

Computer Forensik Szenarien

1. Analyse digitaler Daten im Prozessfall

Die Analyse elektronischer Unternehmensdaten (Electronic Discovery) im Prozessfall gewinnt an Bedeutung. Insbesondere in den Vereinigten Staaten werden bei zivilrechtlichen Prozessen Unternehmen immer mehr dazu verpflichtet, Beweismaterialien für Ermittlungen bereitzuhalten. Eine entsprechende Anfrage kann ein Unternehmen schnell in Erklärungsnot bringen. Aktuell sucht zum Beispiel Intel im Rahmen des Antitrust-Verfahrens gegen AMD verzweifelt nach den Mailboxen von Konzernchef Paul Otellini, dem aktuellen Aufsichtsratsvorsitzenden Craig Barrett sowie dem Vertriebs- und Marketing-Chef Sean Maloney. Diese Entwicklung in Übersee hat auch für europäische Unternehmen, die an einer US-amerikanischen Börse gelistet sind oder Tochterniederlassungen in den USA betreiben, drastische Auswirkungen. In Deutschland selbst hat das Thema Electronic Discovery noch nicht den Stellenwert erreicht wie in der US-amerikanischen Rechtspraxis, jedoch wird auch den Richtern und Staatsanwälten die Bedeutung elektronischer Daten zur Aufklärung von Tatbeständen immer bewusster. So ist es absehbar, dass sich diese Art der Beweiserhebung früher oder später auch in Deutschland und in den anderen europäischen Ländern durchsetzen wird.

In den letzten Jahren hat sich die Vorgehensweise bei Zivilprozessen, den *civil litigations*, in den USA dramatisch verändert. Die *pretrial discovery* ist eine besondere Komponente des US-amerikanischen Prozessrechts, nach dem die potenziellen Parteien eines Zivilprozesses unabhängig von der Beweislastverteilung verpflichtet sind, eventuell prozessrelevantes Material zu offenbaren und dem Gegner zugänglich zu machen. In einem Fall musste die Consulting-Firma Morgan Stanley gegen den Ankläger Ron Perelman eine empfindliche Niederlage hinnehmen. Die Richterin wollte bankinterne Dokumente und insbesondere E-Mails einsehen. Morton Stanley verwies vergeblich darauf, dass eine solche Recherche zu teuer sei. Tatsächlich hatte man aber bewusst E-Mails gelöscht. Diese Unterschlagung von Beweismaterial führte sicher auch zur Prozessniederlage und zu einer Geldstrafe in Höhe von 600 Millionen US-Dollar.

Damoklesschwert für Unternehmen

Solche Vorgehensweisen werden aktuell schon von europäischen Unternehmen, die in den USA tätig sind, gefürchtet. Seit Dezember 2006 hat sich die Situation zusätzlich noch verschärft. Bislang mussten sich Anwälte hauptsächlich durch eine Vielzahl von Aktenordnern durcharbeiten, um an die erhofften Beweise zu gelangen. Waren somit früher hauptsächlich Dokumente in Schriftform betroffen, rücken mit der Digitalisierung der Geschäftsprozesse die elektronisch vorgehaltenen Daten immer mehr in den Mittelpunkt des Interesses. Mehr als 90 Prozent aller geschäftlichen Dokumente werden heutzutage elektronisch erstellt, aber weniger als 30 Prozent davon werden jemals ausgedruckt oder gar archiviert. Meeting-Protokolle, Businesspläne, Entwicklungsunterlagen, Patentschriften, Strategiepapiere, Kundendatenbanken, Wirtschaftswarensysteme und nicht zu vergessen die

Unmengen an E-Mails liegen oftmals nur in elektronischer Form vor und werden nicht einheitlich archiviert.

Sollte bei einem Unternehmen auch nur die leiseste Ahnung eines drohenden Prozesses in den USA bestehen, empfiehlt es sich sofort zu reagieren. Dies bedeutet, dass zunächst grundlegende unternehmensweite Maßnahmen getroffen werden müssen. So gilt es sicherzustellen, dass ab sofort keine geschäftsrelevanten Dokumente, einschließlich E-Mail verändert oder gar gelöscht werden. Ebenso sind Regelungen für Aufbewahrungsfristen von geschäftlichen Dokumenten – auch E-Mails – zu prüfen und einzuhalten.

Infolge der Aufforderung zur Durchführung einer Datenanalyse drohen drastische Sanktionen, wenn das betroffene Unternehmen die erwünschten Daten und Dokumente nicht zur Verfügung stellen will oder kann. Gleiches gilt für den Fall, dass Daten wissentlich oder unwissentlich verändert oder vernichtet wurden.

2. Bestatter – Computer Forensik im Insolvenzfall

Betrug, Untreue und persönliche Bereicherung sind klassische wirtschaftskriminelle Delikte. Undurchsichtige Vermögensverschiebungen und bilanztechnische Manipulationen kommen in der internationalen Wirtschaftswelt ebenfalls immer wieder ans Tageslicht. So gibt es etwa börsennotierte Unternehmen, die künstlich aufgebläht und hoffnungslos überschuldet sind. Droht dann Insolvenz, was auch die Folge schlechten Wirtschaftens sein kann, werden oft Vermögenswerte verschoben, um sie aus der Konkursmasse zu retten. Der taiwanische Elektronikkonzern BenQ soll vor der Insolvenz seiner deutschen Mobilfunk-Tochter rund eine halbe Milliarde Euro aus dem Unternehmen abgezogen haben. Eine derartige Verschiebung von Vermögenswerten liegt vor, wenn Unternehmer Teile des Vermögens, die im Falle der Eröffnung eines Insolvenzverfahrens zur Masse gehören würden, dem Zugriff der Gläubiger entziehen oder diesen Zugriff wesentlich erschweren. Ebenfalls eine Form von Wirtschaftsdelikten ist die gezielte Übernahme konkursgeschwächter Unternehmen. Dabei werden die Filetstücke ausgegliedert und die Vermögenswerte aus dem restlichen Unternehmen verkauft.

Auf dieses „Geschäftsmodell“ haben sich sogenannte „Unternehmensbestatter“ spezialisiert. Diese gehen in der Regel nach folgendem Schema vor: Eine marode Firma wird für einen

symbolischen oder sehr geringen Betrag erworben. Der alte Geschäftsführer wird ersetzt durch einen Strohmännchen, möglichst unauffällig und ohne Schufa-Eintrag. Geschäftsführer, Firmensitz und Firmenname werden dann mehrmals gewechselt, um Gläubiger abzuschütteln und für mögliche Ermittler die Spur zu verwischen. Wichtige Geschäftsunterlagen verschwinden dabei meist auf unerklärliche Weise.

Ziel dieser unlauteren Übernahmeaktivitäten ist es, entweder das Unternehmen von der Bildfläche verschwinden zu lassen oder Vermögenswerte beiseite zu schaffen sowie Kundenstamm und Aufträge auf eine neue Firma zu übertragen. Oft werden auch auf den Namen der mittellosen Firma Büroausstattung, Firmenwagen und anderes erworben oder geleast. Nachdem die Firma pleite ist und aus dem Handelsregister gelöscht wurde, müssen die Gläubiger zusehen, wie sie an ihr Geld oder die Sachen kommen. Hier kommen die Ermittler ins Spiel – und diese setzen vermehrt auf digitale Spuren, welche es auch in einem solchen Fall immer gibt.

3. Anlagebetrug

Fälle von Wirtschaftskriminalität wie das folgende Beispiel kommen immer wieder ans Tageslicht: Ein Finanzmakler lockt viele Kleinanleger mit hochprozentigen Renditen. Nach einiger Zeit meldet der Anlageberater Insolvenz an. Eine erste Prüfung ergibt, dass die „angelegten“ Gelder nicht mehr vorhanden und auch nicht auffindbar sind. Die Kleinanleger haben, zusammen genommen, mehrere Millionen Euro verloren. Was nun?

Für die eingeschalteten Strafverfolgungsbehörden ist in einem solchen Fall die oberste Priorität die Ermittlung und Sanktionierung des Täters. Bis zu einem gewissen Grad bemühen sich die Behörden auch darum, dass die betrogenen Anleger wieder an ihr Geld gelangen. Aussichtsreicher für die geschädigten Kleinanleger ist es jedoch, zusätzlich einen Rechtsanwalt einzuschalten. Nach einer Begutachtung des Falls stellt der beauftragte Jurist die Vermutung an, dass der Finanzberater, mittlerweile in Untersuchungshaft sitzend, seine „Schäfchen“ noch rechtzeitig ins Trockene gebracht hat – also Vermögenswerte verschoben hat. Die Herausforderung besteht nun darin, dies auch nachzuweisen und den Weg des Geldes zu rekonstruieren.

In den im Büro des Anlageberaters beschlagnahmten Papierdokumenten und Aktenordnern fanden sich keinerlei Hinweise weder auf spezielle Bankverbindungen noch auf Immobilien oder Grundstückskäufe, die eventuell im Ausland stattgefunden haben könnten.

Im Beispielfall brachte die Analyse der auf dem PC vorhandenen Daten sehr wertvolle Hinweise auf Beziehungen mit sowohl ausländischen Banken als auch ausländischen Immobilienmaklern zu Tage. Nützlich erwiesen sich dabei die Internet-Protokolldateien. Ebenso fanden die Computer-Forensik-Spezialisten Kaufvertragsunterlagen, die zwar gelöscht waren aber wieder hergestellt werden konnten. Unter anderem konnten Verhandlungen über den Erwerb einer Villa in Florida zu einem Kaufpreis in Höhe von 2,3 Millionen US-Dollar nachgewiesen werden. Nachdem nun konkrete Namen, Orte und entsprechende Zeitabschnitte bekannt waren, brachten mehrere Durchläufe von so genannten Schlüsselwortsuchen über alle Dateien hinweg weitere Dokumente ans Tageslicht: Angebote, Verhandlungsnotizen, auch in Verbindung mit Banken und Maklern in anderen Ländern sowie Terminabsprachen. Neben den Hinweisen zum Erwerb der Villa in Florida fanden sich zahlreiche Hinweise auf weitere konkrete Kaufverhandlungen, darunter eine Finca auf Mallorca, ein Haus in Dubai und eine Segelyacht in Spanien. Ebenfalls aufgespürt werden konnten Bankbeziehungen ins Ausland, vorwiegend in die Schweiz aber auch in die USA, die Bahamas und nach Dubai.

4. Insolvenzverfahren

In einem Insolvenzverfahren lag der Verdacht nahe, dass die vormalige Geschäftsleitung über Gebühr von einem der Investoren beeinflusst wurde. Somit konnte sich in diesem Fall die betreffende Bank zum Nachteil anderen Anteilseigner einen entsprechenden Vorteil bereits vor der Insolvenz verschaffen. Die Durchsicht und Prüfung der Aktenunterlagen ergaben keinerlei Hinweise auf irgendwelche Korrespondenz zwischen der Bank und der damaligen Geschäftsleitung, die auf einen Einfluss hinweisen oder einen solchen bestätigt hätte. Daraufhin wurden die elektronischen Daten, vorrangig der E-Mail-Verkehr zwischen der Geschäftsleitung und der Bank in Betracht gezogen. Da keine betriebsinterne Mitarbeitervereinbarung über die private Nutzung von E-Mail oder Internet bestand, wurden die E-Mails aus Datenschutzgründen mit ausdrücklich eingeholter Einwilligung der betroffenen Person (ehemaliger Vorstandsvorsitzender) aus mehreren hundert Magnetbändern / Sicherungsbändern vor Ort unter Aufsicht eines Mitarbeiters des Insolvenzverwalters extrahiert. Eine Analyse dieser extrahierten E-Mails ergab mehrere Treffer. Hierbei fanden sich E-Mails, die eindeutige Hinweise und „Anweisungen“ auf bestimmte Vorgehensweisen darstellten.

Eine Einflussnahme bzw. zumindest der Versuch zu einer Beeinflussung konnte nachgewiesen werden. Der Vorstandsvorsitzende hatte nicht damit gerechnet, dass sich auch ältere E-Mails, von den inkrementell erstellten Datensicherungsbändern zurückspielen lassen.

5. LogFiles machen auf Datenklau aufmerksam

In einem weiteren Fall war ein leitender Mitarbeiter (Projektleiter) eines größeren Konstruktionsbüros im Begriff sich selbständig zu machen. Um sich einen besseren Start zu ermöglichen, nahm er nicht nur Entwicklungsunterlagen sondern auch noch weitere Mitarbeiter und Kundenprojekte mit. Seinem bisherigen Unternehmen entstand ein Schaden in Millionenhöhe – Mitarbeiter weg, geistiges Eigentum des Unternehmens und auch Kunden weg. Ein zwischenzeitlich beauftragter Rechtsanwalt bat Kroll Ontrack um Unterstützung. Kroll Ontrack sollte die Computerdaten der beteiligten Mitarbeiter, im Besonderen die des Projektleiters, analysieren und folgendes herausfinden. Welche Absprachen gab es zwischen Projektleiter und den mittlerweile abgängigen Mitarbeitern in Vorbereitung zu deren Weggang? Wurde geistiges Eigentum, Entwicklungsunterlagen entwendet und wenn ja welche, wie, wann, von wem? Gab es schon vorbereitende Absprachen zwischen Projektleiter und Kunden? Nachdem von den Festplatten der relevanten PCs und eines Servers Images erstellt waren, konnte mit der Extrahierung der E-Mails begonnen werden. Gesucht wurden E-Mails, die bestimmte textliche auf die neue zu gründende Firma hinweisende Inhalte enthielten. Es konnten mehrere E-Mails identifiziert werden, die sehr eindeutig die Aktivitäten und Vorhaben beschrieben. Des Weiteren wurden E-Mails mit konkreten Inhalten auf geplante Aktionen, inklusive des Vorhabens bestimmte Projekte mit in die neue Firma zu übernehmen, gefunden. Eine Untersuchung der LogFiles des Netzwerk-Projekt-Servers, auf dem die gesamten Entwicklungsprojekte gesondert gespeichert waren, ergab mehrere Zugriffe von den relevanten Personen innerhalb der letzten Tage bzw. Wochen. Ein zeitlicher Abgleich mit den PC-Daten bestätigte die Zugriffe. Weiterhin konnte festgestellt werden, dass einige der Projektunterlagen von den besagten Mitarbeitern auf einen USB Memory Stick kopiert wurden. Dieser hinterlässt nämlich wie jedes Hardware-Modul einen eindeutigen Eintrag.