

## Digitale Spurensicherung gegen Wirtschaftskriminelle

von Jürgen Höfling

**Durch Unterschlagung und Veruntreuung gehen den Unternehmen ungeheure Summen verloren, die teilweise die Firmensubstanz tangieren können. Gefragt sind deshalb sowohl präventive als auch reaktive Abwehrmaßnahmen.**

Datenrettung per Elektronenmikroskop: zu sehen sind einzelne Servertracks und beschädigte Stellen der Datenstruktur. Die großen Fische der Wirtschaftskriminalität schlüpfen nicht durch eine löchrige Firewall ins Unternehmen, sondern sind immer schon da. Fünf bis sechs Prozent des Umsatzes geht den Unternehmen weltweit durch Finanzbetrug verloren, signalisiert eine einschlägige Studie von Ernst & Young. 85 Prozent der Täter kommen dabei aus dem jeweiligen Unternehmen, 55 Prozent stammen aus der oberen Führungsriege. Die Globalisierung frisst sozusagen ihre Kinder. »Mit der Globalisierung werden industrielle Praktiken und kulturelle Normen aufgeweicht. Die Einführung neuer Techniken erzeugt Umbrüche und dadurch innere Spannungen«, versucht Karsten Fuser, Leiter des Bereichs Advisory Services/ Global Financial Services bei Ernst & Young eine erste Analyse der desolaten Situation und er nennt weitere Gründe: »Durch die weitgehende Autonomisierung von Unternehmensbereichen und Arbeitskräften geht auch mental der Zusammenhalt verloren. Firmenauf- und -verkäufe verschärfen noch einmal das interne Klima und senken zusätzlich die Hemmschwelle für Finanzbetrügereien«. Nur 20 Prozent der Verluste werden laut den Erkenntnissen von Ernst & Young aufgedeckt, weiteren 19 Prozent kommen die Versicherungen auf die Spur. Für Ernst & Young-Berater Fuser liegt es im vitalen Geschäftsinteresse der Unternehmen, die kriminellen Energien der eigenen Mitarbeiter in den Griff zu bekommen. Letztlich helfen dabei nur »stärkere Kontrollen und Geschäftsprozesse, die so gestaltet sind, dass sich Finanzmanipulationen schneller aufdecken lassen«. Darüber hinaus sollten ein Ethik-Kodex etabliert und »Mitarbeiter, die Betrugsfälle aufdecken, nicht als Nestbeschmutzer diffamiert werden«.

### *Acht Milliarden Euro Schaden*

Auch Christian Parsow, Berater beim Beratungsunternehmen Deloitte, plädiert für eine Intensivierung der Maßnahmen für Betrugsprävention in den Unternehmen. Er zitiert Zahlen des deutschen Bundeskriminalamts, nach denen sich im Jahr 2005 der durch Finanzbetrug in den Unternehmen angerichtete Schaden auf 4,2 Milliarden Euro belaufen hat. Die Dunkelziffer, so Parsow weiter, bewege sich nach Schätzungen vieler Experten noch einmal bei demselben Wert, sodass von rund acht Milliarden Euro Schaden allein in Deutschland auszugehen sei. Parsow schlägt als eine der Präventivmaßnahmen die durchgängige Nutzung der digitalen Signatur in den Unternehmen vor sowie zusätzlich digitale Zeitstempel-Verfahren, auf deren Basis sich zeitliche Manipulationen besser nachweisen lassen. Die Installation von Prozessen für den Ernstfall ist die erste Voraussetzung für eine Spurensicherung, die nicht im Sande verläuft. »Wenn ein Unternehmen zum Beispiel keine vollständigen Sicherungskopien für die vergangenen Jahre vorhält, dann ist es praktisch unmöglich, bei Betrugsfällen digitale Daten sicherzustellen, die vor Gericht Bestand haben«, sagt Oliver Salzmann, IT-Forensik-Experte bei Deloitte. Die technischen Möglichkeiten für rechtssichere und gerichtsfeste digitale Spurensicherung seien heute vorhanden, man müsse sie nur nutzen und gleichzeitig vermeiden, durch unprofessionelles



cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)

Vorgehen, beispielsweise Maßnahmen an den Originaldaten, Beweismaterial zu zerstören.

#### *Großes Angebot an Forensik-Software*

Beweissicherung ist das A und O der IT-Forensik. »Es ist wichtig, dass die technische Untersuchung sorgfältig und konsistent durchgeführt wird. Man weiß ja im Voraus nicht, ob ein trivialer Verstoß gegen E-Mail-Richtlinien sich nicht später als symptomatisch für ein schweres Betrugsdelikt herausstellt«, meint Andreas Bröhl, Leiter Systems Security Services bei Integralis. Für die Beweissicherung auf Rechnersystemen gibt es verschiedene Software-Werkzeuge. Diese erstellen in erster Linie Sektor-Abbilder der Festplatte (»Images«). Bei Strafverfahren werden in der Regel zwei Images erstellt, eines zur eigentlichen Analyse, das andere wird versiegelt und gesichert als Masterkopie hinterlegt. Gängige Software zur Erstellung von Images und zur Speicheranalyse sind Programmpakete wie EnCase, FTK, Paraben, I-Ways oder auch das quelloffene Tool Knoppix STD (Security Tool Distribution). Die sogenannte Helix-CD ([www.e-fense.com/helix](http://www.e-fense.com/helix)) ist eine an forensische Notwendigkeiten angepasste Distribution von Knoppix.

#### *Live-Analyse oft unverzichtbar*

Dass sich in Unternehmen Fragen der IT-Forensik oft anders stellen als bei Staatsanwaltschaft und Polizei, darauf weist Stefan Strobel von cirosec hin. Während erstere im Zweifelsfall Festplatten beschlagnahmen könnten, möchte man im Unternehmen möglichst wenig Störung des Normalbetriebs verursachen. Anstelle der Festplatten-analyse hätten deshalb Methoden der Live-Analyse am laufenden System einen viel höheren Stellenwert. Auch seien im Unternehmen bisher etablierte Methoden der IT-Forensik oft nicht anwendbar oder nicht hilfreich. Wichtige Server könnten nicht auf Verdacht heruntergefahren werden und die Server-Festplatten seien oft zu groß, um sie Block für Block analysieren zu können. Zudem gebe es moderne Angriffsmethoden, die man auf Datenträgern gar nicht mehr nachweisen könne. In all diesen Fällen sei die Analyse flüchtiger Daten des laufenden Systems eine sehr wichtige Methode. Um diese Daten zu sammeln, gebe es zwei Wege. Entweder man installiere auf allen wichtigen Systemen im Vorfeld Agentenprogramme, die bei Bedarf aktiv werden, oder man erstelle im Vorfeld eine Sammlung an Programmen, mit denen man dann manuell die Daten sammeln könne. Auch bei der Sammlung von persistenten Daten ist im Vorfeld zu prüfen, ob die Sammlung bei laufendem Betrieb oder im ausgeschalteten Zustand durchgeführt werden sollte, sagt Strobel. Schließlich gebe es im Datenträgerbereich einige Informationen, die bei einem Neustart des Systems unwiederbringlich gelöscht würden (virtuelle Dateisysteme) oder die keine sinnvolle Analyse erlaubten (verschlüsselte Dateisysteme oder Container).

#### *Vieles ist rekonstruierbar*

Dass selbst Informationen in Dateien, die unwiederbringlich gelöscht zu sein scheinen, wiederhergestellt werden können, macht Reinhold Kern, Forensik-Experte bei Kroll Ontrack, deutlich. »Ein verbranntes Notebook oder zerschnittene Sicherungsbänder machen diese Datenträger oft nur scheinbar unbrauchbar. Selbst bei Speichermedien, die durch Head Crashes oder durch Brand und Wasser physikalisch beschädigt worden sind, lassen sich meist Daten wiederherstellen«, weiß Kern. Lediglich eine Zerstörung der Trägermagnetschicht mache die Datenwiederherstellung endgültig unmöglich. Selbst angeschlossene externe Datenspeicher wie Festplatten, USB-Stifte oder PDAs lassen sich nachweisen. Bei CDs oder DVDs kann festgestellt werden, mit welchen CD- oder DVD-Brennern

diese beschrieben wurden. Ebenso gibt es Mittel und Wege, um Mobiltelefone oder PDAs zu analysieren. Sogar in Speichern moderner Kopierer und Faxgeräte finden sich Spuren durchgeführter Aufträge. Oft muss aber auch das bei den meisten Unternehmen immer noch große Papierarchiv für die Spurensuche eingesetzt werden. Die Papierdokumente werden eingescannt, mit verschiedenen Suchkriterien versehen und in eine Datenbank eingestellt. Auf die dabei entstandenen einheitlichen Datensätze kann dann mit entsprechenden Analysewerkzeugen zugegriffen werden.

#### *Rechtliche Absicherung*

Technische Maßnahmen gibt es also viele. Der Bedarf an Spurensicherung ist auch da, wenn man die Deliktzahlen sieht, die Strafverfolgungsbehörden und anonyme Firmenbefragungen unisono liefern. Gleichwohl müssen die technischen Fahnder ebenso wie die staatsanwaltschaftlichen Ermittler sich an rechtliche Regeln halten. Die Datenschutzgesetzgebung ist eine dieser Vorgaben. Diese kann zum Beispiel dann unangenehm greifen, wenn innerbetrieblich die private E-Mail- und Internetnutzung nicht oder rechtlich unzureichend geklärt ist. Für Dienstleister im IT-Forensik-Bereich wird es vor Aufnahme ihrer Fahndungsarbeit deshalb die oberste Maxime sein, sich rechtlich abzusichern, das heißt, sich mit Brief und Siegel von Seiten der Geschäftsleitung des beauftragenden Unternehmens bestätigen zu lassen, dass die Fahndungsarbeit rechtmäßig ist.

***Informationweek.de 09.03.07***