ZT IT-KOLUMNE

Computer-Forensik, was ist das?

Nach einem Hackerangriff auf ein bestehendes Computersystem möchte ein Unternehmen wissen, was genau auf dem Computersystem passiert ist. Hier kann die Computer-Forensik helfen! Folgender Artikel gibt eine Einführung in dieses Fachgebiet und beschreibt, was mit Computer-Forensik möglich ist.

Was bedeutet der Begriff „Forensik“ genau?

Der Begriff „Forensik“ stammt aus dem lateinischen Wort „Forum“ (Mehrzahl: Foren). Im antiken Rom wurden Gerichtsverfahren, Urteilsverkündungen, Falluntersuchungen und zuletzt auch die Strafvollzugshandlungen in der Regel auf einem öffentlichen Marktplatz durchgeführt. In der heutigen Forensik werden Arbeitsgebiete zusammengefasst, in denen kriminelle Taten identifiziert, analysiert und rekonstruiert werden. Die Computer-Forensik beschäftigt sich dabei im Speziellen mit dem Nachweis und der Ermittlung von Straftaten in der Computerkriminalität.

Einführung in die Computer-Forensik

Zuerst soll geklärt werden, was Computer-Forensik nicht ist. Mit Computer-Forensik ist nicht, wie man schnell meinen könnte, eine digitale Unterstützung mit Computertechnologien im Rahmen einer Autopsie von ungeklärten Todesfällen gemeint. In der Computer-Forensik geht es darum, eine Autopsie von Computersystemen im Rahmen von straffälligen Handlungen an bzw. mit Computersystemen durchzuführen. Oder ganz allgemein ausgedrückt: Computer-Forensik beschäftigt sich mit der Untersuchung verdächtiger Vorfälle im Zusammenhang mit IT-Systemen. Da heutzutage Dokumente auf Computersystemen digital verarbeitet und gespeichert werden, haben sich kriminelle Straftaten im Bereich von Computersystemen stark vermehrt. Gezielte Hackerangriffe gegen Computersysteme von Unternehmen und auch Privatpersonen werden immer lohnenswerter, da immer mehr wichtige Dokumente und Geldtransfers über das Medium Internet abgewickelt werden. Man kann sich nun sehr leicht vorstellen, dass Datenverluste durch Hackerangriffe für Unternehmen und Privatpersonen sehr leicht existenzgefährdend und bedrohlich werden können.

Die Computer-Forensik interessiert sich hierbei nicht für Sicherheitslösungen von potenziell gefährdeten Computersystemen, sondern versucht, die digitalen Spuren, die Hacker hinterlassen haben, zu sichern und zu analysieren. Dafür müssen genaue Untersuchungsabläufe beachtet werden, um die Ergebnisse der Untersuchung bzw. Analyse für weitere juristische Schritte als „belastende/entlastende“ Beweismittel verwenden zu können. Die Computer-Forensik ist sozusagen eine wichtige Schnittstelle zwischen den betroffenen Unternehmen bzw. Personen und der Justiz. Für eine juristische Verwendung der Ergebnisse in der Computer-Forensik ist es sehr wichtig, die Dokumentation der einzelnen Arbeitsschritte exakt zu erstellen. Während der forensischen Ermittlung bzw. Analyse müssen folgende Fragen gestellt und beantwortet werden:

- Aus welchem Personenkreis kommt der Täter?
- Welche Ziele und Interessen hat der Täter verfolgt?
- Welche Sicherheitslücken bestehen im Computersystem?
- Auf welche Art und Weise konnte der Täter in das Computersystem eindringen?
- Welche Art der Bedrohung liegt vor?
- Welchen Schaden hat das IT-System genommen?
- Welche Auswirkungen hat die Tat auf das Computersystem und Gesamtsystem?
- Welche Gefahr besteht für die Person oder das Unternehmen?

Anhand der Fragenliste ist leicht zu erkennen, welchen Herausforderungen und Schwierigkeiten die Sicherheitsverantwortlichen der Computersysteme gegenüberstehen. Es ist schon schwierig genug, überhaupt eine Bedrohung zu erkennen, geschweige denn eine Eintrittswahrscheinlichkeit einer potenziellen Bedrohung abzuschätzen. Die Computer-Forensik muss eine Eintrittswahrscheinlichkeit abschätzen, da nur so eine Einschätzung des möglichen Schadens getätigt werden kann. Außerdem ist es eine wichtige Aufgabe, für den Fall eines Schadens einen entsprechenden „Notfallplan“ zu erarbeiten, den eine Person oder das Unternehmen sofort im eingetretenen Fall verwenden kann.

Die Eintrittswahrscheinlichkeiten einer Bedrohung des Computersystems können durch weitere Fragen und deren Antworten besser ermittelt werden:

- Wie oft wurde das Computersystem in der Vergangenheit bedroht? Hier muss mit Statistiken und Erfahrungswerten gearbeitet werden.
- Welche Motivation steckt hinter einer Bedrohung?
- Woher kommt der Täter (von außen oder von innen)?
- Welche speziellen Fachkenntnisse muss der Täter besitzen?
- Warum ist gerade dieses Computersystem bedroht worden? Welche besonderen Daten bzw. Informationen mit welchen besonderen Werten werden im System verarbeitet, die eine Attraktivität für potenzielle Angreifer darstellen?
- Wo genau steckt die Verwundbarkeit des Systems oder der Systemkomponenten?
- Wie ist das Unternehmen bzw. die Organisation oder Person überhaupt positioniert?
- Aus welcher Branche stammt das Unternehmen? usw.

Viele Fragen sind zu beantworten, um Eintrittswahrscheinlichkeiten zu ermitteln. Die Computer-Forensik muss auf den bedrohten Computersystemen u. U. umfangreiche Datenbestände (auch aus Datenbanken) auswerten, um den Schaden exakt feststellen zu können. Ohne zusätzliche, spezielle Werkzeuge für die Computer-Forensik ist eine Analyse bzw. Datenauswertung unmöglich.

Die Vorgehensweise in der Computer-Forensik

Der aufmerksame Leser stellt sich jetzt die Frage, wie und in welcher Reihenfolge geht man in der Computer-Forensik denn nun vor? Es sind Unmengen von Fragen zu beantworten, bei deren Beantwortung man schnell den Überblick verliert. Natürlich gibt es in der Computer-Forensik einen festen Prozess, in dem die einzelnen Arbeitsschritte und übergeordnete Fragen exakt festgelegt sind.

- Was ist überhaupt passiert?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Weitere wichtige Fragen sind für eine strafrechtliche Relevanz zu beantworten:

- Wer veränderte die Daten?
- Wer war anwesend und beteiligt?
- Wie kann man sich in der Zukunft vor einer möglichen Wiederholung der Straftat schützen?

Tools/Toolkits für die Computer-Forensik

Spezielle Software für die Computer-Forensik sind Anwendungen, die eine (gerichtsfeste) Erfassung und Analyse von Datenträgern ermöglichen. Zusätzliche Ansätze zur Forensik im Bereich der IT sind z. B. Code-Forensik, die für die Identifizierung und Analyse des Binärcodes von Computerprogrammen ausgelegt ist und Netzwerk-Forensik, die als Erweiterung klassischer „Intrusion Detection“ und „Intrusion Reaction“ anzusehen ist.

Ein „Intrusion Detection System“ (IDS), auch Angriffserkennungssystem genannt, hilft bei der Erkennung von Angriffen, die sich gegen einzelne Computersysteme oder ganze Rechnernetzwerke richten und ergänzt damit eine Firewall. Um die Sicherheit von anderen Netzwerken noch zu erhöhen, kann ein Angriffserkennungssystem auch direkt auf dem Computersystem laufen, das überwacht werden soll (Quelle: wikipedia.de).

Intrusion Reaction bedeutet, dass, sobald ein Angriff oder ein Einbruch durch das Intrusion Detection System erkannt und gemeldet worden ist, darauf reagiert werden muss. Die Reaktion kann ausschließlich vom Administrator ausgelöst oder durch das Intrusion Response System automatisiert werden.

Grundsätzlich können folgende passive Gegenmaßnahmen ergriffen werden:

- Neukonfiguration einer Firewall oder eines Routers, um die Angreifer-IP-Adresse abzuwehren.
- Herunterfahren von Diensten, um Ports zu schließen.
- In ganz schweren Fällen muss der Router vollständig heruntergefahren werden.

Ausblick

Da die Bedrohungslage von Computersystemen in der Zukunft weiter zunimmt, muss die Computer-Forensik auch in der Zukunft beweiskräftige Ergebnisse für die gerichtliche Verwendung erzielen. Die Arbeit wird immer komplexer werden, sodass auch die dafür notwendigen Softwareanwendungen Schritt halten müssen. Das Fachgebiet der Computer-Forensik hat sich in den letzten Jahren durch immer mehr komplexe Hackerangriffe deutlich ausgeweitet und immer mehr Bedrohungsszenarien müssen berücksichtigt werden. Die Zukunft der Computersicherheit wird immer komplexer und es bleibt zu hoffen, dass die Sicherheit der immer komplexeren Computersysteme durch professionell durchgeführte Computer-Forensik verbessert wird. ZT

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung & Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de