Datenbankgestützte Ermittlungen

Unternehmens-Intelligence gegen clevere Täter

Ergibt sich ein Betrugs- oder Diebstahls-Verdacht, stellt sich für die Ermittlungen auch die Frage, ob es sich dabei „lediglich" um einen Einzeltäter handelt oder ob dieser mit weiteren Tätern vernetzt ist. Und auch bei einem neuen Geschäftspartner kann sich die Frage nach dessen Seriosität stellen. Das Schadenspotential kann immer beträchtlich sein, da erfolgreiche "Geschäftsmodelle" nach dem Testen professionell und auch oft über längere Zeit unbemerkt umgesetzt werden. Zwar gibt es zur Betrugsbekämpfung interne Abteilungen, wie beispielsweise die Konzernsicherheit, die Loss Prevention oder die Brand Protection – nicht immer sind aber deren Recherchen und das Aufbereiten der Informationen untereinander koordiniert. Dazu ist der übergreifende Einsatz von „Intelligence"-Lösungen sinnvoll.

Von Jörn Weber, Mönchengladbach

Von einer hohen Zahl an Betrugs- oder Diebstahls-Delikten sind in erster Linie internationale Konzerne betroffen. Durch ihre verzweigte Struktur über viele Landesgrenzen hinweg bieten sie zahlreiche Angriffspunkte. Besonders Unternehmen aus den Hightech-Branchen, der Pharmaindustrie und Markenhersteller der Textilbranche sind geeignete Opfer. Sie bieten wertvolle und schwer nachzuahmende Produkte, die sich zudem gut transportieren und global verkaufen lassen. Aber auch größere Mittelständler können Opfer krimineller Netzwerke werden, wie beispielsweise branchenführende Zulieferer für die Autoindustrie. Denn auch solche „Hidden Champions" bieten gefragte Waren an. Gestohlene Produkte werden dann entweder im In- und Ausland verschoben oder auch im Internet angeboten – etwa über Auktionsmarktplätze, auf denen dann auffallend günstige Artikel angeboten werden.

Drei Fallbeispiele

1. Ein Techniker eines Serviceunternehmens erkannte, dass sich erfundene Garantie-Reparaturen über das System des Herstellers unbemerkt abrechnen lassen. Dadurch konnte er kostenfrei hochwertige IT-Hardware erhalten. Nach einer erfolgreichen „Testphase" nutzte er dann Adressen von weiteren Mitwissern als Lieferadresse und beteiligte diese an den Einnahmen. Die Zahl der erschlichenen Hardware-Komponenten lag schließlich pro Monat bei bis zu 300. Bis zur Aufdeckung erreichte der Schaden rund 350.000 €.

2. In einem Logistikunternehmen war es für Mitarbeiter einfach zu erkennen, auf welchen Paletten sich regelmäßig hochwertige Ware befand. Um in den Besitz dieser Palette zukommen, wurde diese zwar am Zielort angeliefert und vom System des Kunden gescannt – mit Hilfe bestochener Mitarbeiter des Kunden in der Warenannahme verließen die Paletten danach aber wieder das Gelände auf dem Lkw des Logistikunternehmens und wurden dann später auf die Fahrzeuge der Täter umgeladen.

3. Auch die Versicherungswirtschaft kann Opfer krimineller Netzwerke werden. Bekannt sind hier die Tätergruppen, die beispielsweise bei der bewussten Herbeiführung von Autounfällen die Kaskoversicherung schädigen. Die Versicherungen haben dabei das Problem, dass ihnen nur die Falldaten zu ihrem eigenen Fall bekannt sind, aber nicht zwingend auch die von einem identischen „Kunden", der auch andere Versicherungen schädigt.

Die Täter

Das Internet erschwert den Ermittlern dabei die Identifikation der Täter, die sich beispielsweise verschiedene Schein-Identitäten oder -Unternehmen samt Adressen und Webseiten zulegen. Deshalb reicht heute – zum Beispiel bei der Aufnahme neuer Geschäftsbeziehungen – eine einfache Überprüfung von nur den Finanzdaten des Geschäftspartners nicht mehr aus, um eine Entscheidung zur Zusammenarbeit zu treffen. Wichtig sind in einem solchen Fall weitere Informationen, wie etwa zu dessen Management, den Gesellschaftern sowie zur Reputation und bisherigen Kunden. Diese Recherche nennt sich üblicherweise „Due Diligence Investigation".

Die Netzwerke erkennen

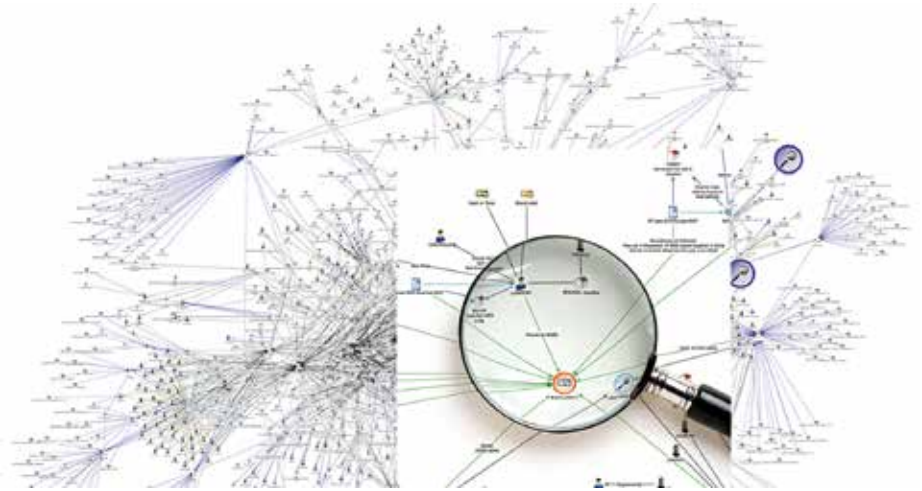
Wichtig für eine angemessene Reaktion im Verdachtsfall ist es, die Gefahr überhaupt einstufen zu können. Wenn sich bei einem Vorfall alle Recherchen lediglich auf eine vermutete Einzeltat beziehen, werden auch verhältnismäßig geringe Ressourcen für diesen Fall bereitgestellt. Ganz anders werden Unternehmen reagieren, die in der Lage sind, einen einzelnen Vorfall mit weiteren in Beziehung zu setzen. Sie werden den Fall völlig anders priorisieren, weil die vermuteten Verluste für das Unternehmen ungleich höher angesetzt werden. Ebenso wichtig ist es, die entstehenden Kosten für Ermittlungen richtig zu kanalisieren und die

Mittel zielgerichtet einzusetzen. Von Bedeutung ist das Erkennen eines Netzwerkes auch, weil die Strafverfolgung später aufgrund der höheren Relevanz des Falls konsequenter sein wird als bei einer Einzeltat.

Der Aufwand: Daten zentral pflegen

Um ein mögliches Täter-Netzwerk zu entdecken, sollten alle unternehmensweit relevanten Informationen zentral erfasst und gespeichert werden. In einer Datenbank können etwa alle fragwürdigen Vorfälle, Personen und Unternehmen sowie deren Beziehungen untereinander gesammelt werden. Oft existieren in Großkonzernen solche Datensammlungen in Sicherheits-, Markenschutz- oder Rechtsabteilungen, überwiegend allerdings dezentral. Wenn aber diese Informationen aktuell und abteilungsübergreifend gepflegt werden, können neue Angriffe bereits bekannten zugeordnet werden.

Dabei ist die Menge der heute öffentlich zugänglichen Informationen dank des Internets so groß, dass schon eine einzelne Suche bereits oft zu einer unübersichtlichen Masse an Informationen führt. Um diese unstrukturierten Daten möglichst zielorientiert nutzen und auch Abgleiche mit vorherigen Analysen oder vorhandenen Fallinformationen erstellen zu können, sollten sie in eine zentrale Intelligence-Plattform einfließen, wie beispielsweise in die IBM-Lösung i2 oder in die Palantir-Plattform. Allerdings: Trotz der Aussage der Hersteller, dass sich viele Datenbanken anbinden lassen und die Plattform damit eine automatisierte Enterprise-Lösung darstelle, stimmt dies nicht immer. Viele Informationen kommen aus Sicht des externen Analysten gar nicht aus internen Datenbanken des Kunden – vielmehr handelt es sich häufig um Berichte, exportierte Listen und andere Einzelinformationen. Diese müssen dann letztendlich manuell oder bestenfalls halbautomatisch in die Datenbank eingegeben werden. Dennoch: Der große Vorteil einer solchen Intelligence-Plattform ist, dass große Datenmengen aus vielfältigen Quellen schnell analysiert werden können. Auch komplexe Suchanfragen können gespeichert und jederzeit und automatisch wieder ausgeführt werden. Letztendlich erkennt der eingesetzte Intelligence Analyst durch die intensive Arbeit mit den Informationen auch wichtige Informationen und Zusammenhänge und kann so wertvolle Beiträge zur Fallklärung leisten.



Ob es sich bei einem erkannten Diebstahl nur um einen Einzeltäter oder um ein Netzwerk an Tätern handelt, lässt sich meist nur mit einer entsprechenden „Intelligence"-Software feststellen. *Bild: corma*

So ist es möglich mit einer unscharfen Sucharithmetik, wie beispielsweise einer 360°-Suche (die Suche in allen Feldern nach Dokumenten und Metadaten innerhalb der Datenbank) sogar Ähnlichkeiten in Informationsbruchstücken verschiedenster Formate und Darstellungsformen zu entdecken. Da diese Intelligence-Lösungen auch den Unicode-Zeichensatz unterstützen, lassen sich Daten auch in verschiedenen Sprachen gleichzeitig untersuchen. Diese

Tipps beim Planen einer Intelligence-Lösung

1. *Individuelles Design der Datenbank*
2. *Analyse der externen und internen Datenquellen auf Import- & Eingabemöglichkeiten*
3. *Enge Verzahnung von Ermittlern und Analysten (gleicher Sachverhaltsstand)*
4. *Ziele und Intelligence Produkte klar definieren*
5. *Trainierte Analysten und Anwender*

Tipps zum Layout einer Intelligence-Datenbank

1. *Sorgfältige Auswahl der relevanten Entitäten (Person, Firma, Adresse, IP Adresse, Fall, Social Network Profil)*
2. *Individuell festlegen, wie diese Entitäten durch Links verbunden werden (z.B. die Verlinkung der Adresse zu Person, Testkauf)*
3. *Importstrukturen definieren*
4. *Anzahl der Nutzer und Sicherheitseinschränkungen festlegen*
5. *Sorgfältige Dokumentation des Designs zu Verwendung im Workflow Training der Anwender*

Weiterführende Informationen auch unter http://blog.corma.de/intelligence-datenbanken-modell-einer-erfolgreichen-intelligence-analyse/

Funktion ist sehr wichtig, da Betrügereien oft über Ländergrenzen hinaus stattfinden und beispielsweise Firmennamen, Personennamen und Adressen immer auch in der Landessprache erfasst werden sollten.

Durch die strukturierte Datenerfassung nach dem „Entitäten-Link-Prinzip“ lassen sich dann Zusammenhänge sicher erkennen. Auf eine Abfrage hin werden etwa alle Webseiten angezeigt, die auf einer IP-Adresse laufen oder es werden Verbindungen zwischen unterschiedlichen Nutzern einer identischen E-Mail Adresse sichtbar. Diese Beziehungen lassen sich in anschaulichen Beziehungsdiagrammen darstellen und dann zielgerichtet auswerten. Auch kann eine einfache forensische Analyse der gesicherten öffentlichen Website-Daten und Dateien, wie beispielsweise Fotos mit GPS-Daten, bisher unbekannte Zusammenhänge zu vorhandenen Informationen hervorbringen. Die hierfür notwendige Toolbox des Analysten/Ermittlers geht dafür weit über das Bekannte hinaus und berührt dabei auch Werkzeuge von Forensikern, Penetration-Testing und Cyber-Security.

Letzten Endes gilt es dann alle „losen Enden“ zusammenzufügen, bis sich das Bild der Täter vervollständigt hat. Besonderes Augenmerk sollte auf alle Schnittstellen gelegt werden, an denen die Internetwelt in die reale übergeht. Beispielweise sind im Netz angegebene Firmendaten wie Adressen und Telefonnummern oder die Betreiber von Internetangeboten durch Recherchen vor Ort zu überprüfen.

Wichtig ist auch, dass die Analysen schnell vorgenommen und Beweise rechtssicher gesammelt werden, denn oftmals existieren fragwürdige Verkaufsangebote im Internet nur für wenige Tage oder Stunden. Vorgetäuschte Identitäten werden meist kurz nach dem Vorfall wieder aufgelöst.

Gesetzeslage

Die konsequente und vollständige Datenerfassung verdächtiger Personen, von Vorfällen und Unternehmen ist dabei unter umsetzbarer Berücksichtigung des Datenschutzes nicht nur erlaubt, sondern eigentlich eine Pflicht. Es gibt zwar keine eindeutige gesetzliche Verpflichtung, aber die Ausstrahlungswirkung von AktG, GmbHG, HGB, KontraG etc. sowie den für viele Unternehmen ja auch relevanten internationalen Bestimmungen wie FCPA, UK Bribery Act ist deutlich genug. Demnach hat die Geschäftsleitung letztlich die Pflicht, erforderliche, zumutbare und angemessene Maßnahmen zu ergreifen, um drohende Schäden (frühzeitig) zu erkennen und abzuwenden.

Ergebnisse

Die Ergebnisse lassen sich vielfältig verwenden: So können die Informationen aus einer Intelligence-Lösung die Rechtsabteilung bei zivil- und strafrechtlichen Auseinandersetzungen unterstützen. Auch können die gewonnenen Informationen (insbesondere neue unbekannte Verbindungen) vor allem die Ermittler und deren Arbeit gezielt voranbringen. In der englischen Sprache wird hier oft von „Actionable Results“ gesprochen. Gemeint ist damit die fertig aufbereitete Darstellung des Falles, die dann den Strafverfolgungsbehörden „auf dem Silbertablett“ präsentiert werden kann. Eine durchdachte Investition in eine solche Lösung unterstützt damit die Konzernsicherheit direkt beim Schutz der Unternehmenswerte. Wichtig ist aber eine maßgeschneiderte Lösung, die die Bedürfnisse des Kunden passgenau erfüllt und keine universelle „out-of-the box“ Lösung. Hier gilt auch, dass je professioneller die Ermittlungen geführt werden, auch die Chancen steigen, dass ein Unternehmen wieder in den Besitz der entwendeten Produkte gelangt.

Fazit

Die veränderte Intelligenz der Täter macht es erforderlich, dass auch der Ermittler sein Wissen und sein Vorgehen auf die Bereiche wie etwa Marktplätze im Internet, anonyme Internetseiten, digitale Beweissicherung (auch von online festgestellten Informationen), strukturierte Internetrecherche und das gezielte Überwachen auf neue Fundstellen anpasst. Dazu muss im Unternehmen eine Vorgehensweise erstellt werden, mit der die relevanten Fakten abgefragt werden können. Dazu gehört Hintergrundwissen über mögliche Täter, mögliche Absatzkanäle der erlangten Ware oder auch das Monitoring der regulären Verkaufskanäle der Produkte des Unternehmens.

Wenn das Unternehmen nicht über eine Konzernsicherheit verfügt, so sollte die Geschäftsführung sich Gedanken darüber machen, welche externen Ermittler qualifiziert und zuverlässig unterstützen können. Idealerweise werden diese Ermittler in einem Rahmenvertrag mit Datenschutzvereinbarung, Service Level Agreement und einer Vertraulichkeitserklärung schon vor dem Ernstfall eingebunden. Das verpflichtet in der Regel zu nichts, erleichtert aber die schnelle Umsetzung von Ermittlungsmaßnahmen.

Über unseren Autor:

Jörn Weber ist ehemaliger Kriminalhauptkommissar und heute Geschäftsführer der corma GmbH, Mönchengladbach. Das Unternehmen berät Kunden bei der Prävention von Betrugsdelikten und bei der Aufklärung komplexer sowie häufig länderübergreifender Fälle von Wirtschaftskriminalität.
Kontakt: jw@corma.de