



Vom wirren Datenhaufen zur logischen Beweiskette

Sobald nach einem wirtschaftskriminellen Vorfall sämtliche Beweise identifiziert, erfasst (Papierdokumente) und gesichert sind, ist zwar ein aufwändiges Stück Arbeit getan. Der anspruchsvollste Teil IT Forensik beginnt jedoch erst jetzt - mit der Analyse der gesammelten Daten und deren gerichtstauglichen Aufbereitung ...

Die Durchführung einer forensischen Analyse ist vergleichbar mit der berühmten Suche nach der Nadel im Heuhaufen und erfordert deshalb bereits bei kleineren Fällen (Datenvolumen bis zu 2 Terabytes) Experten Know-how. Die damit beauftragten Spezialisten müssen über umfassende Kenntnisse von Dateisystemen, der Organisation von Daten auf Rechnersystemen und der Rettung beschädigter oder gelöschter Daten verfügen. Ausgeprägtes kriminaltechnisches Denkvermögen ist eine weitere unverzichtbare Grundlage. Denn letztendlich leistet der Forensiker ein gutes Stück Detektivarbeit, wenn er die gesicherten Inhalte nach gerichtlich verwendbaren Indizien durchsucht und die gefundenen Beweisstücke Schritt für Schritt zur logischen Beweiskette zusammenfügt.

Vor diesem Hintergrund ist es nicht erstaunlich, dass Unternehmen für diese Aufgabe immer häufiger externe Spezialisten hinzuziehen. Entscheidend dabei ist, dass der ausführende Forensiker detailliert über den zu analysierenden Vorfall informiert ist und genau weiss, wonach sein Auftraggeber sucht.

Welche Prozessschritte umfasst eine forensische Datenanalyse?

Wesentliche Voraussetzungen

Die Analyse der Daten wird immer an einem 1:1 Duplikat der Originaldaten vorgenommen. Dabei ist es wichtig, dass die genutzten Speichermedien die Unversehrtheit und Unveränderbarkeit der Daten gewährleisten. Heute wird dazu als Standardformat EnCase verwendet.

Die Wahl adäquater Analysemethoden und -software spielt für die Korrektheit der Analyse eine tragende Rolle.

Der Analyseprozess im Detail

- Die gesammelten Daten werden nach fallrelevanten Kriterien gefiltert und normalisiert. Die Normalisierung eliminiert Doppelspurigkeiten und vermeidet redundante Daten.
- Die extrahierten Daten durchlaufen nun eine Volltext-Indizierung, damit sie von allen beteiligten Ermittlern nach inhaltlichen Kriterien suchbar sind.
- Die konsolidierten Beweisdaten werden aussortiert, strukturiert und unter Gewährleistung höchster Sicherheitsstandards separat abgespeichert.
- Die indizierten und klassifizierten Daten werden in ein marktübliches, für alle involvierten Parteien lesbares und druckbares Format konvertiert.
- Als Vorbereitung für die Erstellung des Expertengutachtens werden nun anhand der reproduzierten Beweisstücke und Indizien die erfolgten Ereignisse rekonstruiert, mit den involvierten Personen und Firmen in Zusammenhang gebracht und chronologisch dargestellt.
- Die dabei ausgeführten Arbeitsschritte werden lückenlos protokolliert und vom Gutachter als logische, für jeden Betrachter (Auftraggeber, Anwälte, Richter, etc.) präzise nachvollziehbare Beweiskette dokumentiert, die vor Gericht standhält und ein erfolgreiches Verfahren optimal unterstützt.

Welche Erkenntnisse liefern die Ergebnisse der Analyse?

Forensische Datenanalysen dienen der Ermittlung ...

- der Identität des resp. der involvierten Täter(s)
- der genutzten Kommunikationswege (soweit rechtlich möglich)
- des Zeitraums der Tat durch chronologische Darstellung («Timeline») aller Vorkommnisse, die zur Untersuchung des Falles oder zur Anklage geführt haben
- des Tatherganges
- der Dimension des Vorfalls (Basis für die Schadensbewertung)
- der Ursachen und Motive, die dazu geführt haben

Ob die Analyse klare Antworten auf alle erwähnten Punkte liefert, hängt sowohl vom Beweismaterial als auch von der richtigen Interpretation der untersuchten Inhalte ab.

Worin besteht der Hauptnutzen für die betroffenen Unternehmen und deren Anwälte?

- Die ermittelten Analyseergebnisse bilden die Grundlage für die Erstellung des abschließenden Expertengutachtens, das die fallrelevanten Zusammenhänge erläutert und in gerichtstauglicher Form präsentiert. Grundsätzlich gilt: je früher die Analyse erfolgt und je aussagekräftiger die daraus hervorgehenden Inputs für das Gerichtsgutachten sind, desto größer sind die Gewinnchancen - sowohl bei Verhandlungen mit der Gegenpartei als auch vor Gericht.
- Zusätzlich bringen forensische Analysen möglicherweise auch entlastendes Beweismaterial ans Licht, das die verantwortlichen Ermittler davor bewahrt, falsche Spuren zu verfolgen und/oder die falschen Personen als Täter zu verdächtigen.
- Der Einsatz marktführender Suchtechnologie sorgt dafür, dass alle Beweisstücke und Indizien nach inhaltlichen Kriterien umgehend auffindbar sind. Dies unterstützt eine effiziente Zusammenarbeit zwischen allen involvierten Parteien.
- Die Aufbereitung und Präsentation der Ergebnisse als gerichtskonformes Gutachten reduziert den Aufwand der Ermittler (Polizei) und der zuständigen Anwälte signifikant und beschleunigt die Überprüfung der Beweislage. Dadurch können die erforderlichen Maßnahmen (Gerichtsverfahren) verzögerungsfrei eingeleitet und durchgeführt werden.

Forensische Untersuchungen sind Vertrauenssache. Bei Scalaris dürfen Sie absolute Diskretion ebenso voraussetzen, wie höchste Professionalitäts- und Qualitätsstandards.

Sprechen Sie mit uns.

Wir stellen Ihnen unser Forensic Services Angebot gerne persönlich vor.

Ihr Ansprechpartner:

Dr. Andrea Galli

Phd. Nat. sci. ETHZ

Head of Economic Crime Intelligence (ECI)

Telefon +41 44 809 25 95

Mobile +41 79 456 76 32

E-Mail andrea.galli@scalaris.com