security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Computer Forensics – IT- Spurensuche, die digitale Autopsie

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

W. Sidler

CEO, VP und Berater,
Swiss IT-Markt AG

Nachdiplom FH Informatiksicherheit, eidg. Wirtschaftsinformatiker und Mitautor des «Sicherheitshandbuches für die Praxis»
www.sihb.ch

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 (engl. Computer-Forensics, Digital Forensics) 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 modere 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 anderem 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 entstanden Schadens nach

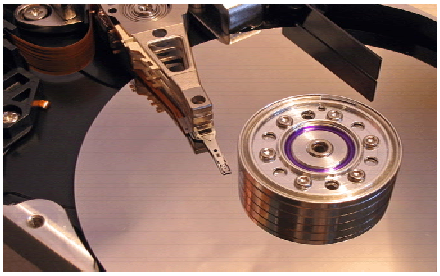
einem Systemeinbruch und

- die Sicherung der Beweise für weitere juristische Aktionen
    - o rechtmässige Beschaffung
    - o unverändert (integer)
    - o 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. Sie sind auch gut beraten, wenn Sie mit einer auf Computer-Forensik spezialisierten Unternehmung, welche auch international tätig ist bereits im Vorfeld einen Zusammenarbeitsvertrag vereinbart haben.

Die Computer-Forensik macht aus Gelöschtem und Verborgenem 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.

Die Revisoren der Firma Enron berichteten der empörten Welt, dass diese Firma eine unbestimmte Menge Daten - Dokumente genauso wie E-Mails - zerstört hätte, die sich auf den finanziellen Niedergang des Unternehmens bezogen. Andrew Rosen jedoch ist überzeugt davon, dass er trotzdem herausfindet, was passiert ist, und erfährt, wer was wann zerstört hat.
Rosen ist Präsident von ASR Data Acquisition and Analysis. Er ist einer der Schnüffler, die die Systeme des Falls durchwühlen, der eine der grössten computerforensischen Untersuchungen aller Zeiten auslöste. Jedenfalls sagen dies Beobachter. Rosen will keine Einzelheiten über seine Arbeit mit den Enron-Systemen preisgeben. "Es ist viel einfacher, die Computerforensik-Arbeiten durchzuführen, die zeigen, was gedruckt, was zerstört, was versandt und was empfangen wurde, als die Tausenden von Papierstreifen wieder zusammenzukleben, die in den Aktenvernichtern stecken."

Das FBI kündigte vor einiger Zeit die Gründung von drei neuen Computerforensik-Zentren in den USA an. Diese neue Technik der Spurensuche wird schon einiger Zeit von den Justizbehörden eingesetzt. Die Werkzeuge dafür sind in vielen grossen Unternehmen, bei Sicherheitsdienstleistern und in Spezialfirmen wie der von Rosen zum alltäglichen Arbeitsmaterial geworden. Die Wissenschaft analysiert die Bits und Bytes, welche auf einer Speicherplatte zurückbleiben, und sichert sie sorgfältig, damit man die Daten in jenem Zustand sieht, bevor sie zuletzt verändert wurden. Sie ist ein kraftvolles Werkzeug für Untersuchungsbeamte wie für interne Sicherheitsleute, die mit der Durchsetzung von Vorschriften der Computerverwendung betraut sind, das Online-Verhalten eines verärgerten Angestellten überprüfen oder die Autoren eines böswilligen Codes aufspüren müssen.

Die Hersteller solcher forensischen Werkzeuge wie Access Data, Guidance Software oder New Technologies arbeiten gemeinsam mit Entwicklern der Universitätslabors und mit Sicherheitsberatern. Diese Firmen geben den Untersuchungsbeamten überdurchschnittliche und sehr leistungsfähige Möglichkeiten, um die Gigabytes zu analysieren, die auf den Speichermedien verdächtiger Computer sitzen, was im Fall von Enron mehrheitlich Windows-Server, -PCs und -Laptops waren.

Die modernen Werkzeuge für Computer-Forensik halten mit der wachsenden Anzahl von Orten Schritt, an denen digitale Beweismittel versteckt werden.

Beispielsweise konnte damit die holländische Polizei mit Daten aus dem Navigationssystem eines Autos Informationen aus einem Handheld fischen. Dies setzt allerdings eine teure Ausbildung der Spezialisten voraus; aber nur dadurch wird die Computer-Forensik für Geschäftswelt und Justiz nutzbringend eingesetzt werden können. Ohne diese Schulung könnte es Jahre dauern, bis ein Untersuchungsbeamter den endgültigen Test besteht und als Experte vor Gericht aussagen kann.

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 wahrscheinlich nachher als überflüssig erweisen.

Phase 2: „Sammeln und Sichern von Beweisen (stark situationsbedingt)“
Beweismittel sollen nach forensischen Massstäben kopiert werden. Computer-Forensiker 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.

Am laufenden Rechner (sofern möglich):
- Systemzeit, angemeldete Benutzer dokumentieren
- Laufende Prozesse identifizieren und dokumentieren (z.B. bei einem Web-Server, Router, Firewall)
- Rechner stoppen (zur Momentaufnahme mittels Image)

Hardware-Konfiguration dokumentieren:
- Datenträger identifizieren (auf Backup-Systeme achten, Memory-Sticks, MP3 Player etc.)
- System überwachen

Bitweise Kopie des Systems (sofern möglich):
- Ohne Änderung am System (Beweisqualität)
- Digitale Signatur über Original und Kopie anfertigen unter mindestens vier Augen

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 Backup-Medien
    - 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 die Schritte, die unternommen wurden, um Beweismittel zu schützen und zu analysieren, können eine Ermittlung glaubwürdig oder unglaubwürdig machen. Zudem ist es die Pflicht eines Computer-

Forensikers, 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

Ablauf einer Ermittlung

- Eröffnen des Falls durch Sachbearbeiter der Polizei aufgrund einer Anzeige oder eines entsprechenden Hinweises
- Untersuchungsrichter (UR) ordnet 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 durch den Sachbearbeiter (IT-Ermittler)
- Einreichen das abschliessenden Berichts an UR

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 Software-Pakete 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. Die Werkzeuge sollen folgende Kriterien erfüllen:

- Beweisbare Unveränderthheit
- Preview Möglichkeit
- Leistungsstarke Suchmöglichkeiten (Files, Bilder, Schlüsselwörter)
- eScript-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, da wurde über ein Terabyte an Daten gesichert.

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 Bit-Mustern 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 ein 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.

Verhindern von Spuren

- Verschlüsselung
    - Wirksamer Algorithmus
    - Langes Passwort
    - Gesamte Disk verschlüsseln
- Richtig löschen
    - Daten
    - Temporär Verzeichnis
    - Internet Temporär Files
- Wipe Free Disk Space (regelmässig)
- Nur verschlüsselte Dokumente per E-Mail
    - Pretty Good Privacy (PGP)
    - Privat Crypto (www.utimaco.com)
- PDA verschlüsselt

- Natel, Smartphones und Blackberry's
    - Keine vertraulichen Daten

Die richtige Vorbereitung und Ausbildung

Wenn Sie die Bildung eines internen Computerforensik-Teams planen oder die Personalabteilung ein solches vorschreiben will, müssen zuerst die Leute richtig ausgebildet werden, bevor man die Software einkaufen geht. 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 an der Fachhochschule in Luzern 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, welches 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 (CyberCop) vermittelt. Es ergänzt die Kenntnisse, welche die Studierenden im Rahmen ihres juristischen Studiums erworben haben, insbesondere in den Bereichen Kriminologie, Kriminaltaktik und Ermittlung, forensische Psychiatrie und Gerichtsmedizin.