Digitaldetektive

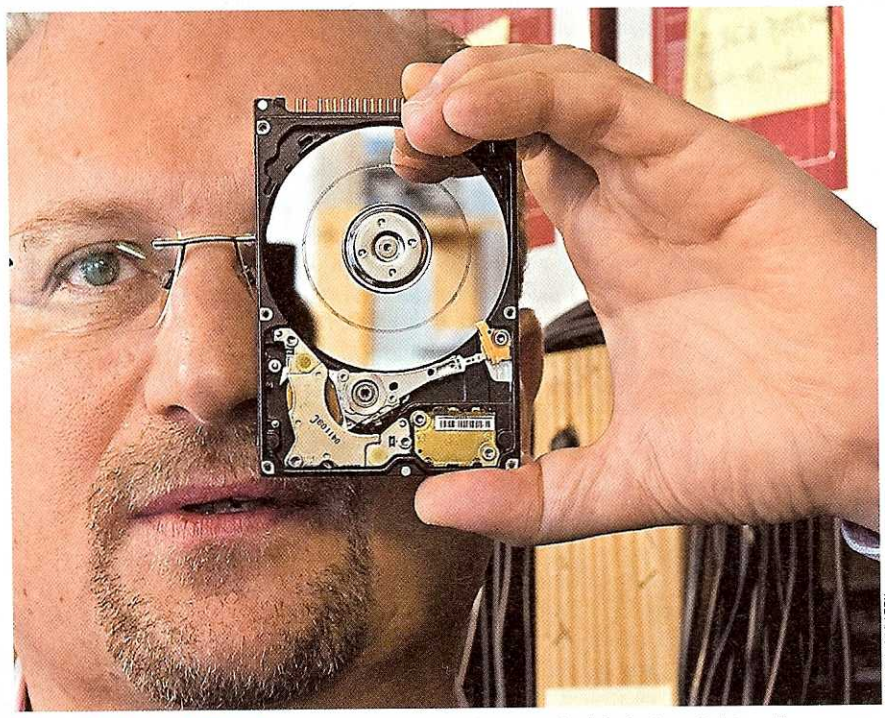
Hightech. Bei Computerkriminalität wie im Fall der Steuersünder-CD werden spezielle Forensiker konsultiert: Sie entlocken Datenträgern selbst gelöscht oder zerstört geglaubte Informationen.

Von Alfred Bankhamer

Eine kleine silberne Scheibe sorgte jüngst für reichlich Aufsehen: Der deutsche Staat gab bekannt, einem Datendieb um 2,5 Millionen Euro die heiß debattierte Schweizer „Steuerflüchtlings-CD" abkaufen zu wollen. Der Datenträger macht wohl nicht nur Steuersünder und Bankmanager nervös, sondern auch viele Unternehmer: Denn der Fall erinnert daran, wie leicht kritische Daten den Weg aus dem eigenen Unternehmen finden können.

Längst ist um die in Bits und Bytes gespeicherten Informationen über Kunden, Märkte, Produkte und Forschungsergebnisse eine milliardenschwere Industrie entstanden. Ein sehr spezieller Zweig dabei ist die Branche der Datenretter und Computerforensiker. Ihr Job, sehr grob umrissen: Sie sollen Datenträgern Infos entlocken, die für den Laien nicht oder nicht mehr zugänglich sind. Im banalsten und zugleich häufigsten Fall geht es dabei um unabsichtlich gelöschte Dateien oder zerstörte Datenträger. In Österreich bieten immerhin acht Unternehmen solche Datenrettung an. Einige davon arbeiten auch als Computerforensiker, um zur Beweissicherung Computer und Datenträger nach verdächtigen Spuren zu durchforsten.

Komplexer wird die Sachlage, wenn es um Delikte wie Datendiebstahl geht – technische Schutzvorkehrungen wie Firewalls helfen da kaum, da in den meisten Fällen der Feind im eigenen Haus sitzt. „Besonders Mitarbeiter im mittleren bis oberen Management, die keinen Aufstiegsweg mehr sehen, gelten als Risiko", weiß der Linzer Datenforensiker Uwe Sailer. Entweder wollen sie dem Unternehmen schaden – etwa durch Zerstörung des Firmennotebooks mit wichtigen Kundendaten – oder schlicht abzocken. „Es ist ja auch verlockend, wenn man sieht, dass man mit Datendiebstahl relativ leicht 2,5 Millionen Euro verdienen kann", sagt der Computerforensiker Markus Joham, Inhaber des Grazer Unternehmens Eticon Datenrettung & Forensik.



WALTER WOBRAZEK

Datenretter Friedrich Wawrik „Auf Speichermedien gibt es auch nicht lesbare Sektoren"

Genaue Kriminalstatistiken zu Datendelikten gibt es nicht. „Bei unternehmensinternen Straftaten kommen generell weniger als 20 Prozent aller Delikte zur Anzeige", schätzt Reinhold Kern, Leiter der deutschen Abteilung für Computerforensik des weltweit größten Datenrettungsspezialisten Kroll Ontrack. Meist regeln Unternehmen solche Vorfälle lieber intern ohne Einsatz von Polizei und Gericht. Der Imageschaden für das Unternehmen könnte letztlich höher sein als der finanzielle Schaden, der durch den Datenverlust entsteht.

Welche Informationen die Steuer-CD zusätzlich zu den Namen der Finanzsünder noch bergen könnte, ist bisher weitgehend unklar – Kenner der Materie meinen, dass vor allem Hinweise auf die Identität des Datendiebs darauf versteckt sein könnten, die Spezialisten auswerten könnten. Kroll-Experte Kern will freilich nicht einmal verraten, ob der Auftrag zur weiteren Analyse der CD tatsächlich bei seinem Unternehmen gelandet ist. Prädestiniert wäre die Firma dafür auf jeden Fall – immerhin erhalten die Computerprofis im Regelfall die ganz heiklen Aufträge. So war Kroll beispielsweise mit der Rettung von Forschungsdaten aus dem 2003 abgestürzten Spaceshuttle betraut.

Rein hypothetisch, so Kern, gäbe es verschiedene Möglichkeiten, die Steuer-CD nach verräterischen Spuren des Täters zu durchforsten. So protokollieren üblicherweise „Logfiles" von Datenbanken, wer wann mit welchem Gerät auf welche Daten zugegriffen hat. Man könnte auch infrage kommende PCs direkt untersuchen. Bei jedem Vorgang werden normalerweise Spuren in meist versteckten Dateien des Betriebssystems hinterlassen. „Ich gehe davon aus, dass spätestens bei der Übergabe der Täter bekannt sein wird, zumindest den Behörden", glaubt Kern.

Forensik-Tools. Die Methode der Datenexperten ist aber auch in weniger spektakulären Fällen meist ähnlich. „Bei der Datenforensik muss der Datenträger zuerst forensisch korrekt gesichert werden", erklärt Gerichtsgutachter Sailer. Es dürfen absolut keine Veränderungen erfolgen, damit die Daten vor Gericht verwendet werden können. Zur digitalen Spurensuche dienen forensische Software-Tools.

„Ins Wasser schmeißen oder mit dem Hammer draufschlagen hilft normalerweise nicht, um Daten zu zerstören"
Markus Joham, Eticon Datenrettung & Forensik

„Auf Speichermedien gibt es nicht lesbare Sektoren, die für den Betrieb und die Fehlerkorrektur dienen", erklärt der Datenrettungspionier Friedrich Wawrik, der mit seinem Unternehmen Computer Repairs in Wien schon 1988 riesige Festplatten reparierte und sehr früh einen der wenigen Reinräume zur Festplattenreparatur in Österreich einrichtete.

Daten werden auf Festplatten grundsätzlich nicht gelöscht, sondern nur überschrieben. Und da sich das Betriebssystem beim Speichervorgang auf der Scheibe beliebig freie Sektoren sucht, bleiben immer Reste der alten Datei übrig. Leichte Spurverschiebung hinterlassen weitere Datenfragmente, die nur mit hohem Aufwand auffindbar sind.

Die häufigsten Hardware-Probleme bei Festplatten sind zerstörte Elektronik, kaputte Schreib-Lese-Köpfe und steckende Motoren. Die Datenrettung basiert meist schlicht auf Ersatzteiltausch, wobei die Ersatzteile genau zur jeweiligen Festplatte passen müssen. Die Datenretter horten tausende Festplatten als Ersatzteillager. „Einfach nur die Datenscheibe ausbauen funktioniert im Regelfall nicht", erklärt Wawrik. Denn die Justagen müssen extrem genau abgestimmt sein, damit die Datenspuren auf der Magnetscheibe wieder gefunden werden können.

Selbst wenn zwecks Beweismaterialvernichtung gleich der Computer samt Festplatte zerstört wurde, ist nicht alle Mühe vergebens. Hard Disc Drives sind oft unterschätzte Hochtechnologieprodukte, die einiges aushalten. So konnte Wawrik schon eine durch einen Tunnelbrand total verkohlte Platte sowie eine Festplatte mit Hundebissspuren in seinem Labor retten. Markus Joham von Eticon rettete nach zwei Tagen Behandlung eine Festplatte einer Serveranlage, die beim Hochwasser 2009 im Burgenland in einem Firmengebäude mehrere Tage unter Wasser gestanden war. Kroll Ontrack barg unter anderem die Daten einer Festplatte, die sechs Monate auf dem Ozeangrund in 600 Meter Tiefe in einem Wrack gelegen hatte, und schaffte es, möglicherweise belastendes Material aus einem völlig zertrümmerten Notebook zu holen, das aus dem Fenster eines Luxusappartements im zwölften Stock geworfen worden war.

Wer also seine digitalen Spuren zuverlässig beseitigen will, muss sich mehr einfallen lassen als rohe Gewalt. Joham: „Ins Wasser schmeißen oder mit dem Hammer draufschlagen hilft normalerweise nicht, um Daten zu zerstören." ■