MHP
MICHAEL HARZ PROJURE GMBH
WIRTSCHAFTSFORENSIK · COMPUTERFORENSIK
BETRIEBSWIRTSCHAFTLICHE SACHVERSTÄNDIGE
IN STRAF-, ZIVIL- UND INSOLVENZVERFAHREN

Computerforensik

Ein Fall aus der Gutachterpraxis

Dr. rer. pol. Michael Harz,
Dr.-Ing. Mathias Bauer
Dipl.-Bw. Jürgen Obermayr
MHP Michael Harz ProJure GmbH
Saarbrücken · Frankfurt am Main

Am Staden 18
66121 Saarbrücken
Telefon: 06 81/95 44 00

Lyoner Straße 14
60528 Frankfurt
Telefon: 0 69/66 55 44 69

Internet: www.harz-projure.de
E-Mail: info@harz-projure.de
Telefax: 06 81/95 44 040

Amtsgericht Frankfurt a.M.
HRB 92616
USt-IdNr.: DE 280590346

Inhaltsverzeichnis **Seite**

1. Allgemeine Beschreibung computerforensischer Methoden

Die Computerforensik "behandelt die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen und der Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren in Computersystemen." (Quelle wikipedia.de)

Insbesondere werden folgende Aspekte abgedeckt:

- Sicherung von Beweisen auf Computersystemen
- Der Computer als Werkzeug zur Vorbereitung oder Durchführung eines Verbrechens
- Der Computer als Tatwaffe

Die Sicherung von Beweisen befasst sich dabei mit so unterschiedlichen Aufgabenstellungen wie der Wiederherstellung gelöschter oder zerstörter Datenträger, der Identifizierung und Nutzbarmachung relevanter Daten innerhalb eines Systems sowie der Datenintegration, d. h. der Zusammenführung von Daten aus unterschiedlichen Kontexten – oftmals in verschiedenen Formaten, Sprachen oder Kodierungen – und mit dem Ziel, Anhaltspunkte für die Feststellung oder Aufklärung eines Vergehens zu finden und diese in gerichtsverwertbarer Form zu sichern.
Die Schwierigkeiten liegen dabei – selbst bei technisch intakten Systemen und Datenträgern – in der Sichtung großer Datenmengen und dem Auffinden relevanter Daten sowie im Umgehen von Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung.

Ist diese Phase abgeschlossen, müssen neben strukturierten Daten (etwa Kontobewegungen oder Telefonverbindungsdaten) oftmals auch Daten in Textform verarbeitet werden. Um beispielsweise aus Emails oder SMS deren wesentlichen Inhalt zu extrahieren, müssen diese unabhängig von den verwendeten Formulierungen und Begriffen auf ihren Gehalt untersucht werden. Dabei kommen Verfahren aus Statistik und Linguistik zum Einsatz, mit deren Hilfe u. a. semantisch verwandte Ausdrücke gefunden werden können.
Auch die im folgenden Fall aus der Gutachterpraxis durchgeführten Datenanalysen sind dieser Phase der Computerforensik zuzuordnen.

Aufgrund der zunehmenden Vernetzung und Virtualisierung vieler Geschäftsprozesse spielt auch der Computer als Tatwaffe eine zunehmend wichtige Rolle. Hier dient die Computerforensik dazu, Einbrüche in Computersysteme und Datendiebstähle anhand vom Eindringling hinterlassener digitaler Spuren aufzudecken, feindliche Angriffe möglichst frühzeitig zu erkennen, um geeignete Gegenmaßnahmen einzuleiten sowie Schadsoftware wie Trojaner unschädlich zu machen.

2. Praxisbeispiel

2.1. Prüfungsauftrag

Im vorliegenden Fall wurden wir von einer Staatsanwaltschaft beauftragt, eventuelle Auffälligkeiten innerhalb der Buchführung und Bilanzierung einer Unternehmensgruppe aufzudecken und diese in einem schriftlichen Gutachten darzustellen. Weiterhin sollten ein Schaden (falls vorhanden) quantifiziert und die Verantwortlichkeiten festgestellt werden.

2.2. Beschreibung und Prüfungsvorgehen

Die zu prüfende Unternehmensgruppe ist eine mittelgroße Baustoffhandlung, die sich aus sechs Unternehmen zusammensetzt. Der Unternehmenssitz liegt im süddeutschen Raum. Die Verwaltungstätigkeiten sowie die Geschäftsführung wurden für alle Gesellschaften von einer Holding ausgeführt. Demnach waren dieser Holding die Geschäftsführung und das Finanz- und Rechnungswesen zugeordnet. Die Geschäftsführung erfolgte durch den Alleingesellschafter und Unternehmensgründer. Der Leiter des Finanz- und Rechnungswesens, der bereits seit 20 Jahren in dem Unternehmen beschäftigt war, genoss aufgrund der langen Beschäftigungszeit auch das volle Vertrauen der Geschäftsleitung. Die Unternehmensgruppe konnte in der Vergangenheit auf ein stetiges Wachstum zurückblicken. Als jedoch in den Jahren 2006 bis 2009 trotz jährlicher Umsatzsteigerung von durchschnittlich 10 % der Gewinn rückläufig war,

erkundigte sich der Unternehmensgründer bei dem Leiter des Finanz- und Rechnungswesens nach den Ursachen hierfür. Dieser erläuterte, dass dies mit den in den letzten Jahren durchgeführten Investitionen in Zusammenhang stehe.
Da dem Unternehmensgründer diese Begründung nicht ausreichend plausibel erschien und es Hinweise auf Unregelmäßigkeiten innerhalb des Unternehmens gab, erstattete er Anzeige.

Im Rahmen der Ermittlungen der Staatsanwaltschaft wurde die Michael Harz ProJure GmbH beauftragt, eventuelle Betrugs- oder Untreuehandlungen anhand der Buchführung und Bilanzierung zu überprüfen.

Im Folgenden werden wir unser Prüfungsvorgehen sowie die eingesetzten Methoden näher erläutern.

2.2.1. Überprüfung von Auffälligkeiten in der Bilanz / GuV / Jahresabschluss

Zur Überprüfung von Auffälligkeiten in der Bilanz / GuV / Jahresabschluss wurde durch das Prüfungsteam die neu entwickelte BilMan-Software herangezogen.
Die BilMan-Software ist inspiriert worden von statistischen Verfahren, die schon seit Jahrzehnten bekannt sind und zur Überprüfung der Integrität numerischer Datensammlungen angewandt werden. Die sogenannte Benford-Verteilung[1] (siehe Abbildung 1) beschreibt die erwartete Verteilung der Anfangsziffern der in einer Zahlensammlung auftretenden Werte. Entgegen der allgemeinen Erwartung sind diese nicht gleichverteilt. Vielmehr ist es so, dass typischerweise rund 30% aller Zahlen mit einer Eins beginnen, aber nur rund 4,5% mit einer Neun. Ein Test anhand dieser Verteilung überprüft, ob die vorhandenen Zahlen signifikant von dieser Vorgabe abweichen.

[1] http://de.wikipedia.org/wiki/Benfordsches_Gesetz

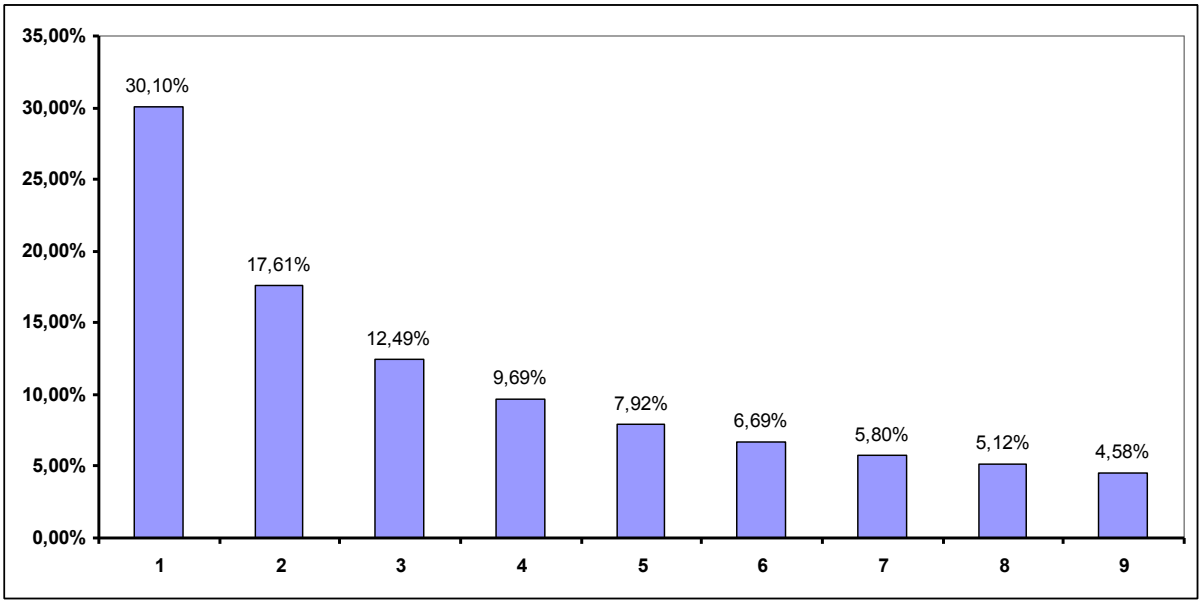

Abbildung 1: Die Benford-Verteilung

Während diese Verteilung einen recht guten Erwartungswert für zahlreiche Datensammlungen bietet, so ist sie doch für eine Anwendung im Bereich der Bilanzprüfung zu unpräzise, da sie einerseits nicht auf die besonderen Eigenheiten von Bilanzen eingeht, andererseits kein spezielles Kriterium bietet, das eine Manipulation der Daten als solche korrekt erkennt.

Die BilMan-Software wurde daher mit Hilfe von etwa 8.000 Bilanzen trainiert. Als Ergebnisse erhielten wir einerseits eine Variante der Benford-Verteilung, wie sie für korrekte Bilanzen repräsentativ ist sowie einen Toleranzkorridor, der zulässige Abweichungen von der Norm beschreibt.

Auf Basis dieser Verteilung wurden mittels Verfahren der Künstlichen Intelligenz verschiedene Modelle automatisch erzeugt, die einerseits die Abweichung der Verteilung der Anfangsziffern von der genannten Variante der Benford-Verteilung überwachen, andererseits 15 typische Manipulationsmuster erkennen. Damit werden nahezu alle Bilanzmanipulationen erfasst. Auf diese Weise wurde ein komplexes Analysesystem entwickelt, in dem zwei unterschiedlich arbeitende Modelle unabhängig voneinander eine vorliegende Bilanz beurteilen. Diese beiden Teilergebnisse werden von einem weiteren Modell zu einer endgültigen Bewertung verknüpft, so dass eine jederzeit nachvollziehbare, objektive Aussage zu einer gegebenen Bilanz getroffen werden kann.

Die folgenden Schritte 1 bis 3 beschreiben den praktischen Einsatz der BilMan-Software:

Schritt 1:
Im ersten Schritt wurden die Jahresabschlüsse der vergangenen 4 Jahre mittels Scanner eingelesen.

Schritt 2:
Der zweite Schritt wurde durch die BilMan-Software automatisch ausgeführt. Die Software ermittelte mittels statistischer Verfahren, dass mit einer Wahrscheinlichkeit in Höhe von 98 % Manipulationen an verschiedenen Geldtransitkonten von fünf Gesellschaften vorgenommen wurden.

Schritt 3:
Da die Software innerhalb des zweiten Schritts mit einer an Sicherheit grenzenden Wahrscheinlichkeit festgestellt hatte, dass Manipulationen innerhalb der verschiedenen Bilanzen vorgenommen wurden, wurden die von der Software angegebenen Bilanzpositionen näher überprüft. So konnte festgestellt werden, dass die Buchungen auf den angegebenen Geldtransitkonten in der Regel als Gegenkonto ein Bankkonto auswiesen. Das Prüfungsteam hat sich aufgrund dessen entschlossen, mittels speziell entwickelter EDV-Techniken eine Überprüfung sämtlicher auf diesen Konten erfassten Zahlungsflüsse vorzunehmen.

2.2.2. Überprüfung der Zahlungsflüsse mittels speziell entwickelter EDV-Techniken

Es kann sinnvoll sein, die Zahlungsflüsse eines Unternehmens oder einer Unternehmensgruppe regelmäßig auf Auffälligkeiten zu untersuchen. Diese sind definiert als Abweichungen vom normalen Geschäftsverlauf und werden typischerweise in Form manuell erstellter Muster innerhalb eines Systems verwaltet. Diese Muster ergeben sich entweder durch gesetzliche Vorgaben (z. B. Verpflichtung zur Überprüfung aller Zahlungsflüsse oberhalb eines bestimmten Schwellenwerts oder in eine bestimmte Region), durch Vorgaben des Managements (z. B. Überprüfung aller Zahlungen durch Verrechnungsschecks) oder durch Erfahrungswerte der betreffenden Mitarbeiter, die bereits mit der Aufarbeitung inkorrekter Zahlungen betraut waren. Somit können sich auch Muster ergeben, die sich über mehrere Zahlungsvorgänge erstrecken (z. B. mehrere Zahlungen an den gleichen Empfänger mit identischem Betrag oder gerade unterhalb einer vom Management als kritisch vorgegebenen Grenze).

Neueste Entwicklungen setzen auch hier intelligente Methoden wie Data Mining ein, um solche Muster automatisch zu identifizieren und die Trefferquote insbesondere bei nicht offensichtlichen Unregelmäßigkeiten zu erhöhen. In allen Fällen bleibt jedoch eine manuelle Nachprüfung erforderlich, da es für viele Auffälligkeiten durchaus plausible Erklärungen geben kann.

In dem vorliegenden Fall konnten die in Einsatz gebrachten EDV-Techniken innerhalb kürzester Zeit sämtliche Transaktionen des manipulierten Bilanzkontos sowie die Transaktionen der Gegenkonten überprüfen. Dazu wurden durch das Prüfungsteam vor Ort Abfragen definiert, mit denen die Software diese Transaktionen durchleuchtete.

Zu diesen Abfragen gehörten unter anderem:

- Wie viele Buchungen wurden auf diesem Konto im Betrachtungszeitraum vorgenommen?
- Wie viele Buchungen enthielten den gleichen EURO-Betrag?
- Welche Gegenkonten innerhalb der Finanzbuchhaltung wurden angesprochen?
- Welche Bankkonten wurden angesprochen?
- Wie häufig wurden diese Bankkonten angesprochen?
- Welche Buchungen enthalten den gleichen Buchungstext?
- Welche der Zahlungen wurden per Scheck geleistet?
- Bei welchen Bankkontonummern gibt es keine Übereinstimmung zu den Stammdaten der Kreditoren?

Mit Hilfe dieser Abfragen war festzustellen, dass eine große Anzahl von Zahlungen mit Verrechnungsschecks geleistet wurden. Da dies primär nicht ungewöhnlich sein muss, wurden in Folge dessen die Scheckempfänger mit den Kreditoren der einzelnen Gesellschaften abgeglichen. Bei diesem Abgleich konnten wir feststellen, dass unrechtmäßige Zahlungen stattgefunden haben, da diese Transaktionen weder einem bereits im System erfassten Kreditor noch einer Eingangsrechnung von anderen Kreditoren zugeordnet werden konnten. Es konnte außerdem festgestellt werden, dass die Zahlungen auf Privatkonten außerhalb der Unternehmensgruppe sowie an einen fiktiven Lieferanten geleistet wurden.
Weiterhin ergab die manuelle Überprüfung der Zahlungen, dass die ausgestellten Verrechnungsschecks ausschließlich von dem Leiter des Finanz- und Rechnungswesens ausgestellt wurden. Zur Überprüfung, ob eventuell ein Zusammenhang zwischen ihm und den unrechtmäßigen Zahlungen besteht, wurde in Folge dessen durch das Prüfungsteam eine Netzwerkanalyse durchgeführt.

2.2.3. Netzwerkanalyse zur Überprüfung des Zusammenhangs zwischen Zahlungen und Mitarbeiter

Bei einer Netzwerkanalyse geht es darum, nicht offensichtliche Verbindungen zwischen Personen, Unternehmen, Objekten usw. aufzudecken. Das Problem liegt darin, dass die zugehörigen Daten typischerweise in unterschiedlichen Datenbanken abgelegt sind, die zum Zweck der Analyse – unter Einhaltung der Vorschriften des Datenschutzes – miteinander verknüpft werden müssen. Abbildung 2 zeigt, welche Datenbanken im vorliegenden Beispiel relevant waren.

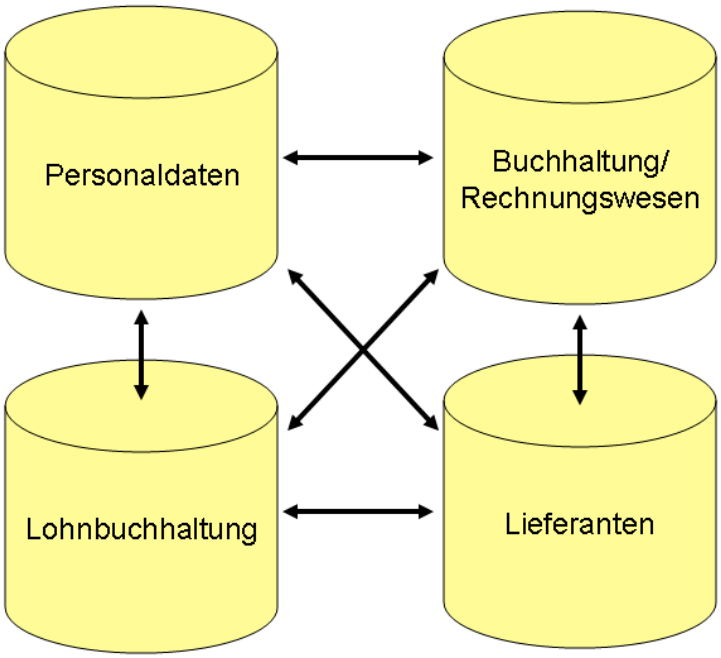

Abbildung 2: Datenbanken innerhalb eines Unternehmens

Bei gegebenem Betrugsverdacht können beispielsweise gezielt Verbindungen zwischen Lieferanten bzw. Zahlungsempfängern und Mitarbeitern gesucht werden. Zu diesem Zweck ist es vorteilhaft, innerhalb der entsprechenden Daten mit einer geeigneten Anfragesprache direkt nach bestimmten Mustern zu suchen. Eine solche Anfrage könnte etwa lauten "Gib mir alle Lieferanten, die die gleiche Adresse wie einer unserer Mitarbeiter haben." Solche Systeme benötigen also einen Experten, der exakt weiß, nach welcher Art von Verbindung er sucht.
Aktuelle Ansätze unterstützen den Bediener durch eine ausgefeilte Visualisierung der Zusammenhänge zwischen einzelnen Datensätzen und sind

teilweise in der Lage, aus Trainingsdaten die Muster für betrügerisches Verhalten zu extrahieren und die Suche danach zu automatisieren.

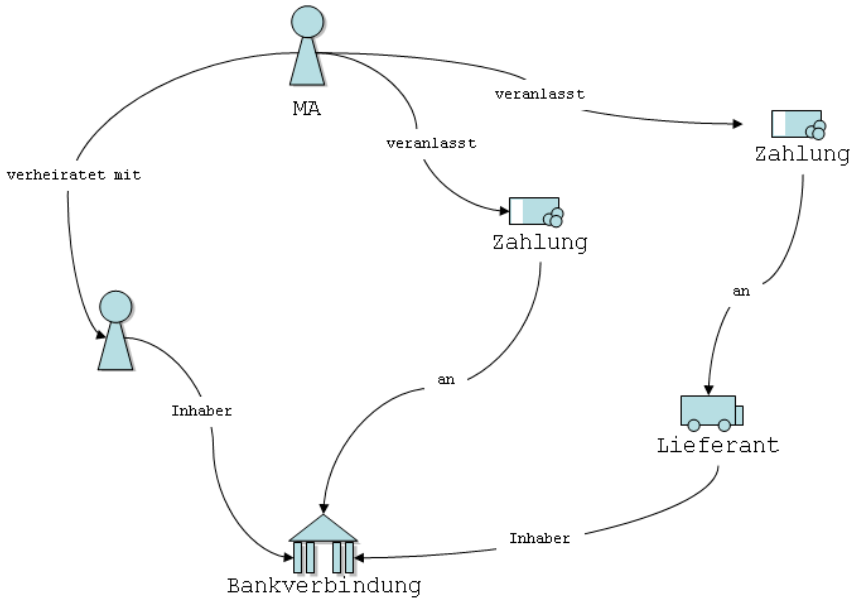

Abbildung 3: Netzwerkstruktur auffälliger Zahlungen

Abbildung 3 veranschaulicht die Vernetzung von Personen, Organisationen und sonstigen Objekten, deren Daten im Zusammenhang mit mehreren Zahlungen stehen. Eine visuelle Inspektion dieses Netzwerkes macht deutlich, dass offensichtlich von einem Mitarbeiter Zahlungen auf ein Konto seiner Ehefrau veranlasst wurden. In einem Fall erfolgte die Zahlung direkt, in einem anderen Fall wurde dafür ein Lieferant zwischengeschaltet, der jedoch die gleiche Bankverbindung besitzt.

Das Auffinden solcher Verbindungen kann unterstützt werden durch intelligente Systeme, die heuristisch nach Auffälligkeiten – z. B. gleiche oder ähnliche Werte in bestimmten Datenattributen – suchen und diese visualisieren.

Durch den Einsatz der Netzwerkanalyse konnten wir schließlich herausfinden, dass die Zahlungen an die Privatkonten der geschiedenen Frau des Leiters Finanz- und Rechnungswesens ohne jegliche Gegenleistung geleistet wurden bzw. an einen Lieferanten erfolgten, der gar nicht existierte und dem ebenfalls ein Bankkonto der geschiedenen Frau zugeordnet war.

2.3. Zusammenfassung

Durch den Einsatz der selbstentwickelten BilMan-Software sowie neuester Methoden der Computerforensik (Data Mining) in Verbindung mit dem betriebswirtschaftlichen Know-How konnte dem Leiter des Finanz- und Rechnungswesens nachgewiesen werden, dass er die Unternehmensgruppe über mehrere Jahre hinweg um mehr als 2,5 Mio. € betrogen hatte. Der verantwortliche Mitarbeiter vereinnahmte das Geld durch Ausstellen von Verrechnungsschecks, die von der geschiedenen Ehefrau auf deren Privatkonten eingelöst wurden und durch das Erstellen und Bezahlen von Rechnungen für einen fiktiven Lieferanten. Aufgrund des Einsatzes der beschriebenen Methoden der Computerforensik, insbesondere der BilMan-Software und des Data Mining lag im vorliegenden Fall das Prüfungsergebnis bereits nach 2 Wochen vor. Eine manuelle Prüfung hätte demgegenüber ein Vielfaches an Zeit in Anspruch genommen. Im Rahmen der Strafverfolgung wird der Einsatz von Methoden der Computerforensik in den nächsten Jahren erheblich zunehmen.