Digitale Spuren sichern und auswerten

Alltag und Arbeitsfelder der IT-Forensik

Die „dunkle Seite“ der Digitalisierung hat viele Gesichter: IT-Sicherheitsvorfälle, Schadsoftware, Hackerangriffe, Cybercrime, -war, -terrorism und einige mehr. Computerforensik ist aus dem Bestreben entstanden, Computerkriminalität – so sie denn mit adäquaten Methoden nicht zu verhindern war – wenigstens aufzuklären. Computerforensik beschäftigt sich also mit der systematischen Untersuchung krimineller Handlungen an Computersystemen oder anderen digitalen Systemen. Grundsätzlich ist Computerforensik also die Untersuchung verdächtiger Vorfälle im Zusammenhang mit IT-Systemen, die Sammlung von Beweisen und die Auswertung derselben zur Feststellung von Tatbestand, Täter und Ablauf.

Die IT-Forensik umfasst mehrere Teilbereiche. Klassischerweise unterscheidet man die reguläre Computerforensik und die forensische Datenauswertung. Erstere beschäftigt sich mit der Untersuchung von Computersystemen, seien sie mobil oder stationär, Letztere beschäftigt sich mit der Spurensuche in zumeist sehr umfangreichen Datenbeständen – E-Discovery-Prozesse bei Unternehmensfusionen oder beim Verdacht auf Wirtschaftskriminalität sind hier klassische Fälle. Im Alltag eines Unternehmens begegnet uns die normale Computerforensik in mehreren Kontexten:

1. Angriffe auf IT-Systeme sind heute alltäglich geworden, die Aufklärung derselben wird üblicherweise mit computerforensischen Mitteln durchgeführt. Die Behandlung derartiger IT-Sicherheitsvorfälle (engl. Incidents) fasst man unter den Begriff „Incident Response“. Ob diese als Teilbereich der Computerforensik gelten soll oder einen eigenständigen Zweig darstellt, der sich der Computerforensik als Werkzeug bedient, wird kontrovers diskutiert, soll hier aber nicht näher beleuchtet werden. Die juristische Verfolgung von Tätern wiederum nutzt dann Beweise, die mittels computerforensischer Methoden gesammelt wurden.

2. Doloses Verhalten, Compliance-Verstöße oder anderes Fehlverhalten von Mitarbeitern geben ebenfalls häufig Anlass zu einer computerforensischen Untersuchung. Hier sind übliche Fragestellungen, ob, wo und wie viel ein Mitarbeiter privat gesurft hat, ob ein Mitarbeiter auf fremde Nutzerkonten oder Mailboxen zugegriffen hat oder ob vertrauliche Unternehmensdaten abgeflossen sind

Grenzen der Computerforensik

Viele Firmen, die erstmals eine forensische Untersuchung in Auftrag geben, sind überrascht darüber, welche konkreten Fragen beantwortet werden können. Fernsehserien wie „Navy CIS" oder die diversen „CSI"-Variationen, die mit der Realität leider erschreckend wenig gemein haben, prägen das Bild dieser Disziplin. Leider lässt sich ein verpixeltes Digitalfoto auch mit den besten Rechnern der Welt nicht in eine hochaufl - sende 3D-Darstellung des Tatorts umwandeln, und auch das im Auge eines Fotografierten gespiegelte Buch wird normalerweise nicht lesbar zu machen sein. Auch kann (und darf) ein Forensiker sich nicht ohne Weiteres in fremde Datenbanken hacken, Handys über mehrere Kontinente hinweg verfolgen und dafür Minuten brauchen. Wenn er dagegen Zugriff auf die Protokolle der Netzbetreiber hat, reicht schon die einmalige Einwahl für eine erste Lokalisierung, der dramatisch herunterzählende Countdown und die Straße für Straße präziser werdende Ortung sind dagegen Erfindung Ein Mobiltelefon wählt sich in Netze ein, je nach Netzqualität und Bewegung sind es ein oder mehrere Netzknoten. Befindet sich nur ein Netzknoten in Reichweite des Handys, verrät der Anwender in einem langen Telefonat nicht mehr über seinen Standort als mit einer SMS.

Andererseits lässt sich auch viel mehr erfassen, als Filmemacher sich das vorstellen können. Je nach benutztem Betriebssystem, verstrichener Zeit und Arbeitsweise der Anwender können zum Teil minutiöse Protokolle der Tätigkeiten am Rechner, der aufgerufenen Programme und so weiter erstellt werden. Auch im privaten Modus aufgerufene Webseiten können unter Umständen protokolliert sein. Diese Vielzahl an Datenquellen schafft jedoch neue Probleme: Man kann einen Computerforensiker ärgern, indem man sie oder ihn ein System analysieren lässt, ohne anzugeben, was man eigentlich wissen möchte. Computerforensik muss die Flut der Daten einschränken und beherrschbar machen. Am einfachsten lässt sich dies häufig über zeitliche Faktoren realisieren („Die Datei wurde am 21.07. erstellt und war spätestens ab dem 23.07. einem Konkurrenten bekannt."), teilweise auch über die zu untersuchenden Tätigkeiten oder andere möglichst konkrete Auslöser und Fragestellungen. Solche Einschränkungen sind unverzichtbar für eine erfolgreiche und schnelle Untersuchung.

Und nicht zuletzt existieren zahlreiche Missverständnisse über die Dauer einer computerforensischen Untersuchung. Die Computerspezialistin Abby Sciuto aus „Navy CIS" lässt uns glauben, dass ein Forensiker sich das System nur zweimal anschauen braucht und die relevanten Daten dann findet Das

mag in Einzelfällen auch zutreffen – die Suche nach Standardschadsoftware etwa geht häufig so schnell –, aber spätestens dann wenn ein Fall vor Gericht landen soll, muss mit einem mehrtägigen Aufwand gerechnet werden. Der Grund hierfür ist einfach: Digitale Daten sind leicht manipulierbar. Dementsprechend muss nicht ein Hinweis auf ein Verhalten gefunden werden („Ich finde einen Eintrag für hotmail.com in der Internet Explorer History."), sondern es müssen in erster Linie alternative Erklärungsmöglichkeiten ausgeschlossen werden („Jemand bearbeitete die History-Datenbank, eine Schadsoftware hat die Seite aufgerufen, es war nur eine Werbeeinbindung …").

Was zu beweisen wäre

Die Computerforensik liefert Informationen und Beweise etwa für arbeitsrechtliche und strafrechtliche Maßnahmen, für eine Verbesserung des IT-Betriebs, aber auch für den normalen Unternehmensalltag, für die Revision und Audits. Ergebnisse entsprechender Untersuchungen werden häufig als Beweise in Prozessen verwendet oder sind sogar ausschlaggebend für die Eröffnung eines solchen. Folglich müssen digitale Beweise auch prozessrechtlichen Ansprüchen genügen. In Deutschland sind jedoch, anders als beispielsweise in den USA, die gesetzlichen Regelungen oder höchstrichterlichen Urteile zu diesem Thema noch sehr vage. Es existiert eine Reihe von Leitfäden, es gibt die polizeiliche Praxis und mehr oder weniger formalisierte Industriestandards. Diese laufen aber weitgehend auf „Dokumentation und allgemeine Akzeptanz der Methoden" heraus. Für den Praktiker hat dies zwar auch Vorteile – ein Fehler bei der Datenerfassung muss den Beweis an sich noch nicht wertlos machen –, bringt am Ende aber mehr Nachteile. Unklare Regelungen sorgen im Zweifelsfall dafür, dass man sich auf einen Maximalkompromiss der vorsichtigen Arbeitsweisen einstellen muss, um Risiken zu minimieren. Im Unternehmen müssen Vorbereitungen durchgeführt sowie Regelungen und Rahmenbedingungen geschaffen werden, die eine entsprechend saubere Arbeitsweise ermöglichen.

Die Untersuchung vorbereiten

Aber auch abgesehen von den genannten juristischen Rahmenbedingungen müssen Vorüberlegungen angestellt werden. Die Computerforensik bewegt sich in einem rechtlichen Spannungsfeld. In der Mehrzahl deutscher Unternehmen ist die private Internetnutzung zwar offiziell verboten, das Verbot wird praktisch aber selten durchgesetzt. Entsprechend beschränkt das BDSG die Sammlung und Auswertung von Daten, zugehörige Prozesse müssten eigentlich durch den Datenschutzbeauftragten des Unternehmens begutachtet werden, aber auch die Einbindung des Betriebs- oder Personalrats ist notwendig. Eine Auswertung des betrieblichen Netzwerkverkehrs kann beispielsweise zur Überwachung der Mitarbeiter eingesetzt werden, denn die Untersuchung eines PCs verrät sehr genau, wann ein Angestellter an seinem Platz saß und wie lange gegebenenfalls die Pausen waren.

Damit geklärt werden kann, was die Computerforensik zu leisten imstande ist und wo ihre Grenzen liegen, und um die rechtlichen sowie organisatorischen Rahmenbedingungen für eine Untersuchung zu schaffen, sollten Unternehmen und Behörden sich deshalb schon im Vorfeld und unabhängig von konkreten Vorfällen mit dem Thema Computerforensik auseinandersetzen. Insbesondere wenn es um die Aufarbeitung von IT-Sicherheitsvorfällen geht, kann der spätere Ablauf dieser zeitkritischen Projekte ganz erheblich beschleunigt und verbessert werden, wenn im Vorfeld die richtigen Rahmenbedingungen geschaffen werden.

Forensik der Zukunft – Zukunft der Forensik

Allein mit den Vorbereitungen ist es leider nicht getan: Die Computerforensik muss mit der rasanten Entwicklung der IT Schritt halten. Eines ist dabei sicher: Neue IT-Systeme werden die Datenflut immer nur vergrößern. Die Überwachbarkeit von Menschen wird dabei weiter zunehmen und die Möglichkeiten der Computerforensik werden immer größer. Das Abwägen zwischen der Privatsphäre der Mitarbeiter und dem Aufklärungsbedürfnis eines Unternehmens ist in diesem Kontext immer wieder neu vorzunehmen. Hier Rahmenbedingungen zu schaffen, die die Privatsphäre oder informationelle Selbstbestimmung ermöglichen, gleichzeitig aber der immer größeren Wichtigkeit von IT und der diese begleitenden neuen Bedeutung der Aufklärung von IT-Sicherheitsvorfällen Rechnung zu tragen, wird keine leichte Aufgabe werden. ■

Digitale Daten sind leicht manipulierbar. Dementsprechend geht es in der Computerforensik nicht nur darum, einen Hinweis auf ein Fehlverhalten zu finden, sondern es müssen in erster Linie alternative Erklärungsmöglichkeiten für das Verhalten ausgeschlossen werden.

SEBASTIAN NERZ,
ist Leiter der Abteilung für Computerforensik und Incident Response der SySS GmbH und hält Vorlesungen an den Hochschulen Esslingen und Albstadt-Ebingen