Sebastian Nerz

Elektronische Spurensuche mithilfe der Computerforensik

© SySS

Auch wenn das papierlose Büro noch nicht Realität ist, sind IT und Computer aus dem Unternehmensalltag nicht mehr wegzudenken. Egal ob es um E-Mails für den Kundenkontakt geht, um Buchhaltungs- oder Forschungssysteme, die steigende Anzahl der Homeoffice-Arbeitsplätze oder die in naher Zukunft alternativlose Voice-over-IP Technologie – Computer sind Teil unseres beruflichen Alltags. Die Schattenseiten dieser Entwicklung beschäftigen in jüngerer Vergangenheit die Medien: IT-Sicherheitsvorfälle, Schadsoftware, Hacks, die ständigen Debatten über Cybercrime, -war, -terrorism und Ähnliches.
Zur Verfolgung straf- und zivilrechtlicher Ansprüche hat sich die sog. Computerforensik entwickelt. Sie beschäftigt sich mit der Forensik – also 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 Auswertung derselben zur Feststellung von Tatbestand, Täter und Ablauf.

Die Arbeitsfelder der IT-Forensik

Die IT-Forensik kennt mehrere Teilbereiche: Klassischerweise unterscheidet man die reguläre Computerforensik und die forensische Datenauswertung. Erstere beschäftigt sich mit der Untersuchung von Computersystemen, seien sie mobil oder traditionell, letztere mit der Suche nach Spuren in zumeist sehr großen Datenbeständen – e-Discovery-Prozesse bei Unternehmensfusionen oder beim Verdacht auf Wirtschaftskriminalität sind hier klassische Fälle. Im Unternehmensalltag begegnet uns die normale Computerforensik an mehreren Stellen:

1. Angriffe auf IT-Systeme sind mittlerweile an der Tagesordnung, die Aufklärung derselben wird üblicherweise mit computerforensischen Mitteln durchgeführt. Die Behandlung solcher IT-Sicherheitsvorfälle (engl. Incidents) wird unter den Begriff „Incident Response“ gefasst. Ob diese als Teilbereich der Computerforensik gelten soll oder einen eigenständigen Zweig darstellt, der sich der Computerforensik als Werkzeug bedient, ist eine kontrovers diskutierte Fragestellung, die hier nicht näher beleuchtet werden soll. Die juristische Verfolgung der Täter wiederum nutzt dann Beweise, die über computerforensische Methoden ermittelt wurden.
2. Kriminelles Verhalten, Compliance-Verstöße oder anderes Fehlverhalten von Mitarbeitern sind häufig ebenfalls Gegenstand computerforensischer Untersuchungen. Die üblichen Fragestellungen lauten dann, ob, wo und wie viel ein Mitarbeiter privat gesurft, ob er auf fremde Nutzerkonten oder Mailboxen Zugriff genommen oder ob vertrauliche Unternehmensdaten gestohlen wurden.

Grenzen der Computerforensik

Für viele Unternehmen, die eine erste forensische Untersuchung durchführen lassen, ist es dabei überraschend, welche konkreten Fragen beantwortet werden können. Das Bild der Disziplin ist geprägt von Fernsehserien wie „Navy CIS“ oder den diversen CSI-Variationen (Crime Scene Investigation), die mit der Realität erschreckend wenig gemein haben. Ein verpixeltes Digitalfoto lässt sich auch mit den besten Rechnern der Welt nicht in eine hochauflösende 3D-Darstellung des Tatorts umwandeln oder das im Auge des Fotografierten gespiegelte Buch kann nicht lesbar dargestellt werden.
Auch kann (und darf) ein Forensiker sich nicht einfach in fremde Datenbanken hacken, Handys über mehrere Kontinente verfolgen und dafür nur Minuten brauchen. Hat er dagegen Zugriff auf die Protokolle der Netzbetreiber, reicht schon die einmalige Einwahl des Täters für eine erste Lokalisierung. Die laufende Stoppuhr mit der immer präziseren Ortung sind dagegen Erfindungen. Ein Handy wählt sich in Netze ein, je nach Netzqualität und Bewegung sind es ein oder mehrere Netzknoten. Hat ein Handy nur einen Netzknoten in Reichweite, verrät der Anwender in einem mehrstündigen Telefonat nicht mehr über seinen Aufenthaltsort als mit einer SMS.
Auf der anderen Seite kann viel mehr erfasst werden als Hollywood sich das vorstellt. Je nach Betriebssystem, verstrichener Zeit und Arbeitsweise der Anwender können z. T. minutiöse Protokolle der Tätigkeiten am PC, der aufgerufenen Programme uvm. erstellt werden. Auch im privaten Modus angesurfte Webseiten können u. U. protokolliert sein. Diese Vielzahl an Datenquellen schafft aber auch neue Probleme. Lautet der Auftrag an den Computerforensiker ein System zu analysieren, sollte er oder sie auch wissen, wonach genau gesucht wird. Die Computerforensik muss die Datenflut einschränken und beherrschbar machen. Am einfachsten geht dies häufig über zeitliche Faktoren („Das Dokument wurde am 21. Juli erstellt und war spätestens ab dem 23. Juli einem Konkurrenten bekannt“), teilweise auch über die zu untersuchenden Tätigkeiten oder andere möglichst konkrete Auslöser und Fragestellungen. Solche Einschränkungen sind essenziell für eine erfolgreiche und schnelle Untersuchung.
Nicht zuletzt gibt es viele Missverständnisse über die Dauer einer computerforensischen Untersuchung. Die Computerspezialistin *Abby Sciuto* aus der bereits genannten Fernsehserie Navy CIS lässt uns glauben, dass ein Forensiker sich das System nur zweimal anschauen muss und dann die relevanten Daten findet. Das mag in einzelnen Fällen auch zutreffen – die Suche nach Standardschadsoftware geht beispielsweise häufig so schnell –, aber spätestens wenn ein Fall vor Gericht gebracht werden soll, ist mit einem zeitlichen Aufwand im Rahmen von Tagen zu rechnen. Der Grund hierfür ist ganz einfach: Digitale Daten sind einfach manipulierbar. Entsprechend muss nicht *ein* Hinweis auf ein Verhalten ge-

funden werden („Ich finde einen Eintrag für hotmail.com in der Internet Explorer History"), sondern es müssen vor allem alternative Möglichkeiten ausgeschlossen werden („Jemand bearbeitete die History-Datenbank, eine Schadsoftware hat die Seite aufgerufen, es war nur eine Werbeeinbindung, …").

Digitale Beweise für Verfahren und Prozesse

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

Vorbereitung auf Forensik

Die Computerforensik bewegt sich in einem rechtlichen Spannungsfeld. In den

www.fotolia.com © pn_photo

Digitale Beweise: Nur eine exakte und saubere Arbeitsweise ermöglicht die Durchsetzung rechtlicher Ansprüche.

meisten deutschen Unternehmen ist die private Internetnutzung beispielsweise zwar offiziell verboten, praktisch wird das Verbot aber selten durchgesetzt. Entsprechend beschränkt das Bundesdatenschutzgesetz die Sammlung und Auswertung von Daten. Die zugehörigen Prozesse müssten zudem eigentlich durch den Datenschutzbeauftragten des Unternehmens begutachtet werden. Aber auch die Einbindung des Betriebs- oder Personalrats ist wichtig. Eine Auswertung des Netzwerkverkehrs in einem Unternehmen kann beispielsweise zur Mitarbeiterüberwachung eingesetzt werden, denn die Untersuchung eines PCs verrät sehr genau, wann ein Mitarbeiter an seinem Platz saß und wie lange gegebenenfalls die Pausen waren.
Um zu klären, was die Computerforensik kann und wo ihre Grenzen sind und um die rechtlichen und organisatorischen Rahmenbedingungen für eine Untersuchung aufzubauen, sollten sich daher Unternehmen und Behörden schon im Vorfeld und unabhängig von konkreten Anlässen mit Computerforensik beschäftigen. Gerade wenn es um die Aufarbeitung von IT-Sicherheitsvorfällen geht, kann der spätere Ablauf dieser zeitkritischen Projekte ganz erheblich beschleunigt und verbessert werden, soweit die Rahmenbedingungen im Vorfeld geschaffen wurden.

Blick in die Zukunft

Mit der Vorbereitung allein ist es aber nicht getan: Die Computerforensik muss mit der schnellen Entwicklung der IT Schritt halten. Eines ist dabei sicher: Neue IT-Systeme werden die Datenflut immer weiter vergrößern. Die Überwachbarkeit von Menschen wird dabei zunehmen, die Möglichkeiten der Computerforensik immer größer werden. Die Abwägung zwischen der Privatsphäre von Mitarbeitern und dem Aufklärungsbedürfnis des Unternehmens muss immer wieder neu stattfinden. Hier Rahmenbedingungen zu schaffen, die Privatsphäre oder informationelle Selbstbestimmung ermöglichen, gleichzeitig aber der wachsenden Bedeutung der IT und der damit einhergehenden neuen Bedeutung der Aufklärung von IT-Sicherheitsvorfällen Rechnung tragen, wird die Herausforderung der Zukunft.

Sebastian Nerz, Tübingen
sebastian.nerz@syss.de
www.syss.de

INFORMATIONEN ZUM AUTOR

Sebastian Nerz ist studierter Bioinformatiker. Er leitet die Abteilung für Computerforensik und Incident Response bei der SySS GmbH, Tübingen, und ist Dozent an den Hochschulen Esslingen und Albstadt-Sigmaringen.