Computer Forensics: Die digitale Autopsie

ILLUSTRATION: CW/THÜ

Nach einem Sicherheitszwischenfall gilt es, Beweismittel zu sichern. Dabei kommt es nicht nur darauf an, Spuren zu entdecken – man muss sie auch gerichtsverwertbar sicherstellen. **VON WOLFGANG SIDLER***

Wie reagiert man am besten auf einen Sicherheitsvorfall im Computerbereich? Diese Frage stellen sich in letzter Zeit immer mehr Firmen, Organisationen und auch Privatpersonen. Ist auch nur im Entferntesten damit zu rechnen, dass der Vorfall in einem Rechtsstreit oder in einer Strafverfolgung eine Rolle spielen könnte, muss besonders überlegt gehandelt werden, um die Beweislage nicht zu verschlechtern. Leider werden dabei oft aus Unwissenheit, in guter Absicht oder auch in Panik viele Fehler gemacht, die eventuelle Spuren der kriminellen Aktionen unwiederbringlich vernichten oder ihre Verwendung in einem Gerichtsprozess verhindern.

Der Begriff Computer-Forensik oder auch Digitale Forensik hat sich in den letzten Jahren für den Nachweis und die Ermittlung von Straftaten aus dem Bereich der Computerkriminalität durchgesetzt. Viele sehen in der Computer-Forensik eine moderne Form der schwarzen Magie, die vermeintlich vernichtete Daten wieder rekonstruiert oder entschlüsselt. Informationen, von denen man gar nicht wusste, dass sie existieren, kommen plötzlich zum Vorschein und selbst gebrauchte Kopierer geben geheime Dokumente preis. Doch so erstaunlich manche Ergebnisse auch aussehen mögen – auch der beste Forensiker kann keine Daten herbeizaubern, die physikalisch nicht mehr vorhanden sind. Und noch eine kleine Warnung vorweg: Computer-Forensik erfordert einiges an Systemkenntnis und man sollte schon ganz genau wissen, was man tut. Nicht zuletzt müssen bei einer Analyse natürlich immer auch Datenschutzaspekte und Persönlichkeitsrechte berücksichtigt werden.

Die Ziele einer forensischen Analyse nach einem Hackerangriff oder Fällen von Computersabotage, Datendiebstahl, Wirtschaftsspionage oder einem anderen möglicherweise ernsthaften Sicherheitsvorfall sind in der Regel die Identifikation des Angreifers, das Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte, die Ermittlung des entstandenen Schadens nach einem Systemeinbruch sowie die Sicherung der Beweise für weitere juristische Aktionen.

Die wesentliche praktische Frage bei der Computer-Forensik lautet hierbei: Wie stellt man sicher, dass soviel gerichtsverwertbare Informationen wie möglich von einem kompromittierten System gesammelt werden können, wobei der aktuelle Zustand dieses Systems so wenig wie möglich verändert wird? Zur Beantwortung dieser scheinbar einfachen, aber in der Umsetzung recht komplexen Frage muss bei der Computer-Forensik bereits im Vorfeld geklärt werden:

- Wie wird der Angriff verifiziert?
- Wie sollen der kompromittierte Rechner und die zugehörige Umgebung gesichert werden?
- Welche Methoden können für die Sammlung von Beweisspuren verwendet werden?
- Wo sucht man nach Anhaltspunkten und wie können sie gefunden werden?
- Wie kann das Unbekannte analysiert werden?

Dies bedeutet allerdings auch, dass sich das Security-Management des Unternehmens im Vorfeld auf einen möglichen Security Incident vorbereiten muss. Hierzu zählen die Erstellung von Security-Incident-Response- beziehungsweise Notfallplänen und ein angemessenes Training der Sicherheitsspezialisten im Umgang mit Security-Tools und den Methoden zur Behandlung von Sicherheitsvorfällen. Firmen sind auch gut beraten, wenn sie mit einer auf Computer-Forensik spezialisierten Unternehmung, die auch international tätig ist bereits im Vorfeld einen Zusammenarbeitsvertrag vereinbart haben.

Das richtige Vorgehen

In einer ersten Phase gilt es, mögliche Beweismittel zu identifizieren. Aufgrund eines

* Wolfgang Sidler ist eidg. Wirtschaftsinformatiker und Mitautor des «Sicherheitshandbuches für die Praxis», www.sihb.ch.

Verdachtsmoments wird eine Untersuchung eingeleitet. Da es während einer forensischen Untersuchung möglich ist, dass spätere Phasen der Ermittlung neue Beweismittel aufdecken, sollten die ersten Schritte möglichst umfangreich sein und genau protokolliert werden. Beispielsweise sollen bei einer Hausdurchsuchung mit Beschlagnahmungen möglichst alle Datenträger mitgenommen werden, auch wenn sich einige wahrscheinlich nachher als überflüssig erweisen.

In der nächsten Phase müssen Beweise gesammelt und gesichert werden. Beweismittel sollen nach forensischen Massstäben kopiert werden. Computerforensiker machen möglichst exakte Kopien der Daten der Beweismittel, Bit für Bit und womöglich in einem einzigen Datenstrom. In der Fachsprache der IT-Welt heisst diese Art zu kopieren auch Datenspiegelung oder Klonen. Mit einem digitalen Fingerabdruck wird anschliessend geprüft, ob die Daten der Quelle mit denjenigen der Kopie übereinstimmen. Stimmen die Fingerabdrücke überein, ist Gewähr gegeben, dass der Forensiker eine identische Kopie des Originals in seinen Händen hält, die die Basis für weitere Untersuchungen darstellt.

In der dritten Phase werden die Kopien der ursprünglichen Datenträger schliesslich auf Spuren untersucht und ausgewertet. Eine Voranalyse überprüft die Vollständigkeit des Beweismaterials. Dabei müssen Arbeitskopien der zu analysierenden Daten erstellt werden und eine Zusammenstellung der vorhandenen Datenträger und deren Inhalte angefertigt werden. Bei entsprechendem Verdacht sollte ausserdem nach versteckten Aufzeichnungen gesucht werden. Diese können sich auf unbenutzten Bereichen von Backupmedien oder auf speziellen Speicherbereichen befinden. Gelöschte Daten werden soweit möglich rekonstruiert.

Die vierte Phase schliesslich umfasst die Analyse sowie die Berichterstattung. Die gefundenen Beweise werden unter Umständen während eines Gerichtsverfahrens diskutiert und ausgewertet. Die Beschreibung der Resultate, die Dokumentation und die Schritte, die unternommen wurden, um Beweismittel zu schützen und zu analysieren, können eine Ermittlung glaubwürdig oder unglaubwürdig machen. Dazu gehören unter anderem das Erstellen einer Liste von Suchwörtern und Signaturen gesuchter Muster, die Analyse der zugänglichen Bereiche bezüglich dieser Kriterien, die Suche sowie die Dokumentation von Zusammenhängen von Anomalien. Zudem ist es die Pflicht eines Computer-Forensikers, die manchmal komplexen technischen Vorgänge für nicht technisch versierte Laien verständlich und nachvollziehbar zu beschreiben.

Das richtige Werkzeug

Neben den Geheimdiensten und Strafverfolgungsbehörden, die normalerweise ihre eigene Forensik betreiben, haben vor allem Datenrettungsunternehmen die Computer-Forensik für sich entdeckt und lassen sich dabei nicht so gerne in die Karten schauen. Jedes Betriebssystem beschreibt eine Festplatte auf seine spezielle Art und verwaltet auch Files unterschiedlich. Forensische Werkzeuge müssen diesen Methoden genau folgen, um Kopien von Beweismitteln zur Analyse herzustellen und zu prüfen, was jeweils vorliegt. Auf dem internationalen Markt gibt es einige renommierte kommerzielle Hard- und Softwarepakete wie Encase, Safeback oder Smart, die oft auch im Bereich der Strafverfolgung zum Einsatz kommen.

«Die Computer-Forensik befasst sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen durch die Analyse von digitalen Spuren.»

Daneben existieren aber auch eine Vielzahl von Open-Source-Tools, die sich entweder im Computer-Forensik-Bereich einsetzen lassen oder sogar speziell dafür entwickelt wurden. Die Werkzeuge sollen folgende Kriterien erfüllen:

- Beweisbare Unveränderheit
- Preview-Möglichkeit
- Leistungsstarke Suchmöglichkeiten (Files, Bilder, Schlüsselwörter)
- E-Script-Sprache zum Programmieren von Suchsequenzen (alle Web-Adressen, spezielle Dateitypen)

Das wichtigste Hilfsmittel für eine forensische Analyse ist somit eine ausreichend grosse Festplatte, die eine Datei der Grösse der zu sichernden Festplatte aufnehmen kann. Es gibt Fälle, bei denen über ein TBbyte an Daten gesichert werden musste.

Daten sicher löschen

Beim Thema «Dateien sicher löschen» gehen die Meinungen sehr weit auseinander. So empfiehlt das BSI (Bundesamt für Sicherheit in der Informationstechnik) beispielsweise, die Daten mindestens zwei- bis dreimal mit verschiedenen Bitmustern zu überschreiben, andere gehen davon aus, dass Dateien 35-mal nach Gutman-Methode überschrieben werden müssen, um sicher gelöscht zu werden. Gemäss einer Untersuchung der Zeitschrift CT wurden Daten ein- bis dreimal überschrieben und an professionelle Datenrettungsfirmen gesendet. Bereits diejenigen Dateien, welche einmal überschrieben wurden, konnten nicht mehr wiederhergestellt werden. Anders sieht es jedoch aus, wenn Festplatten mechanisch zerstört werden sollen. Dabei können die Daten meist in Speziallabors wiederhergestellt werden.

Die richtige Vorbereitung

Wenn ein Unternehmen die Bildung eines internen Computerforensik-Teams plant oder die Personalabteilung ein solches vorschreiben will, müssen zuerst die Leute richtig ausgebildet werden, bevor die Software eingekauft wird. Doch trotz internem Team sollten die Sicherheitsdienstleister und ihre Angebote geprüft und verglichen werden.

Computer-Forensik ist auch Bestandteil der in der Schweiz anerkannten Ausbildung zum Executive Master of Information Security an der Fachhochschule in Luzern. Der neue Studienbereich Forensik und Wirtschaftskriminalistik hat die prozessuale Wahrheitsfindung in Bezug auf alle Formen der Kriminalität zum Gegenstand und richtet sich an Vertreterinnen und Vertreter von Justiz und Polizei. Die Fachhochschule Luzern betreibt ein eigenes IT-Security-Lab, das von wissenschaftlichen Mitarbeitern sowie verschiedenen Dozenten aus dem Nachdiplomstudium Informatiksicherheit betrieben wird und somit eine intensive Zusammenarbeit mit Partnern aus Wirtschaft, Industrie und Behörde fördert. Das Kernangebot besteht aus dem Nachdiplomkurs Forensik, der das praktische Grundlagenwissen der Strafverfolgung für IT-Ermittler vermittelt. Es ergänzt die Kenntnisse, welche die Studierenden im Rahmen ihres juristischen Studiums erworben haben, insbesondere in den Bereichen Kriminologie, Kriminaltaktik und -technik, Fahndung/Ermittlung, forensische Psychiatrie und Gerichtsmedizin. ■

WEITERE INFORMATIONEN

So lassen sich Spuren verhindern:

So lassen sich Spuren verhindern:

- Sichere Verschlüsselung: Wirksame Algorithmen und lange Passwörter verwenden, die gesamte Festplatte verschlüsseln
- Richtiges Löschen von Daten und temporären Verzeichnissen
- Daten auf einer Festplatte mit einem «Wipe-Tool» unwiederbringlich löschen
- E-Mail mit vertraulichem Inhalt verschlüsseln
- PDA verschlüsseln bzw. mit einem Passwortschutz versehen
- Vertrauliche Daten auf Natel, Smartphones und Blackberrys vermeiden