



Fakten, Fakten, Fakten:

IT-Forensiker überführt Industriespione

Wahrheitsgetreue Information schützt vor potenziellen Geschäftsrisiken und stellt wasserdichtes Beweismaterial für Anklage und Verteidigung dar.

Der einfache Zugang zu den jeweils relevanten Daten sorgt nicht nur für effiziente Geschäftsprozesse, sondern ist heutzutage existenzkritisch. Denn jede Form des Risikomanagements ist auf das Zuspätkommen der entsprechenden Informationen angewiesen, um Gefahren rechtzeitig erkennen und entsprechende Schutzmaßnahmen ergreifen zu können. Auch im Ernstfall, wenn es darum geht, vor Gericht das rechtskonforme Verhalten oder als Ankläger einen Verdacht zu beweisen, zählt nur eine eindeutig nachvollziehbare Faktenlage.

Die traditionellen Methoden der Datenverwaltung werden diesen Anforderungen, welche die Disziplin Governance, Risk & Compliance (GRC) an das Informationsmanagement stellt, nicht gerecht. Kaum ein Unternehmen verfügt über ein ganzheitliches Konzept, das einen zentralen und schnellen Zugriff auf alle vorhandenen Informationen gewährleistet. Sie werden in zahlreichen, isoliert betriebenen elektronischen Systemen und teilweise nach wie vor in Papierform aufbewahrt. Für viele Fragestellungen reicht die interne Wissensbasis auch gar nicht aus. Spezifische Informationen und Nachrichten sind dann erforderlich, um ein vollständiges und aktuelles Bild über Personen, Organisationen und Situationen zu erhalten. Wenn im Falle eines Rechtsstreits die Aufgabe darin besteht, die verstreuten Datenmassen möglichst schnell nach Indizien zu durchsuchen und eine gerichtsverwertbare Argumentation aufzubereiten, wird diese Problematik hochbrisant. Das kann mehrere Mann-Monate manueller Arbeit bedeuten und entsprechende Kosten verursachen. Und immer besteht das Risiko, wesentliche Informationen zu übersehen.

Vor allem international agierende Organisationen werden zunehmend mit Wirtschaftsdelikten wie Veruntreuen, Industriespionage, Unlauterer Wettbewerb, Betrug, Geldwäsche, Korruption oder Terrorismusfinanzierung konfrontiert und benötigen professionelle Unterstützung – sowohl für präventive Maßnahmen als auch für die Überführung krimineller Subjekte. So wurde die Scalaris AG kürzlich in einem sehr dreisten Fall der Industriespionage als Experte für die Beweismittelsicherung hinzugezogen. „Die Existenz eines europaweit tätigen Technologieunternehmens schien durch einen illegalen Informationsabfluss in hohem Maß bedroht zu sein. Es gab



zahlreiche Indizien, die in Summe ein recht eindeutiges Bild ergaben, aber keine Beweise, um rechtliche Schritte einzuleiten“, erklärt Dr. Andrea Galli, Head of Economic Crime Intelligence bei Scalaris, die Ausgangslage. In kürzester Zeit analysierte das Unternehmen aus Glattbrugg alle relevanten Datenquellen und fasste die einzelnen Indizien zu einem wasserdichten Gerichtsgutachten zusammen – mit dem Erfolg, dass die Angelegenheit in einem Express-Verfahren nach nur drei Monaten von der Staatsanwaltschaft aufgenommen wurde. Schnelle erste Hausdurchsuchungen setzten vorab ein wirkungsvolles Signal, dass die Täter auf keinen Fall ungeschoren davonkommen würden und verhinderten weitere Schäden. Das Gericht verurteilte sie schließlich zu hohen Geldbußen und Schadensersatzzahlungen.

Gefahr im Verzug

Kurz nachdem ein Top-Manager das Unternehmen verlassen hatte, sorgte eine kleinere Kündigungswelle von Mitarbeitern in Schlüsselpositionen für Unruhe. Der Weggang mehrerer Personen innerhalb kurzer Zeit war für die 5.000 Mitarbeiter Organisation ungewöhnlich und ist in der know-how-intensiven Technologiebranche zudem höchst bedenklich. Nachdem bekannt wurde, dass der erwähnte ehemalige Top-Manager regelmäßigen Kontakt zu Mitarbeitern und Kunden pflegte, war die Schlussfolgerung logisch: Anscheinend war es das Ziel, Mitarbeiter und Kunden abzuwerben. Da der Verlust weiterer wichtiger Know-how-Träger und schließlich der Kunden geradezu absehbar war, durfte man keine Zeit verlieren, um rechtliche Schritte anstoßen. Aber was hatte man in der Hand, um den Verdacht zu beweisen? Kündigungen sowie Treffen mit Ex-Kollegen und Kunden sind per se nicht gesetzeswidrig. Auf Empfehlung einer Kanzlei kontaktierte man Scalaris. In der Hoffnung, dass der Hauptverdächtige und mögliche Komplizen innerhalb der Organisation Spuren, beispielweise in Form von Dokumenten und E-Mails, hinterlassen hatten, erhielt der IT-Forensiker den Auftrag zur Beweismittelsicherung.

Systematische Spurensuche

Wie der Begriff schon verrät, kombiniert IT-Forensik ausgefeilte Technologie für die Analyse großer Datenmengen mit weitreichender forensischer Expertise. „Wir besitzen zwei forensische Labors, die mit entsprechender Such- und Analysetechnologie ausgestattet sind. Für papierbasiertes Datenmaterial bieten wir Komplettlösungen zur Digitalisierung. Dazu gehören auch hochsichere und vertrauliche Logistikdienstleistungen,



damit die Nachforschungen geheim bleiben. Die technologische Ausstattung für die schnelle Verarbeitung riesiger Datenvolumina ist allerdings nur die halbe Miete. Genauso wichtig ist es, zu wissen, wie Beweismittel zu sichern und ein gerichtskonformer Bericht zu erstellen sind“, so Galli.

Damit elektronische Daten als Beweis zugelassen werden, muss der IT-Forensiker beispielsweise gerichtskonforme Kopien der eingereichten Datenträger erstellen. Erst wenn die Informationen „eingefroren“, das heißt unveränderbar sind, erfolgen Datenextraktion und -indizierung. Über eine intelligente Suchmaschine kann das gesamte zur Verfügung stehende Datenmaterial einfach und gezielt durchsucht werden. Dies erfordert die enge Zusammenarbeit mit dem Kunden und dessen Anwalt. „Wir benötigen möglichst detaillierte Informationen über Verdachtsmomente und müssen zugleich wissen, wie diese aus juristischer Sicht am besten zu beweisen sind“, erläutert Galli. Die Suche nach Indizien erfolgt über Stichwörter. Die relevanten Resultate werden isoliert und chronologisch aneinander gereiht, um die Geschehnisse zu rekonstruieren. In diesem konkreten Fall hat die Analyse von Festplatten Schritt für Schritt weitere Verdächtige und im Endeffekt ein gründlich geplantes Komplott aufgedeckt. 90 Personen aus unterschiedlichen Ländern waren daran beteiligt und wie befürchtet auf dem besten Weg, Mitarbeiter und Kunden in ein ähnliches, international tätiges Unternehmen zu „transferieren“.

OSINT

Fakten, Fakten, Fakten. Das Gericht fordert lückenlose Darstellungen. Wenn Betrüger aus den internen Reihen nicht ausreichend Spuren hinterlassen oder diese erfolgreich beseitigen, aber auch um außen stehende Kriminelle zu überführen, empfehlen sich Recherchen in sogenannten OSINT-Quellen (Open Source Intelligence). „Open Source“ steht in diesem Fall für öffentlich zugängliche, meist kostenpflichtige Informationsquellen wie Zeitungen, Internet, Bücher, wissenschaftliche Magazine, Radiosendungen, Fernsehen oder Verzeichnisse. Der ad hoc Zugang für punktuelle Recherchen macht nur über Intermediäre wie Scalaris Sinn, die über fortlaufende Lizenzverträge mit den Datenbank Anbietern verfügen. Außerdem ist der clevere Einsatz von Suchtechnologie erforderlich, um die Abfragen zu verschleiern. Im beschriebenen Fall ergab die Abfrage von Computer und E-Mail Domain Registern beispielsweise, dass mancher Mitarbeiter ein Doppelleben führte und bereits für die neue Organisation tätig war.

Economic Crime Intelligence (ECI)



Dr. Andrea Galli

Head of Economic Crime Intelligence (ECI), Scalaris AG

Mehr als 15 Jahre Erfahrung als Information Business Consultant namhafter Unternehmen. Führender Open Source Intelligence Experte in Europa. Leiter der Economic Crime Intelligence Division der Scalaris AG.

