iMes IT-Forensik/Datenforensik

Betrieblicher Investitions- und Datenschutz

Computerbetrug / Schadsoftware (Malware) aufspüren

Wenn Daten verschwinden oder der Verdacht der Spionage im Raum steht, ruft das die fortschrittlichen Methoden der **IT-Forensik/Datenforensik** auf den Plan. Die **IT-Forensik** ist ein großes Gebiet, das sich verschiedenster moderner Methoden bedient, um Tatabläufe zu rekonstruieren und in letzter Folge dem Täter auf die Schliche zu kommen. Damit ist die **IT-Forensik** ein essenzieller Bestandteil jedes Konzepts, das die Computersicherheit eines Unternehmens komplett abdeckt.

Die Erfahrung unserer **IT-Forensiker** zeigt, dass die Bedrohung der Computersicherheit oftmals nicht von außen erfolgt, sondern eventuell vom benachbarten Arbeitsplatz. Netzwerke können noch so gut gegen externe Bedrohungen abgesichert sein – gegen Angriffe aus den eigenen Reihen sind viele Sicherheitsvorkehrungen wirkungslos.

Unter **IT-Forensik/Datenforensik** versteht man die Untersuchung von verdächtigen Vorfällen an Computer-Systemen. Dazu gehören sowohl die Feststellung des Tatbestandes und des Tathergang es, als auch die Ausforschung des Täters sowie die **Wiederherstellung** der Daten.

Szenario:

- Besteht der Verdacht, dass jemand Ihre Systeme manipuliert?
- Sie vermuten, jemand verwendet Ihren Computer zu illegalen Aktivitäten?
- Ihr Provider hat Ihnen mitgeteilt, dass auf Ihrem Server eingebrochen wurde?

Nutzen:

- Untersuchung Ihrer Computersysteme
- Sicherung, Auswertung und Analyse digitaler Spuren
- Frühzeitiges Einleiten von Gegenmaßnahmen
- Wiederherstellung der Daten
- Aufbereitung und Auswertung der Untersuchungsergebnisse

Vorgehensweise:

Grundsätzliches:

- Unterscheidung zwischen **lebenden** und **toten** Systemen
  - In lebenden Systemen können sich noch Beweise im Arbeitsspeicher, in der Prozessliste etc. befinden
  - Bei toten Systemen ist der Inhalt des Arbeitsspeichers nicht mehr ohne weiteres auslesbar

iMes IT-Forensik/Datenforensik

Betrieblicher Investitions- und Datenschutz

Computerbetrug / Schadsoftware (Malware) aufspüren

Vorgehensweise bei lebenden Systemen:

- Lebendes System wird auf **Schadsoftware** untersucht
  - Aufdeckung von eventuell vorhandenen **Rootkits**
  - Verdächtige Prozesse werden untersucht
- Werden verdächtige Spuren entdeckt, erfolgt die Analyse der gesamten Festplatte

Vorgehensweise bei toten Systemen:

- Erstellung einer 1:1-Kopie (**Image**)
  - Auf einer Kopie der Kopie wird Untersuchung durchgeführt
  - Image wird in einer gestützten Umgebung virtualisiert und so **live** untersucht

Besteht der Verdacht, dass das System infiziert wurde, gilt es, möglichst wenige Spuren zu verwischen.

Bei Windows werden z. B. beim Herunterfahren oder Neustarten tausende Dateien geschrieben. Damit wird es immer schwieriger, **digitale Spuren** zu sichern. Nach dem Verdacht ist es am besten, das Computersystem im IST-Zustand zu belassen und eine fachkundige Person (**Incident Handler** oder **Forensiker**) zu Rate zu ziehen. Die einzige vertretbare und empfohlene Aktion ist das Ziehen des Netzwerksteckers. Damit ist das System isoliert und kann keinen Schaden mehr anrichten.