Ontrack® Forensics

Computer Forensik

Gerichtsverwertbare Analyse digitaler Spuren in der Wirtschafts- und Computerkriminalität.

- Datenmissbrauch
- Industriespionage
- Datendiebstahl
- Bilanzfälschung
- Vorsätzliche Datenlöschung
- Veruntreuung

In vielen Strafprozessen werden elektronische Beweismittel immer relevanter. IT-kundige Straftäter nutzen den Fortschritt in der Informationstechnologie, um alte Straftaten mit modernen Mitteln zu begehen. Der PC wird zum Tatwerkzeug!

Sehr geehrte Kunden,

In den letzten zwei Jahren wurde international nahezu jedes zweite Unternehmen Opfer eines Wirtschaftsdeliktes. Keine Branche blieb von Wirtschaftskriminalität verschont. Handel, Telekommunikation und der Finanzsektor stehen an der Spitze der betroffenen Sparten. Trotzdem halten 55% der deutschen Unternehmen es für unwahrscheinlich, dass sie in den nächsten fünf Jahren selbst Opfer einer Wirtschaftsstraftat werden.

Immerhin rund ein Viertel aller Täter stammen aus der eigenen Führungsetage.
Die Risikolage wird zu selten realistisch eingeschätzt – was dazu führt, dass die Investitionsbereitschaft und das Engagement zur Prävention sehr gering ist.

Daraus lässt sich ableiten, dass sich ein steigender Bedarf an Aufklärungsarbeit für Ermittler und – mit der steigenden Bedeutung elektronischer Daten – auch für Computer Forensik-Spezialisten ergibt.

In den meisten europäischen Ländern existieren allerdings strenge Datenschutzgesetze, die eine deutlich wahrnehmbare Hürde bezüglich Früherkennung und Aufklärung von unternehmens-internen Wirtschaftsstraftaten darstellen. Bei Ermittlungen müssen z. B. relevante Daten der betreffenden Personen schon vor Ort oder im Inland (Kroll Ontrack Labor) selektiert und extrahiert werden, bevor sie – auf Anforderung US-Amerikanischer Anwälte oder der Securities and Exchange Commission (SEC) – in die USA geschickt werden dürfen. Es besteht allgemein Verunsicherung in der Auslegung bzw. Anwendung der Datenschutz- und Telekommunikationsgesetze.

Kroll Ontrack hat sich in den letzten Jahren weltweit von einem Datenrettungs-Dienstleister zu einem der führenden Anbieter von Computer Forensik und Electronic Discovery etabliert. Mit der weltweiten Präsenz und technologisch modernst ausgestatteten Labors bietet Kroll Ontrack Global Playern aus Industrie, aber auch lokalen Unternehmen, optimale Voraussetzungen für diskrete, gerichtsverwertbare Beweisermittlungen in allen Fällen von Wirtschaftskriminalität.

Unsere Prioritäten sind auch die der Unternehmer:
- Früherkennung, diskrete Ermittlungen und Untersuchungen schon bei einem Anfangsverdacht
- Schadensbegrenzung
- Aufklärung des Tatbestandes
- Wiedergutmachung

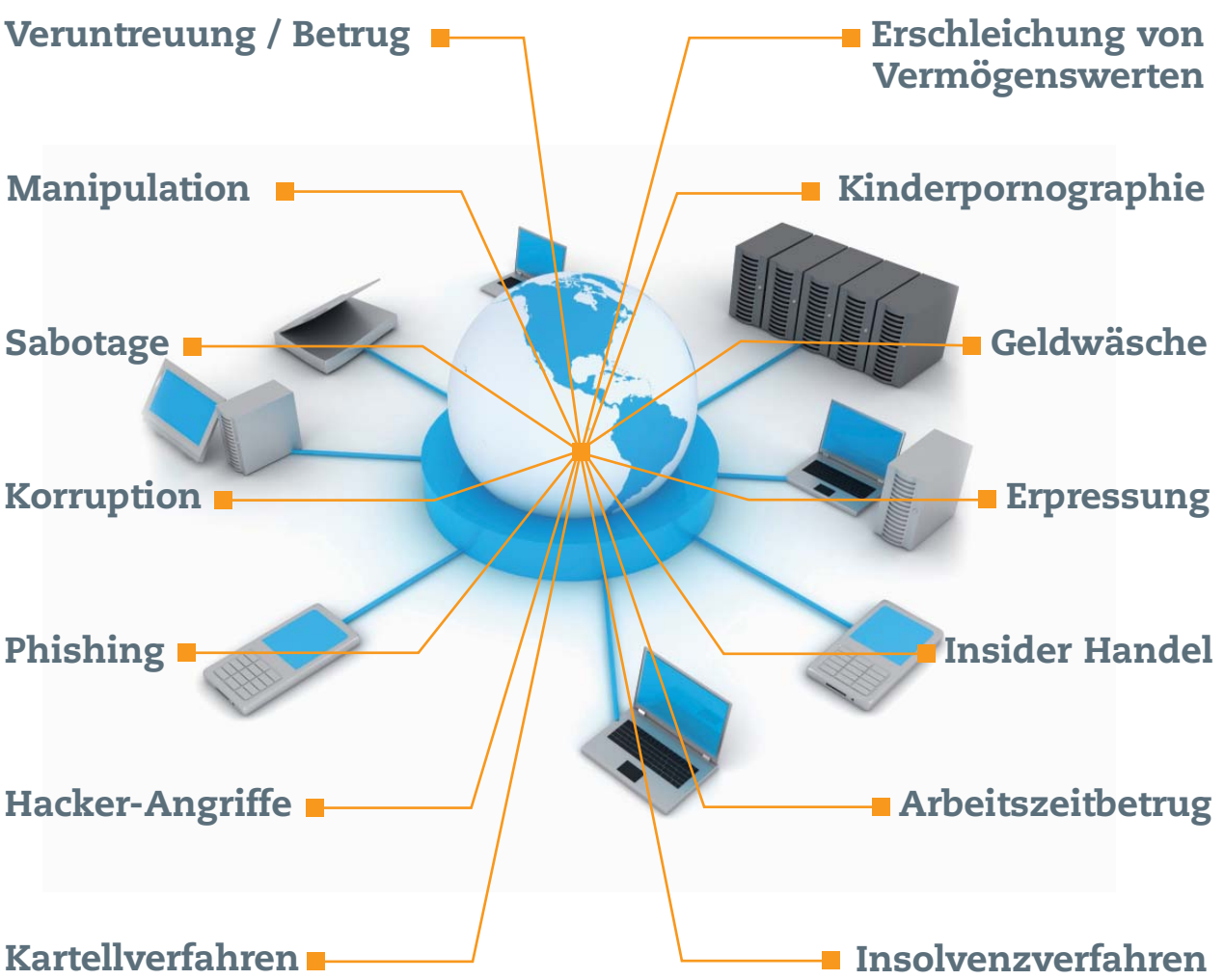
Ihr Reinhold Kern

Director Computer Forensik
Kroll Ontrack GmbH

Die Welt ist digital...

Noch nie war das Wohl moderner Unternehmen so stark abhängig von einer funktionierenden und sicheren IT-Landschaft wie heute! Von E-Mail-Kommunikation bis zu ganzen Warenwirtschaftssystemen – alle diese Daten sind ausschließlich elektronisch gespeichert. Aber wie sieht es mit der Sicherheit aus – sind die kritischen Daten sicher vor unbefugtem Zugriff oder Manipulation?

> **Eine neue Generation IT-kundiger Straftäter nutzt den Fortschritt der Informationstechnologie, um alte Straftaten mit neuen Mitteln zu begehen.**
>
> Reinhold Kern, Director Computer Forensik



Wirtschaftskriminalität - die Täter und ihre Motive

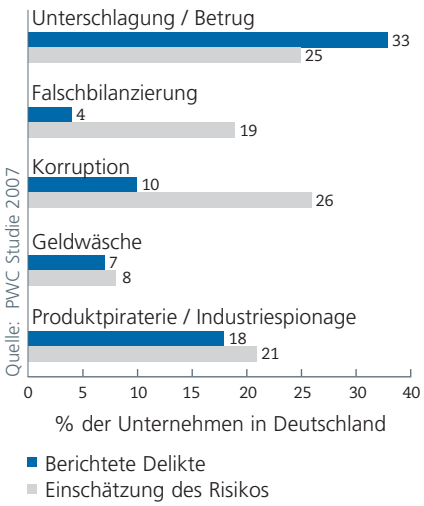
Wirtschaftskriminalität hat viele Gesichter
Nationale und internationale Studien bestätigen, dass 60-80% aller Wirtschaftstaten von so genannten Innentätern – eigenen Mitarbeitern und Ex-Mitarbeitern – begangen werden. Wobei offiziellen Schätzungen zufolge lediglich ca. 20% zu einer Strafanzeige führen – die Angst vor einem öffentlichen Image- oder Reputationsschaden ist bei vielen Unternehmen zu groß.

Aus unzufriedenen Mitarbeitern können Täter werden. Hemmschwellen, eine Straftat zu begehen sinken bei:

- Unzufriedenheit im Unternehmen
- privaten Problemen
- finanziellen Problemen
- unangemessenem Lebensstandard

Nur jedes fünfte Unternehmen schätzt die Risikolage realistisch ein, was im Endeffekt zu geringerer Investitionsbereitschaft und zu wenig Engagement zur Prävention führt.

Risikoeinschätzung und reale Opferzahl nach Delikten in Deutschland

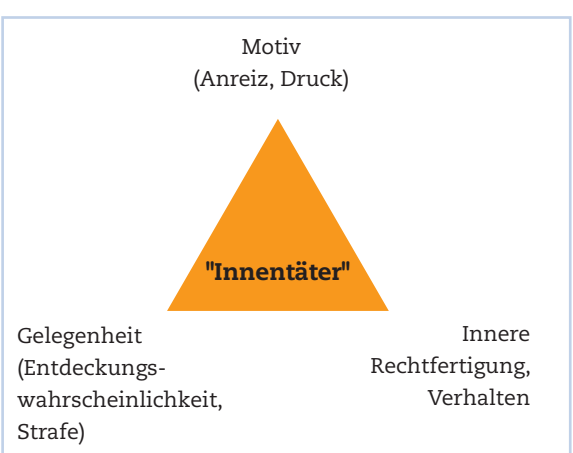


Top Management Fraud:
Täter aus der Führungsetage
Das Phänomen Top-Management-Fraud ist in der jüngsten Vergangenheit immer wieder Gegenstand öffentlicher Berichterstattung geworden. Immerhin 30% aller Delikte – spektakuläre Betrugsfälle auf nationaler und internationaler Ebene – werden von Tätern aus dem Top-Management verübt.

Ursachen hierfür können sein:
- mangelndes Unrechtsbewusstsein
- leichte Verführbarkeit
- Gier nach Macht und Geld
- Management Override

Über 60% aller unternehmensinternen Delikte werden überhaupt erst durch Tippgeber bekannt.

Täterindividuelle Faktoren: "The Fraud Triangle"



Vom Verdacht zum Beweis - die richtige Vorgehensweise.

Wie auch immer ein Verdacht auf eine unternehmensschädigende Tat zustande gekommen ist, Sie entscheiden über die darauf folgenden Schritte:

Es stellt sich in jedem Fall die Frage, ob eine Strafanzeige angestrebt oder lieber auf eigene Ermittlungen zurückgegriffen werden soll, um den bestehenden Verdacht zu erhärten.

Wichtig ist die schnelle Schadensbegrenzung und die Aufklärung - über die Möglichkeiten einer Sanktionierung oder Wiedergutmachung können Sie später entscheiden.

Die Vorteile eines unabhängigen Ermittlers liegen auf der Hand. Während bei einer behördlichen Strafverfolgung ganz klar die Ermittlung des Täters und dessen Sanktionierung im Vordergrund stehen, liegt im Gegensatz dazu bei internen Ermittlungen der Fokus auf Diskretion, Schadensbegrenzung und Wiedergutmachung.

Wenn Sie sich für eigene Ermittlungen entscheiden ist es wichtig, folgendes zu berücksichtigen:

Gibt es eine Betriebsvereinbarung, die die private Nutzung von Internet und E-Mail regelt?

- Datenschutzbestimmungen beachten.
- Niemals an Original-Speichermedien direkt untersuchen. Beweiskraft von Dokumenten könnte vernichtet werden.
- Sicherstellung des aktuellen relevanten Datenbestandes.
- Sogenannte elektronische Beweise sind keine Urkundenbeweise sondern Augenscheinbeweise.

-> daher ist es besonders wichtig, die Integrität, die Glaubwürdigkeit sowie die Lückenlosigkeit der Beweiskette zu gewährleisten.

Strafverfolgungsbehörde	Eigenermittlung
Priorität: ■ Aufkärung und Sanktionierung	**Priorität**: ■ Schadensbegrenzung ■ Aufklärung / Wiedergutmachung ■ Ruhe bewahren
Risiko: ■ öffentliches Bekanntwerden des Falles ■ Image-/Reputationsschaden ■ Polizei übernimmt und bestimmt ■ erhöhte Unruhe durch Verhöre ■ interner Vertrauensverlust	**Risiko**: ■ Datenschutzgesetze ■ Interne Interessenkonflikte ■ Glaubwürdigkeit ■ Beweiskraft

“ **Seit Jahren unterstützt Kroll Ontrack Unternehmen, deren Anwälte und auch Strafverfolgungsbehörden bei der Aufklärung von Wirtschaftsstraftaten.** Reinhold Kern, Director Computer Forensik

Was ist Computer Forensik?

Unter Computer Forensik versteht man die gerichtsverwertbare Erfassung und Analyse elektronischer Daten sowie die Erstellung eines, auch für einen Nicht-IT-Experten, verständlichen Berichts, der auch zur Vorlage bei Gericht geeignet ist.

Elektronische Spurensuche
Heute lassen sich die relevanten Beweise vor allen Dingen in den Datenspeichern von Computern finden. Unsere Spezialisten untersuchen dazu alle Speichermedien auch von mobilen Geräte: Festplatten, RAID-Systeme, Backup-Bänder, PDAs, Handys, USB-Sticks, Flash-Cards, DVDs, etc.

Gerichtsverwertbare Beweise
Alle Aktivitäten am PC hinterlassen Spuren, die nur bei forensischer Sicherstellung und professioneller Vorgehensweise vor Gericht als Beweismittel standhalten.

Für die effiziente Suche nach relevanten Beweisen und wertvollen Hinweisen können nicht nur gelöschte Dateien und Dokumente wiederhergestellt werden, es können auch Dateifragmente in nicht aktiven oder ungenutzten Festplattenbereichen ausgelesen werden.

Computer Forensik Experten entgeht nichts
Schlagkräftige Beweise finden sich häufig auch in versteckten, versehentlich oder mutwillig gelöschten, passwortgeschützten oder verschlüsselten Daten.

> **„Kein Anwalt, der für sich in Anspruch nimmt, seine Mandanten engagiert zu vertreten, kann es sich leisten, wichtige elektronische Beweismittel außer Acht zu lassen, die sich im Büroschrank nicht finden lassen!“**
>
> **RA Hans-Peter Herrmann**

WER hat WAS, WIE, WANN getan?

- Wer hatte offiziell Zugriff auf die Daten?
- Welche Dateien und Informationen wurden von wem und wann zuletzt genutzt?
- Von wem wurden Daten wohin (USB-Stick, CD ROM, DVD, externe Festplatte, ...) kopiert?
- Gibt es unauthorisierte Zugriffe? (Hacker von Außen und Innen, Passwort Cracker Software)
- Welche Internetseiten wurden besucht?

Alle diese Fragen können unsere Experten nach Analyse des Datenmaterials beantworten.

Kroll Ontrack unterstützt Sie weltweit:

- Beratung zur Vorbereitung und Durchführung
- Erfassung und Aufbereitung global verteilter Daten auch aus unterschiedlichen IT-Plattformen
- Aufbereitung der Daten unter Berücksichtigung der lokalen Datenschutzbestimmungen
- Extrahierung, Filterung und De-Duplizierung der relevanten Daten zur Reduzierung der Gesamt-Datenmenge
- Suche nach relevanten Dokumenten z.B. nach Schlagwörtern
- Erstellung gerichtsverwertbarer Berichte
- Expertenzeuge

In vielen Fällen von Unternehmensübernahmen oder Fusionen bis hin zu rechtlichen Auseinandersetzungen (Straf- oder Zivilrecht) müssen auch elektronische Dokumente abgerufen und zur Prüfung vorgelegt werden! Stichwort: Electronic Discovery

Empfehlungen für eigene Ermittlungen

Vorbereitung und Prävention:

Notfallteam
Stellen Sie ein Team aus den unterschiedlichsten Bereichen – IT, Recht, Betriebsrat, Datenschutzbeauftragter, Management - zusammen, das über die weitere Vorgehensweise bestimmt.

Notfallplan erstellen
Erstellen Sie eine Eskalationsprozedur
– wer muss intern informiert werden
– wer nimmt anonyme oder offizielle Hinweise entgegen
– wer könnte Sie bei einem Vorfall unterstützen, z. B. ein externer Anwalt oder Dienstleister

Datenschutz - Betriebsvereinbarung
Treffen Sie mit Ihren Mitarbeitern eine Betriebsvereinbarung, die die private Nutzung von E-Mail und Internet regelt.

Datenverfügbarkeit
Sorgen Sie dafür, dass Ihre Daten jederzeit in lesbarer Form zur Verfügung stehen.

Im Ernstfall

Ruhe bewahren
Tätigen Sie keine übereilten Handlungen.

Notfallplan berücksichtigen
Arbeiten Sie den Notfallplan gewissenhaft ab, im besten Fall externe Berater schon in der Vorphase einbeziehen.

Beweiskraft erhalten
Die Integrität der Daten muss absolut erhalten bleiben. Niemals Originalmedien z.B. PCs bzw. Festplatten verdächtigter Mitarbeiter direkt untersuchen! Immer erst eine forensische 1:1 Kopie erstellen lassen. Alle Arbeitsschritte müssen zur Erhaltung der Chain of Custody exakt dokumentiert werden und Ergebnisse nachvollziehbar sein.

Interessenskonflikte vermeiden
Welcher Mitarbeiter untersucht wen oder was - kollegiale Beziehungen beachten!

Glaubwürdigkeit
Durch den Einsatz externer, anerkannter, neutraler und objektiver Experten erhöht sich die Glaubwürdigkeit vor Gericht.

Computer Forensik-Prozess

Die Durchführung einer forensischen Untersuchung erfolgt in genau festgelegten Schritten, um eine vollständige Kontrolle, lückenlose Dokumentation und umfassende Beweissicherung zu gewährleisten. Wir unterstützen Sie während des gesamten Prozesses.

Beratung

Unsere Forensik-Projektmanager erarbeiten gemeinsam mit Ihnen eine effiziente Strategie für die Abfrage, Analyse und Aufbereitung der Daten. Zuerst muss geklärt werden, in welchen Datenspeichern relevante Hinweise, Spuren oder Beweise zu finden sein könnten. Auch Server und LogFiles des Netzwerkverkehrs enthalten oftmals wichtige Informationen.

Gerichtstaugliche Datenerfassung

Um eine gerichtsverwertbare Ausgangssituation zu ermöglichen, muss ein bitgenaues 1:1 Image erstellt werden, bei dem jedes einzelne Bit bzw. jeder Sektor miterfasst wird. Für dieses Abbild wird eine eindeutige Prüfsumme (MD5 Hash-Wert) errechnet, die eine eventuelle Manipulation der Daten auf einen Blick feststellbar macht.

Wiederherstellung gelöschter Dateien

Mit speziellen Software-Tools und entsprechendem Fachwissen lassen sich aus dem Image sowohl gelöschte Dateien, als auch Dateireste wieder rekonstruieren. Computer Forensik-Experten ermitteln, ob Computerbeweismittel gefälscht, verändert oder gelöscht wurden. Auch der Inhalt von Dateiresten kann auf andere oder neue Indizien hinweisen.

Analyse und Datenschutz

Da das erfasste Datenvolumen meist sehr hoch ist, und bei Weitem nicht alles für den konkreten Fall von Relevanz ist, wird versucht, die Datenmenge nach bestimmten Kriterien (Zeiträume, relevante Personen, Eliminierung von Redundanzen) einzugrenzen.

Dokumentation, Berichterstattung und Expertenzeuge

Während des ganzen Prozesses muss eine lückenlose Dokumentation des Arbeitsablaufes angefertigt werden, da im Hinblick auf die spätere Gerichtsverwertbarkeit eine hohe Qualitätsanforderung an die Beweismittel besteht. Jeder einzelne Arbeitsschritt wird in speziellen Formularen festgehalten, um später problemlos nachvollzogen werden zu können. Unsere Experten sind jederzeit dazu bereit, bei Bedarf als Expertenzeuge vor Gericht auszusagen.

Rückgabemedien

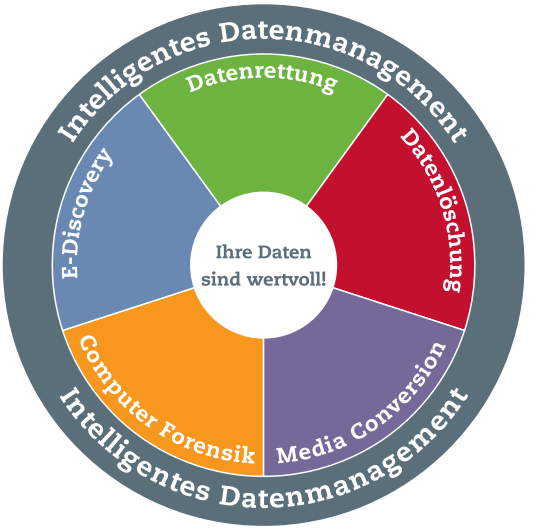
Die gefundenen relevanten Daten und Ergebnisse werden auf einem Medium (externe USB-Festplatte) oder auch in Papierform zurückgegeben. Außerdem gibt Kroll Ontrack Ihnen eine Software an die Hand, mit welcher die Daten weiter untersucht und analysiert werden können.

[1)] Informationen zum Datenschutz erteilt das Bundesamt für Sicherheit in der Informationstechnik: www.bsi.de

Kroll Ontrack bietet intelligentes Datenmanagement.

Kroll Ontrack ist führender Anbieter von Dienstleistungen in den Bereichen Datenrettung, -löschung, -konvertierung und Computer Forensik. In Deutschland ist die Kroll Ontrack GmbH mit 70 Mitarbeitern seit 1996 in Böblingen vertreten. International bietet das Unternehmen seine Dienstleistungen in 22 Ländern und 15 Sprachen an.

Zuverlässige Datenrettung
Bei der professionellen Datenrettung in Labor und Reinraum gibt es meist nur einen Versuch, die Daten wieder herzustellen. Unsere Datenrettungs-Experten machen Daten von allen Speichermedien und Betriebssystemen wieder zugänglich. Weltweit kann Kroll Ontrack auf jährlich mehr als 50.000 erfolgreiche Datenrettungen verweisen.



Endgültige Datenlöschung
Das sichere Löschen sensibler unternehmensinterner Informationen gewinnt auch im Hinblick der Einhaltung von Unternehmensrichtlinien und Gesetzen stetig an Bedeutung. Für die unterschiedlichen Ansprüche von Behörden und Unternehmen bietet Kroll Ontrack die Möglichkeiten der Datenlöschung per Hardware (Degausser DG.02), Software oder als individuellen Service im Labor.

Sichere Daten- und Medienkonvertierung
Der Begriff Konvertierung bezeichnet im Allgemeinen die Überführung einer Datei von einem Dateiformat in ein anderes. Das gilt für den Transfer von Daten zwischen unterschiedlichen Medien und Dateisystemen ebenso, wie für die Übertragung von Daten von einem Speichermedium auf ein anderes. Unsere Experten übertragen sogar Daten von längst veralteten auf moderne Medien (z. B. Backup-Systeme).

Computer Forensik
Die Wiederherstellung und Sicherung elektronischer Daten, die Recherche und Analyse von Indizien, die in digitaler Form vorliegen, sowie ihre gerichtsfeste Dokumentation, ist Fokus der Computer Forensik. Schon kleinste Fehler können zur Vernichtung von elektronischen Spuren führen, deswegen ist eine professionelle Vorgehensweise von Anfang an unabdingbar, so dass die gefundenen Dokumente als Beweismittel auch vor Gericht standhalten.

Electronic Discovery
E-Discovery ist der Prozess, angeforderte Unternehmensdaten gerichtsverwertbar zu erfassen, aufzubereiten und zu analysieren. Wenn große Datenmengen von mehreren involvierten Juristen, Revisoren oder Ermittlern an unterschiedlichen Standorten analysiert werden sollen, ist der Zeit- und damit auch der Kostenaufwand meist sehr hoch. Aufgrund der Standortproblematik und der verschiedenen beteiligten Analysten ist oft auch der Kommunikationsaustausch nicht optimal - Electronic Discovery ist hier die richtige Lösung.

Kroll Ontrack GmbH
Hanns-Klemm-Str. 5
71034 Böblingen
Fon +49 (0)7031/644-277
Fax +49 (0)7031/644-125

forensik@krollontrack.de
www.krollontrack.de

KROLL ONTRACK®

Vertrauen Sie auf die Besten.