

Computer-Forensik – digitale IT-Spurensuche

Wolfgang Sidler

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

Wie reagiert man am besten auf einen Sicherheitsvorfall im Computerbereich? Diese Frage stellen sich in letzter Zeit immer mehr Firmen, Organisationen und Privatpersonen. Ist auch nur im Entferntesten damit zu rechnen, dass der Vorfall in einem Rechtsstreit oder einer Strafverfolgung eine Rolle spielen könnte, muss besonders überlegt gehandelt werden, um die Beweislage nicht zu verschlechtern. Leider werden 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. In Anlehnung

an die allgemeine Erklärung des lateinischen Wortes Forensik, ist die Computer-Forensik ein Teilgebiet das sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen z.B. durch Analyse von digitalen Spuren beschäftigt.

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 er-

fordert 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 ernsthaftem Sicherheitsvorfall sind in der Regel:

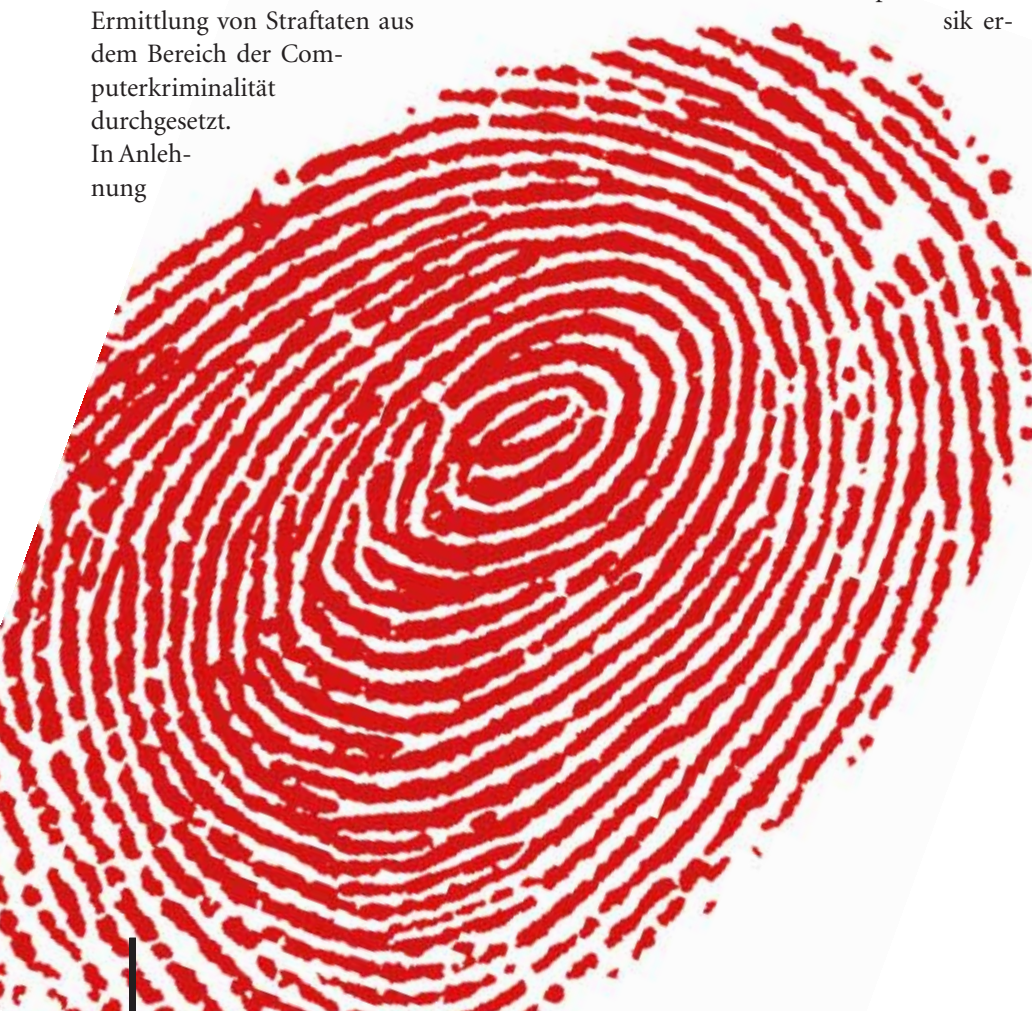
- die Identifikation des Angreifers,
- das Erkennen der Methode oder Schwachstelle, die zum Systemeintritt geführt haben könnte,
- die Ermittlung des entstandenen Schadens nach einem Systemeintritt und
- die Sicherung der Beweise für weitere juristische Aktionen
 - rechtmässige Beschaffung
 - unverändert (integer)
 - Entstehung gesichert (authentisch)

Die wesentliche praktische Frage bei der Computer-Forensik lautet hierbei:

Wie stellt man sicher, dass soviel gerichtsverwertbare Informationen (sog. Beweismittel) wie möglich von einem kompromittierten System gesammelt werden können, wobei der aktuelle Zustand bzw. Status 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 zählt die Erstellung von Security Incident Response – bzw. Notfallplänen und ein angemessenes Training der Sicherheitsspezialisten im Umgang mit Security Tools und den Methoden zur Behandlung von Sicherheitsvorfällen. Man ist gut beraten, wenn mit einer auf Computer-Forensik spezialisierten Unternehmung, welche auch international tätig ist, bereits im Vorfeld ein Zusammenarbeitsvertrag vereinbart wurde.

Die Computer-Forensik macht aus Ge löschem und Verborgenen Beweise, die vor Gericht Hand und Fuss haben. Dass das bitter nötig ist, zeigt die Kriminalität innerhalb der Informationstechnik. Zahlreiche alte und neue verbrecherische Betätigungsfelder fordern heute die Profis im Schnüffeln heraus.

Das richtige Vorgehen

Phase 1 «Identifikation möglicher Beweismittel»

Aufgrund eines 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 dieser Phase möglichst umfangreich sein und genau protokolliert werden. Beispielsweise sollen bei einer Hausdurchsuchung mit Beschlagnahmungen möglichst alle Datenträger mitgenommen werden, auch wenn sich einige nachher wahrscheinlich als überflüssig erweisen.

Phase 2 «Sammeln und Sichern von Beweisen (stark situationsbedingt)»

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, welche die Basis für weitere Untersuchungen darstellt.

Phase 3 «Aufarbeiten»

Die Kopien der ursprünglichen Datenträger werden im Anschluss auf Spuren untersucht und ausgewertet. Eine Voranalyse überprüft die Vollständigkeit des Beweismaterials.

- Arbeitskopien der zu analysierenden Daten erstellen
- Zusammenstellung der vorhandenen Datenträger und deren Inhalte (Verzeichnisse) anfertigen
- Bei Bedarf/Verdacht nach versteckten Aufzeichnungen suchen
 - unbenutzte Bereiche von Backupmedien
 - spezielle Speicherbereiche
 - «gelöschte» Daten soweit möglich rekonstruieren

Phase 4 «Analysieren und Berichten»

Die gefundenen Beweise werden unter Umständen während eines Gerichtsverfahrens diskutiert und ausgewertet. Die Beschreibung der Resultate, die Dokumentation und Schritte, die unternommen wurden um Beweismittel zu schützen und zu analysieren, können eine Ermittlung

glaubwürdig oder unglaubwürdig machen. Zudem ist es die Pflicht eines Computerforensikers, die manchmal komplexen technischen Vorgänge für nicht technisch versierte Laien verständlich und nachvollziehbar zu beschreiben.

- Erstellen einer Liste von Suchwörtern oder Signaturen gesuchter Muster (z.B. Bilder, Programme etc.)
- Analyse der zugänglichen Bereiche bezüglich dieser Kriterien
- Zusammenhänge sowie Anomalien (z.B. Filetyp/Extension) suchen und dokumentieren
- Einsatz von geeigneten Werkzeugen

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/oder Softwarepakete wie Encase, SafeBack oder SMART, die oft auch im Bereich der Strafverfolgung zum

Einsatz kommen. 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.

Daten sicher löschen

Beim Thema «Dateien sicher löschen» gehen die Meinungen sehr weit auseinander. So empfiehlt das BSI (Bundesamt für Sicherheit in der Informationstechnik) 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 eine professionelle Datenrettungsfirma 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.

Verhindern von Spuren

- Verschlüsselung: Wirksamer Algorithmus, langes Passwort, gesamte Disk verschlüsseln
- Richtig löschen (Wipe Tool): Daten, Temporär-Verzeichnis, Internet Temporär Files
- Mails mit vertraulichem Inhalt verschlüsseln
- PDA mit einem Passwort schützen
- Natel, PDA, Smartphones und Blackberry's: Keine vertraulichen Daten

Die richtige Vorbereitung und Ausbildung

Wer die Bildung eines internen Computerforensik-Teams plant oder die Personalabteilung ein solches vorschreiben will, müssen zuerst die Leute richtig ausgebildet werden, bevor man die Software einkauft. 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 Informa-

tion 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 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 I», der das praktische Grundlagenwissen und -können der Strafverfolgung für IT-Ermittler (Cyber-Cop) 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 ■