Forensik – Spurensicherung

Wurde ein erfolgreicher Cyber-Angriff auf ein Unternehmen verübt, gilt es Spuren zu sichern, um den Vorfall und das Vorgehen nachvollziehen zu können. Dabei gilt es einige Dinge zu beachten, um diese auch gerichtlich verwerten zu können (Beweismittel) und nicht Spuren zu zerstören. Hier kommt die IT-Forensik zum Einsatz.

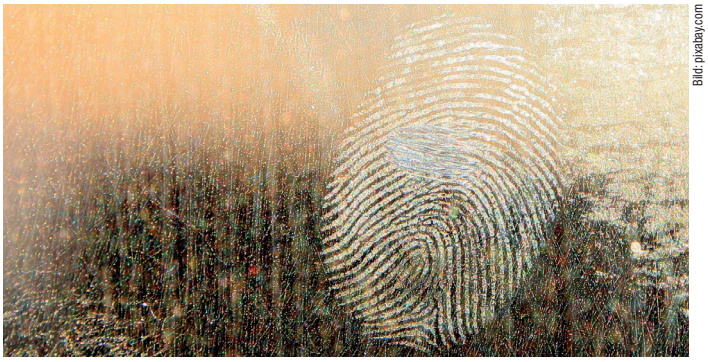


Bild: pixabay.com

Ein strukturiertes Vorgehen hilft, alle notwendigen Beweise rechtssicher zu sammeln und auszuwerten.

Wir kennen dies von TV-Sendungen wie CSI. Doch im echten Leben ist es doch nicht so einfach und so schnell.

Folgende Ziele werden dabei verfolgt:
- die Identifikation des Angreifers,
- das Vorgehen und die ausgenutzte Schwachstelle, die zum Systemeinbruch geführt hat,
- die Ermittlung des entstandenen Schadens, und
- die Sicherung der Beweise für weitere Schritte.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert IT-Forensik wie folgt: IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

Die IT-Forensik kann in Computer-Forensik und Daten-Forensik unterteilt werden.
- Die Daten-Forensik beschäftigt sich mit den gespeicherten Daten (Datenbanken).
- Die Computer-Forensik mit den darunter liegenden Systemen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Ablauf einer forensischen Ermittlung

Bei einer forensischen Ermittlung durch die Polizei werden folgende Schritte durchgeführt [1]:
- Eröffnen des Falls durch Sachbearbeiter der Polizei aufgrund einer Anzeige oder eines entsprechenden Hinweises
- Untersuchungsrichter (UR) ordnet (unter anderem) eine Hausdurchsuchung (HD) an
- Beginn der allgemeinen Ermittlungen im Fall
- Abschätzen der zu untersuchenden IT-Infrastruktur
- Allenfalls Einbezug von externen Experten
- Vorbesprechung und Durchführung der HD
- Sicherstellung und Aufbereitung der Daten
- Analyse der Daten
- Einreichen des abschliessenden Berichts an UR

Vorgehensweise

Ein Bearbeitungsvorgang in der IT-Forensik lässt sich in fünf Phasen unterteilen:

Vorbereitung

In einem ersten Schritt gilt es alle Massnahmen vor dem eigentlichen Eintreten eines Ereignisses zu planen. Dazu gehören die Sammlung von Logdaten, sicherstellen dass alle Systeme die korrekte Zeit haben oder auch die Durchführung einer Risikoanalyse zum Abschätzen der möglichen Eintrittspunkte.

Identifikation

Das Ziel einer forensischen Analyse ist die Beantwortung der folgenden Fragen:
- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

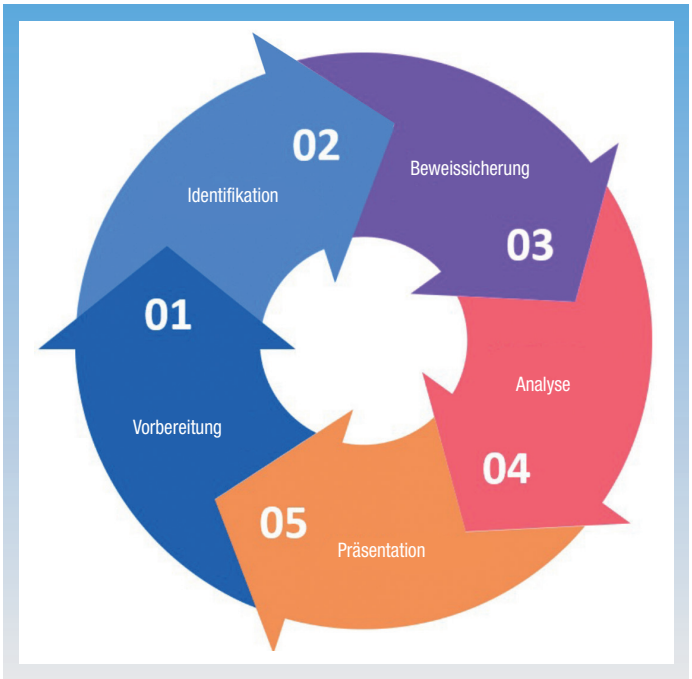
Im Fall der Strafverfolgung oder einer Sicherheitsbewertung können weitere Fragestellungen relevant werden:
- Wer hat es getan?
- Wie kann eine Wiederholung vermieden werden?

Beweissicherung

Der erste Schritt muss es immer sein, keine Spuren zu vernichten. Das beinhaltet nicht mit Original-Daten zu arbeiten, Zugriffe auf die zu untersuchenden Daten einzuschränken, E-Mail-Zugriffe anzupassen, Passwörter wo notwendig anzupassen. Untersuchungen können Post-Mortem, das heisst mit eins-zu-eins-Kopien von Systemen oder per Live-Response, welche am laufenden System erhoben wurden. Dies kann bei Verschlüsselungstechniken oder proprietären Systemen der Fall sein. Muss das System ausgeschalten werden, können Daten verloren gehen. Auch das Trennen der Netzwerkverbindung kann die Echtheit der Daten gefährden. Daher ist es wichtig, diesen Entscheid klar zu dokumentieren.

Analyse

Die verschiedenen Daten werden mittels verschiedener Programme aufbereitet, analysiert und die notwendigen Beweise extrahiert. Dabei fallen sehr viele Daten an, die in einen Zusammenhang gebracht werden müssen. Es ist wichtig, den roten Faden nicht zu verlieren. Ein ideales Werkzeug ist hier der Zeitstrahl. Alle Infor-



Fünf Phasen der IT-Forensik.

Literatur

[1] Informationssicherheitshandbuch für die Praxis 9.0
[2] https://www.dfir.training/
[3] https://digital-forensics.sans.org/
[4] https://digital-forensics.sans.org/community/papers/gcfa/windows-10-forensic-platform_13102

mationen werden in zeitlicher Reihenfolge aufgelistet und dadurch übersichtlich visualisiert.

Präsentation

Die gesammelten Daten werden nach der Auswertung so aufbereitet, dass auch Laien, wie auch andere Experten nachvollzogen werden kann, was geschehen ist. Dies wird klassischerweise in einem Bericht festgehalten, der die notwendigen Fakten präsentiert. Die Interpretation der Ergebnisse muss dabei in einem eigenen Kapitel erfolgen. Dies kann folgende Punkte enthalten:

- Ermittlung der Identität des Täters/der Täter
- Ermittlung des Zeitraumst
- Ermittlung des Umfanges
- Ermittlung der Motivation
- Ermittlung der Ursache und Durchführung

Werkzeuge

Die Auswahl an verfügbaren Forensik-Werkzeugen ist sehr gross. Es gibt einige Portale, die die Suche nach dem richtigen Werkzeug erleichtern. So bietet das seit 2016 geführte Portal der DFIR-Community DFIR.training [2], eine herstellerunabhängige und detaillierte Suchmaske. Nutzer können die Einträge bewerten, was die Orientierung bezüglich der Qualität der Produkte erleichtert. Zudem bietet die Seite Ressourcen zum Testen von Tools sowie Kurzanleitungen und Infografiken.Eine weitere Quelle ist das Digital Forensic Portal [3] des SANS Institute. Dort ist auch eine Anleitung zu finden, wie Windows 10 zu einer forensischen Untersuchungsplattform gemacht werden kann [4].

Datenanalyse

Für die Datenanalyse ist viel Erfahrung notwendig. Es macht Sinn, dies mehrmals zu üben, bevor ein infiziertes System untersucht wird. Ansonsten könnten schnell Spuren vernichtet werden. Bei Betriebssystemen können unter anderem die folgenden Informationen weiterhelfen:

- Firewall-Logs
- System-Ereignisse
- Hardware-Informationen
- Software-Installation
- Partitionen und Ordnerstruktur
- Systemkonfigurationen
- Netzwerk-Informationen (Routing, ARP-Tabellen, MAC-Adressen, IP-Verbindungen, Freigaben)

Zusammenfassung

Wurde eine Straftat begangen ist guter Rat teuer. Ein strukturiertes Vorgehen hilft, alle notwendigen Beweise rechtssicher zu sammeln und auszuwerten. Verschiedene Werkzeuge und Dateien liefern wertvolle Informationen, die es gilt zu sichern und mit entsprechendem Wissen zu analysieren. Dies gilt auch bei einer Malware. An der richtigen Stelle gesucht, kann vielleicht sogar der Schädling unkenntlich gemacht werden und die Systeme laufen wieder wie zuvor.