Elektronische Beweismittelsicherung auf der Basis von Computer Forensik

Peter Böhret, Reinhold Kern

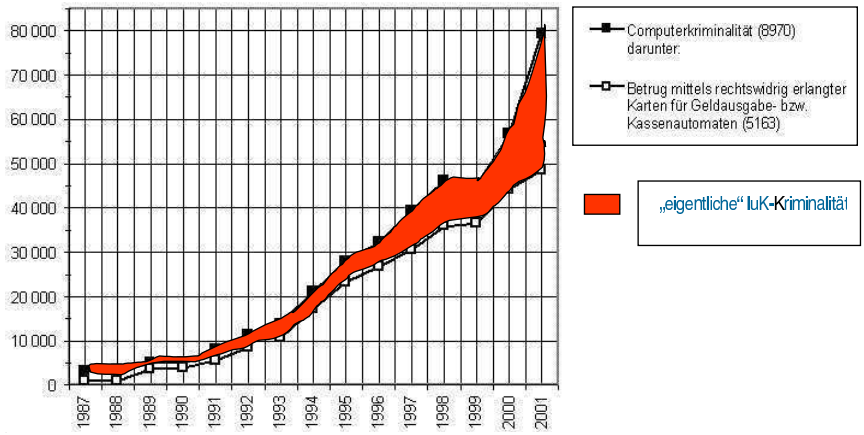
Kroll Ontrack GmbH
Hanns-Klemm-Straße 5
71034 Böblingen
rkern@krollontrack.de

Zusammenfassung: Die starke Wachstumsrate der Computerkriminalität (laut BKA Zuwachs von 2000 auf 2001 39,8 Prozent) und die hohe Dunkelziffer im Bereich der Wirtschaftskriminalität lässt die Computer Forensik als Instrument der Wiedergewinnung beweiskräftiger Daten und der Identifikation von Beweismaterial auf Computersystemen immer stärkere Bedeutung gewinnen. Zur Sicherung rechtserheblicher Daten sind neben der genauen Kenntnis von Hard- und Software festgelegte Sicherungsstrategien und -techniken unerlässlich. Nur die umsichtige, kriminalistisch korrekte Begutachtung am Tatort, forensische Untersuchung geeigneter Originalkopien oder Images der Datenträger und durchgängige Protokollierung führen zu einem beweiskräftigen Resultat.

1 Computerkriminalität in der Wirtschaft aus Sicht der Computer Forensik

Mit der Verbreitung des PCs wird der Computer einerseits selber Instrument von Straftaten anderseits als allgegenwärtiger Speicher der über ihn vollzogenen Aktivitäten aufschlussreiche Quelle und wichtiges Rechercheinstrument bei der Verfolgung von Vergehen. Neue Herausforderungen für Anwälte, Staatsanwälte, Richter ebenso wie für das

1.1 Statistiken



1.2 Fallbeispiele

Erfahrener Experten führen Wirtschaftdelikte auf so genannte „Innentäter“ – Mitarbeiter oder auch ehemalige Mitarbeiter – zurück, über die in vielen Fällen nie berichtet wird. Ein Mitarbeiter fühlt sich ungerecht behandelt oder wurde gekündigt, kopiert Vertragsdokumente, Kundenadressenlisten oder wichtige Konstruktionspläne und bietet sich hiermit bei einem neuen potenziellen Arbeitgeber, eventuellen Wettbewerber, an. Hieraus können sich erhebliche Image- und Folgeschäden für ein Unternehmen ergeben.

2 Rechtliche Voraussetzungen und Grundlagen

Da bei Untersuchungen der Computer Forensik in der Wirtschaft Daten rekonstruiert werden, die von anderen (z.B. Arbeitnehmern) erfasst und bearbeitet wurden, muss die rechtliche Grundlage für Untersuchungen rechtzeitig im Arbeitsvertrag oder entsprechenden Zusatzvereinbarungen unter Hinzuziehung aller Entscheidungsgremien wie dem Betriebsrat gelegt werden.

2.1 Chain of Custody (Lückenlose Dokumentation)

PIN-Nummern für die Kreditkarte, die Geldkarte, ... die Passwörter für den Computer ... was soll / muss man sich noch so alles merken. Ob am Bildschirm, unter der Tastatur oder in der obersten Schublade des Schreibtisches, meist finden sich die notierten Passwörter im Umkreis eines Meters um den PC herum. Dies ermöglicht auch Unberechtigten einen Zugriff auf einen fremden PC.

Durch Computer Forensische Untersuchungen lassen sich viele Aktivitäten am PC nachweisen, aber es ergibt nicht den 100%-igen Beweis, dass auch der berechtigte Nutzer des PCs (Mitarbeiter) tatsächlich selbst die verhängnisvolle Email verfasst, ein Dokument verändert oder den PC sonst wie manipuliert hat. Ein später bei forensischen Untersuchungen erhaltener „Beweis“ stellt also lediglich ein Glied einer Beweiskette für die Schuld aber auch für die Unschuld eines Verdächtigten oder Beklagten dar.

Deshalb ist es äußerst wichtig und unabdingbar den Weg und die Art der Untersuchung und Ermittlung genauestens zu protokollieren. Auch ist nachweisbar sicher zu stellen, dass auch nach einer Erfassung der Daten (Beschlagnahme durch Strafverfolgungsbehörden oder bei 1:1 Kopien / Images der Datenträger im Besonderen bei privaten, eigeninitiierten Ermittlungen) und im weiteren Verlauf der Untersuchungen die Originalität der Daten erhalten bleibt. Nur eine lückenlose Dokumentation / Protokollierung aller Aktivitäten erlaubt eine Reproduktion der Untersuchungen bzw. deren Ergebnisse.

3 Technische Möglichkeiten

Die Suche nach rechtserheblichen Daten setzt nicht nur die genaue Kenntnis der Mechanik und Funktion von Speichermedien sondern auch das Wissen um deren Speicherprozesse und Dateiverwaltung auf hardwarenaher Systemebene, aber auch auf Ebene der Betriebssysteme und der Programme voraus.

3.1 Speichermedien

Die große Vielfalt an Speichermedien wie Magnetbänder (DAT, Streamer, DLT, AIT ...) oder Festplatten und deren technologischen Innovationen führen zu immer neuen Herausforderungen für die Ermittler und Computer Forensiker.

3.2 Defekte und Löschverfahren

Im guten Glauben an die Technik verlassen sich die „Täter“ meist auf oberflächliches Löschen von Dateien oder Formatieren von Festplatten oder zerstören Speichermedien physikalisch um verräterische Spuren zu verwischen.

3.3 Gegenmaßnahmen und „Reparaturen“

Experten der Strafverfolgungsbehörden und einige wenige auf Wiederherstellung von z.B. gelöschten Daten, auch von mechanisch zerstörten Datenträgern, spezialisierte Dienstleistungsunternehmen mit speziellen Labors, sind meist in der Lage solche vermeintlich verwischten Spuren wieder sichtbar und gerichtserheblich verwendbar zu machen.

4 Computer Forensik in der Praxis

Bei Untersuchungen vor Ort, gilt es das Augenmerk auf den Ist-Zustand des PC zu richten und ihn zu dokumentieren. Hierzu gehört die Dokumentation der Umgebungsbedingungen ebenso wie eventuell die Sicherung des Speichers und der Bildschirmanzeige des laufenden Rechners. Auf keinen Fall darf mit dem Rechner weitergearbeitet werden! Die Datenträger des Rechners müssen sichergestellt und im Labor sektorweise ohne Veränderung der Meta-Daten kopiert werden. Wiederherstellungsaktionen und Datenrecherche sollten soweit wie möglich nur an einer zweiten Kopie der Daten erfolgen. Der Originaldatenträger muss unverändert bleiben und alle Wiederherstellungs- und Rechercheaktionen lückenlos protokolliert werden, um die Beweiskraft vor Gericht zu erhalten.

4.1 Data Collection

Mit speziellen Geräten, die ein Schreiben auf eine Festplatte verhindern – so genannte “Write Blocker“ – werden 1:1 Kopien, so genannte Images der Festplatten erstellt, die alle einzelnen Bits erfassen um somit eine 100%-ige Kopie des Originals zu erhalten. Von diesen Original-Kopien wird eine zweite Kopie erstellt, die später für die eigentlichen Untersuchungen und Analysen verwendet wird. Die erste Original-Kopie wird zur Sicherheit in einem Safe aufbewahrt. Somit ist sicher gestellt, dass zu jeder Zeit eine Reproduktion der Untersuchungsergebnisse, z.B. für ein Gegengutachten, möglich ist.

4.2 Data Recovery

Jetzt sind die Computer Forensik Experten gefordert mittels spezieller Software Programme z. B. gelöschte Dateien wieder sichtbar und lesbar zu machen. Hierzu werden sowohl

am Markt frei verfügbar Software Programme oder proprietäre, spezielle Software Programme der o.g. privaten Labors. Ist ein Speichermedium z.B. eine Festplatte mechanisch beschädigt, so müssen die Daten in einem eigens für solche Fälle eingerichteten Reinraum wieder hergestellt werden, denn selbst das kleinste Staubkorn auf einer offenen Festplatte könnte zu einer weiteren Zerstörung der Plattenoberfläche führen und somit die Lesbarkeit sehr stark beeinträchtigen wenn nicht sogar unmöglich machen.

4.3 Filter, Suche und Deduplikation

Mittels Filterprogramme und entsprechender Suchkriterien werden die verfügbaren Daten auf relevante Daten und Dokumente untersucht. Sehr oft finden sich Duplikate von Dokumenten innerhalb des zu untersuchenden Datenbestandes, die eine Analyse, alleine schon durch die Menge, unnötig erschweren. Mit speziellen Software Programmen lassen sich solche Duplikate (z.B. Emails an verschiedene Adressaten) oder auch leere Seiten von Word Dokumenten herausfiltern. Jedes einzelne gefundene Dokument kann nun auf seine Inhalte hin überprüft und katalogisiert werden.

4.4 Reporting

Die gesamte angesprochene Vorarbeit dient und ermöglicht Ermittlern der Strafverfolgungsbehörden oder private Ermittler zur Auswertung und Beurteilung der relevanten Daten und Dokumente. Erst diese Katalogisierung und überschaubare Zusammenstellung der Resultate erlaubt den Ermittlern eine zeitnahe Auswertung der Fakten.

Bisher waren Anwälte, Staatsanwälte wie auch Richter gewohnt Dokumente und Beweise „Schwarz auf Weiß“ zu bewerten und zu beurteilen, d.h. gefundene „Elektronische Beweise“ mussten auf Papier ausgedruckt werden. Moderne Software Lösungen erlauben heute Ermittlern und Teams von jedem Standort aus gleichzeitig Auswertungen und Ergebnisse über so genannte Viewer (Betrachter) online zu analysieren und darzustellen.

5 Bedeutung der Computer Forensik für Unternehmen

Firmencomputer nehmen eine Schlüsselstellung in der Wirtschaftkriminalität ein. Die Computer Forensik bietet die Chance, einem Anfangsverdacht nachzugehen und Ermittlungen zielgerichtet zu führen. Auch wenn zunächst der Schutz des Unternehmens und nicht die Strafverfolgung im Vordergrund steht, müssen Indizien und Verdachtsmomente so erhoben werden, dass Sie eine strafgerichtliche Verfolgung nicht behindern oder gar ausschließen. Dieser Wunsch macht die Computer Forensik nicht nur zu einer sensiblen Schnittstelle zwischen Unternehmen und Justiz, sondern auch zu einem Thema für Spezialisten der Datenwiederherstellung und Ermittlung.