtet wie der virtuelle Speicher einzelner Prozesse. Im Gegensatz zu den bekannten Methoden der Festplatten-Analyse werden hier fortgeschrittene Methoden zur Informationsgewinnung verwendet, die darauf zielen, Malware (Würmer, Trojaner, etc.) sowie Kernel-Rootkits zu erkennen, Code-Injection-Angriffen nachzuvollziehen oder generell Daten direkt aus dem Speicher (Bilder, Dokumente, etc) zu extrahieren.

Bei der Dead-Analyse geht es um die Sammlung und Analyse persistenter Daten. Die Teilnehmer werden mit der Erstellung von Festplatten-Images vertraut gemacht, der Auswertung der Dateisystem-Metadaten, der Behandlung diverser Dateisysteme (NTFS, ext3, etc.), der Wiederherstellung gelöschter Daten und

der Auswertung von Logfiles.

Im **rechtlichen/organisatorischen Teil** wird ein Rechtsanwalt der Anwaltskanzlei Amann detailliert auf die Vorgehensweise nach der Entdeckung von Einbrüchen eingehen. Fall für Fall wird die Sammlung, Sicherung und Auswertung gerichtsfester digitaler Spuren als Beweismittel zur erfolgreichen Rechtsverfolgung durchgespielt.

Dabei wird berücksichtigt, welche Tätergruppe in Betracht kommt, welches übergeordnete Ziel (bspw. Schädigung der Firma) der Angriff wirklich hatte, was geschützt werden muss und welches Schadenspotential der Angriff hatte. Ebenso wird erörtert, welche Beweismittel durch eigene Ermittlungen beschafft werden können, welche nur unter Einschaltung Dritter oder der Polizei und in wieweit eine Strafanzeige gegen Verdächtige hilft.

Nach Abschluss des Trainings sind die Teilnehmer in der Lage, die Wege eines Einbrechers nachzuvollziehen. Sie wissen, wie sie im Falle eines Systemeinbruchs reagieren müssen und welche Anforderungen an die gerichtsfeste Sammlung, Speicherung und Auswertung digitaler Spuren als Beweismittel beachtet werden müssen.

Themenbereiche:

- Sammlung und Sicherung flüchtiger Daten
- Sammlung und Sicherung persistenter Daten
- Zusammenstellung einer Werkzeugsammlung
- Auswertung der gesammelten Daten
- Hash-Datenbanken
- Carving
- Gezielte Suche nach Begriffen
- Extrahierung und Analyse von Zeitstempeln
- Extrahierung und Analyse von Logfiles
- Beschreibung verschiedener Anti-Forensik-Techniken
- Haupt- und Prozessspeicheranalyse
- Auffinden und Deaktivierung von Rootkits
- etc.

Behandelte Werkzeuge: Open-Source- sowie kommerzielle Werkzeuge

Behandelte Betriebssysteme: Windows, Linux, Unix

Zielgruppe:

Administratoren, Sicherheitsverantwortliche, CERT-Teams, betriebliche Ermittler

Voraussetzung:

Grundlegende Kenntnis von Windows, Linux und Unix. Von Vorteil sind



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern. Eine Teilnahme am Training "Hacking Extrem" ist von Vorteil.

Preis: 2.400,- €

Das Training wird in deutscher Sprache von erfahrenen Trainern und in Kooperation mit der Anwaltskanzlei Amann durchgeführt.