

Ontrack® Forensics



# Whitepaper Forensik

KROLL ONTRACK®

Vertrauen Sie auf die Besten.

## Inhaltsverzeichnis

---

<b>Elektronische Beweismittelsicherung auf der Basis von Computer Forensik</b>	<b>2</b>
<b>Einführung: Daten und Datenmissbrauch</b>	<b>3</b>
Statistische Bewertung	4
<b>Aufgabenbereiche der Computer Forensik</b>	<b>6</b>
Wer den Schaden hat	7
Flexible Daten	9
Alles was Recht ist	11
<b>Vorgehen der Computer Forensik</b>	<b>13</b>
Erste Schritte	13
Protokollierung	14
Sicherung der Daten	15
Wiederherstellung der Daten	15
Eingrenzung des Datenmaterials	16
<b>Prozessablauf</b>	<b>19</b>

## Elektronische Beweismittelsicherung auf der Basis von Computer Forensik

### Hände hoch! Sofortmaßnahmen bei Verdacht.

Wenn Sie den Verdacht haben, dass in das Netz Ihres Unternehmens eingebrochen wurde oder aus dem Netzwerk unberechtigter Weise Daten nach außen übertragen wurden oder andere interne oder externe schädigende und kriminelle Eingriffe auf ihre Computer stattfinden, dann:

- Bewahren Sie Ruhe.
- Sondieren Sie die Lage.
- Vermeiden Sie übereilte, hektisch und nicht durchdachte Aktionen. Der Schaden, den Sie spontan anrichten können, ist nicht abzusehen!
- Nehmen Sie alle Aktionen im Beisein von Zeugen vor, die später bezeugen können, dass keine Daten verändernden Eingriffe vorgenommen wurden.
- Verschießen Sie den Raum, in dem sich der oder die verdächtigen Rechner befinden, so dass auch im Weiteren keine Manipulationen vorgenommen werden können.
- Belassen Sie die Geräte, die untersucht werden sollen, unbedingt im aktuellen Zustand.
- Ausgeschaltete Geräte bleiben ausgeschaltet.
- Eingeschaltete Geräte bleiben eingeschaltet und werden – wenn nötig – vom Netzwerk getrennt, beispielsweise durch Entfernen des entsprechenden Patchkabels oder durch Entfernen der W-LAN-Karte.
- Stellen Sie mit Administratoren und Verantwortlichen einen detaillierten Plan auf, der die aktuellen Gegebenheiten berücksichtigt und festlegt, wie bei der Beweissicherung vorgegangen werden soll.

Die Experten von Kroll Ontrack haben die Erfahrung gemacht, dass ein sehr hoher Prozentsatz der Beweiskraft elektronischer Medien in den ersten 30 Minuten verloren geht durch falsche Behandlung der Daten und Geräte und falsche Einschätzung beziehungsweise Nicht-Erkennen der Situation. Da sich lediglich vermuten lässt, worum es sich bei den so vernichteten Indizien handeln könnte – beispielsweise Anzeige des Bildschirms oder die flüchtigen Informationen, die sich aus dem Inhalt des Arbeitsspeichers ergeben können – schweigen sich Statistiken über die Höhe des durch Unwissenheit und fehlende Professionalität verursachten Schaden aus.

Bedenken Sie, dass sichergestellte Rechner und Datenspeicher später oft die einzigen verfügbaren Indizien beinhalten. Nur mit Hilfe der Computer Forensik können Sie im Zweifelsfall die entscheidenden Beweise sichern. Sofern Sie keine Erfahrung auf dem Gebiet der Computer Forensik haben, wenden Sie sich unbedingt zur Beratung und weiteren Planung an ein Fachunternehmen:

#### **Kroll Ontrack GmbH**

Hanns-Klemm-Straße 5

71034 Böblingen

Germany

**Telefon:** +49 (0)7031/644-0

**Fax:** +49 (0)7031/644-100

**E-Mail:** [info@krollontrack.de](mailto:info@krollontrack.de)

**Internet:** [www.krollontrack.de](http://www.krollontrack.de)

## Einführung: Daten und Datenmissbrauch

*„Die Bedeutung des PC im gesellschaftlichen Leben hat sich zur Kulturtechnik entwickelt, so dass wir mit Recht von einer neuen Epoche in der Entwicklung der Menschheit reden können. Die eigentliche innovative Kraft hat die Software, gerade im Bereich der geistigen Arbeit. Die heutige Komplexität wäre ohne diese Revolution nicht möglich geworden. Die Kehrseite sind die Sicherheitsprobleme: Die Zunahme von Cybercrime macht mir Sorgen.“*

**Otto Schily, ehemaliger Bundesminister des Inneren**

Mit diesen Worten würdigte Otto Schily anlässlich des 20. Jahrestags der Gründung von Microsoft einerseits die rasante Entwicklung des PC und seiner Möglichkeiten, warnte aber andererseits gleichzeitig vor den Risiken. Das Speichern und Abrufen allzeit verfügbarer Informationen, das Aufbewahren und Übermitteln von Daten in Sekundenschnelle, dies macht unsere Kultur und Wirtschaft in einer Weise effizient und schafft assoziative und logische Verbindungen über alle Grenzen hinweg.

Mit dem Gewicht, dass der Computer in unserem Zeitalter „gerade im Bereich der geistigen Arbeit“ gewonnen hat, etablierte er sich gleichzeitig als neue Plattform der Kriminalität, nicht zuletzt des Diebstahls geistigen Eigentums und der Verletzung von Urheberrechten, Copyright und vor allem Patenten. Da ein System keinen direkten Einblick in das bietet, was mit ihm getan wurde, erscheinen solche kriminellen Aktivitäten leicht verschleierbar und schwer nachzuvollziehen. Und doch gibt es zahlreiche Spuren, die sich bei genauer Betrachtung vor allem auf seinen Datenträgern finden lassen. Diese Indizien zu lokalisieren, zu konservieren und zu analysieren ist Aufgabe der Computer Forensik.

### **Gefahren erkennen, Fehler vermeiden**

Nur wer weiß, wo die Gefahren liegen und dass er sie nicht schutzlos und schicksalsergeben akzeptieren muss, kann Fehler vermeiden.

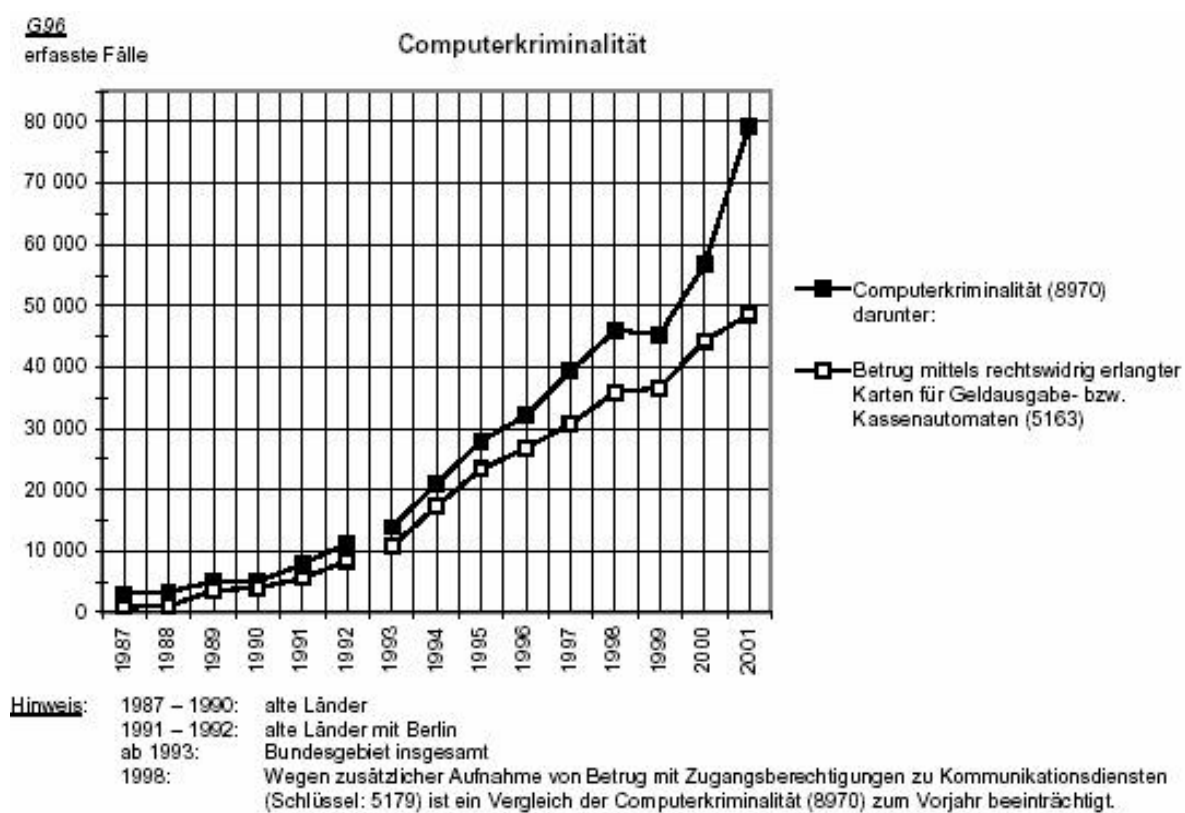
Gerade unter dem Gesichtspunkt, dass aus einem anscheinend kleinen Vorfall ein großes Delikt werden kann, ist umfassende Information als erste Vorsichtsmaßnahme gar nicht hoch genug einzuschätzen. Mit der Kenntnis der Gefahren und Schäden, dem Wissen, um die Möglichkeiten der Prophylaxe und Verfolgung, und dem Bewusstsein, dass die Weichen für viele Schritte rechtzeitig und zielgerichtet gestellt werden müssen, können zwar längst nicht alle Angriffe im Vorfeld abgewehrt, wohl aber rasch eingegrenzt und gezielt ermittelt werden. Nach einem Angriff oder unberechtigten Zugriff auf die Daten eines Computers oder einer Verletzung der Integrität des Firmennetzes erweist sich die Computer Forensik als die vorrangige Maßnahme der Schadenbegrenzung und Täterermittlung.

Computer Forensik ist das zentrale Element für seriöse Beweissicherung und fundierte Analyse des verfügbaren Materials, und der Computer Forensik Experte ist der kompetente Partner im Kampf gegen die Zunahme und das Ausufern von Cybercrime im meist vertraulichen Rahmen des Unternehmens.

Die Chancen, die durch digitale Techniken entstehen, beinhalten für alle von uns auch die Pflicht, uns Ihre Gefahren und Gefährdungen bewusst zu machen und geeignete Maßnahmen zu ergreifen, um geistiges Eigentum auch auf digitaler Ebene gegen Verfälschung, Diebstahl, Spionage und Sabotage zu schützen.

## Statistische Bewertung

Die starke Wachstumsrate der Computerkriminalität – laut BKA 39,8 Prozent von 2000 auf 2001– und die hohe Dunkelziffer macht die Computer Forensik als Instrument der Wiedergewinnung beweiskräftiger Daten und der Identifikation von Beweismaterial auf Computersystemen zum zentralen Ermittlungs-instrument. Zur Sicherung rechtserheblicher Daten sind neben der genauen Kenntnis von Hard- und Software festgelegte Sicherungsstrategien und -techniken unerlässlich. Nur die umsichtige, kriminalistisch korrekte Begutachtung am Tatort, forensische Untersuchung geeigneter Originalkopien oder Images der Datenträger und durchgängige Protokollierung führen zu einem beweiskräftigen Resultat.



Quelle: Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, PKS Berichtsjahr 2001, Bundeskriminalamt Wiesbaden, Seite 242 unter <http://www.bka.de/pks/pks2001/index2.html>

Das rasante Wachstum der Computerkriminalität dokumentiert die Kriminalstatistik, die allein von 2000 auf 2001 eine Zunahme der relevanten, erfassten Fälle um 39,8 Prozent auf 79.283 verzeichnet. Dabei entfielen auf den Computerbetrug (rechtswidrigen Vermögensvorteil durch Datenmanipulation) mit 17 310 Fällen beinahe dreimal so viele Fälle wie im Vorjahr (2000: 6 600 Fälle). Doch auch die Datenspionage liegt mit 1.463 Fällen im Vergleich zum Vorjahr (2000: 538 Fälle) ähnlich hoch. Die Computersabotage hat mit 862 Fällen einen Zuwachs von über 50 Prozent (2000: 513 Fälle). Auch andere Delikte, wie Fälschung, Täuschung und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten liegen bei Zuwächsen weit jenseits der 100 Prozentmarke. Lediglich bei der Software-piraterie ist ein leichter Rückgang zu verzeichnen.

Fallentwicklung und Aufklärung (Tabelle 01)

Bereich: Bundesgebiet insgesamt

T232

Schlüssel	Straftaten(gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2001	2000	absolut	in %	2001	2000
3970	Computerkriminalität	79 283	56 684	x <sup>1)</sup>	x <sup>1)</sup>	56,8	48,0
	davon:						
5163	Beitrag mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassensautomaten	48 610	44 284	4 326	9,8	41,7	41,8
5175	Computerbetrug -§263a StGB-	17 310	6 600	10 710	162,3	77,9	67,0
5179	Beitrag mit Zugangsberechtigungen zu Kommunikationsdiensten	8 039	2 198	5 841	265,7	84,2	81,5
5430	Fälschung beweismittelbarer Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	920	268	652	243,3	95,8	90,3
6742	Datenveränderung, Computersabotage -§§ 303a, 303b StGB-	862	513	349	68,0	45,4	52,6
6780	Ausspähen von Daten	1 463	538	925	171,9	82,6	46,1
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	1 672	1 361	311	22,9	99,2	97,3
7152	Softwarepiraterie in Form gewerbetätigen Handelns	410	937	-527	-56,2	96,1	99,6

<sup>1)</sup> Durch einen Zurechnungsfehler ist die Fallzahl in beiden Jahren geringfügig zu niedrig. Die korrekten Daten lauten für 2001: 79 286 erf. Fälle; 2000: 56 699 erf. Fälle. Dies ergibt eine Steigerung von 22 587 Fällen bzw. 39,9%.

Quelle: Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, PKS Berichtsjahr 2001, Bundeskriminalamt Wiesbaden, Seite 242 unter <http://www.bka.de/pks/pks2001/index2.html>

Da bei der Computerkriminalität nationale Grenzen permanent überschritten werden, handelt es sich bei Vorsorge und Bekämpfung auch um eine internationale Aufgabe. Zusätzlich zu den verschiedenen Projekten, die eine einheitliche Basis für die Verfolgung von Computerkriminalität in der Europäischen Union und darüber hinaus schaffen sollen, arbeitet das Europäische Parlament an einer Strategie zur Schaffung einer sicheren Informationsgesellschaft (A5-0284/2001, Quelle: <http://www.europarl.eu.int/meetdocs/committees/libe/20020708/472956de.pdf>) und einem Rahmenbeschluss über Angriffe auf Kommunikationsnetze und Informationssysteme (A5-0328/2002, Quelle: <http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//NONSGML+REPORT+A5-2002-0328+0+DOC+PDF+VO//DE&L=DE&LEVEL=3&NAV=S&LSTDOC=Y>).

Im Europarat wurde Ende 2001 von den 44 Mitgliedsländern des Europarates und ihren Partnern USA, Kanada, Japan und Südafrika eine internationale Konvention über Cyberkriminalität angenommen. Auch der Praxis der Strafverfolgung nimmt sich die Europäische Union an, beispielsweise im geförderten Projekt CTOSE (Cyber Tools Online Search for Evidence, Quelle: <http://www.ctose.org/>), das versucht, die manipulationssichere Speicherung und gerichtstaugliche Aufbereitung von Beweisen bei computerbasierten Verbrechen im Internet einheitlich zu definieren.

## Aufgabenbereiche der Computer Forensik

Die neue Dimension und die Geschwindigkeit, die Kriminalität durch Computer und weltweite Netzwerke erhält, zeigen nicht nur wie anfällig die Informationsgesellschaft gegen kriminelle Attacken ist, sondern gleichzeitig auch, wie wenig vorbereitet sie bei der Strafverfolgung und der dazu notwendigen Beweiserhebung dasteht. Das Gebiet der Sicherung und Wiederherstellung von Daten, der Recherche und Analyse von Indizien, die vornehmlich in digitaler Form vorliegen sowie ihre gerichtsfeste Dokumentation, ist Fokus der Computer Forensik, die somit zu einem der wichtigsten Beweismittlungs-instrumente des 21. Jahrhunderts wird. Die digitale Beweissicherung der Computer Forensik bezieht heute alle Arten der Aufzeichnung und Dokumentation von Information mittels Computern und Datenträgern ein.

### Wirtschaftskriminalität mittels Computer

Diese Varianten der Wirtschaftskriminalität sollten Sie kennen:

- **Hacking** | Eindringen in Computer(netze) zum Zweck der Spionage, Sabotage, Fälschung oder anderen Angriffen durch Zugangsentschlüsselung und Passwort-erschleichung
- **Computerspionage** | Ausforschung von Patenten, Forschung und Entwicklung, Buchhaltung, Vertriebs- und Kundendaten durch Hacking, Kopien oder unrecht-mäßige Aneignung von Datenträgern
- **Computersabotage** – meist logische, mitunter aber auch physische Schädigung von Datenträgern, Computern und Netzwerken durch Viren, Würmer und Trojaner, aber auch Angriffe aus dem Web, beispielsweise Blockade durch Überflutung der Netzanbindung per DoS (Denial of Services)
- **Datenfälschung** | Änderung von Abrechnungsdaten, Konten und Bilanzen durch externes Hacking oder interne Manipulationen oder Verschleierungen
- **Produktpiraterie** | Software- und Datendiebstahl, durch Vertrieb von Programm-kopien (Raubkopie) oder unberechtigten Zugriff auf kostenpflichtige, gespeicherte Informationen

Zu den Wirtschaftsdelikten kommen andere Varianten der Computerkriminalität, die ebenfalls für Unternehmen relevant werden können – vornehmlich durch Verfehlungen von Mitarbeitern. Hierzu zählen Äußerungsdelikte (Kinderpornographie, Volksverhetzung etc.), Verletzung des Persönlichkeitsrechts (Erpressung, Mobbing) und Teilnahme zum organisierten Verbrechen, für das das Internet heute eine nicht zu unterschätzende Kommunikations- und Aktionsplattform bietet.

Ein Großteil aller PC-Dokumente – immerhin werden 90 Prozent aller Informationen heute elektronisch gespeichert – wird niemals ausgedruckt, sondern nur als elektronische Nachricht oder E-Mail-Anlage bearbeitet, weitergeleitet und aufbewahrt. Hier kann der Verlust von Daten – ob nun durch Systemfehler, versehentliche Löschung oder beabsichtigte Sabotage – zu einem für ein Unternehmen kritischen Informationsleck werden. Wichtige E-Mails enthalten Absprachen, Diskussionen, Vorvereinbarungen, zwingende Vertragsbestandteile, Rahmendaten, Liefertermine, Adressen und Memos, deren Verlust zum Großteil unersetzlich ist. Wer immer den Mailbestand einer Firma (Inhalt aller E-Mails eines Unternehmens) kennt, weiß, dass schon eine Lücke von einem Tag kritisch für den kontinuierlichen Fortlauf werden kann, ganz zu schweigen vom Zeit- und Arbeitsaufwand und den Folgekosten, die entstehen, wenn sich die Daten nicht wieder herstellen lassen.

Und wer den Mailbestand kennt, weiß auch über so gut wie alle Interna und Strategien eines Unternehmens Bescheid, kennt Geschäftsberichte und buchhalterische Einzelheiten der Bilanzen sowie Entwicklungen und Ideen etc.

*Die neue Offenheit, die Informationen und Daten in Zugriff, Verfügbarkeit und Austausch erhalten, bildet gleichzeitig eine neue, noch nie gekannte Gefahr, die Kontrolle über die Daten zu verlieren.*

Computerkriminalität ist nicht auf Konzerne und Großunternehmen beschränkt, sondern Computerkriminalität findet ebenso wie andere Wirtschaftsverbrechen, Betrug und Spionage immer und überall statt. Somit bleibt auch Computer Forensik als Maßnahme zur Beweissicherung nicht den Großen vorbehalten, sondern bietet im Zweifels- und Verdachtsfall auch kleinen und mittelständigen Unternehmen die Werkzeuge und Dienste, ihre Firma zu schützen.

Wer sich mit dem Schutz von Firmen, ihrer dauerhaften Wettbewerbsfähigkeit und der Abwehr von Angriffen auf Unternehmen beschäftigt, erfährt heute, dass im Umfeld des Themas Computer Forensik seine Sicherheit vorbereitet und gewährleistet wird. Dieses Bewusstsein sollte bei Vorständen, Geschäftsführer sowie Anwälten, Richtern, Staatsanwälten und Ermittlern vorhanden sein, lange bevor es um konkrete Verdachtsmomente oder gar Strafverfolgung geht. Zur entsprechenden frühzeitigen Kontrolle von Entwicklungen, die für ein Unternehmen kritische Folgen haben könnten und zur Ergreifung entsprechender Sicherheitsmaßnahmen sind Unternehmen sind Geschäftsführungen durch das KonTraG-Gesetz (Kontrolle und Transparenz im Unternehmensbereich) seit 1998 verpflichtet.

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. §91 Abs.2 Aktiengesetz

## Wer den Schaden hat

Die Schäden, die durch Computerkriminalität verursacht werden, belaufen sich insgesamt auf Größenordnungen von jenseits der 50 Milliarden Euro-Marke, wobei die hohe Dunkelziffer eine genaue Einschätzung unmöglich macht. Hinzu kommt, dass für die präzise Zuordnung von Schadensfällen eine randgenaue Abgrenzung nötig wäre, was bei den sich oft überlagernden Delikten kaum mehr möglich ist: Computerkriminalität bedeutet in den meisten Fällen auch Wirtschaftskriminalität, mitunter organisiertes Verbrechen und kann sogar Angriffe auf das Leben von Menschen zur Folge haben – beispielsweise durch erpresserische Datenmanipulationen in sicherheitsrelevanten Zusammenhängen wie der Steuerung von Kernkraftwerken oder der Verwaltung von Versorgungs- und Rettungsdiensten (z.B. Krankenhäuser, Feuerwehr) und der Planung militärischer Aktionen.

### **Alle Achtung! Hier sollten Sie aufpassen.**

Indizien, die ein Unternehmen zur Vorsicht mahnen sollten, sind

- wenn der Mitbewerb gleiche Ideen hat, ähnliche Projekte entwickelt oder identische Konstruktionen vorlegt
- wenn Kunden unruhig werden, härtere Preisverhandlungen führen und mit internen Details argumentieren
- wenn Mitarbeiter offenkundig unzufrieden sind, ihre Entlassung befürchten oder bereits entlassen wurden
- wenn der Verkehr im Netzwerk schlagartig ansteigt, vor allem der Verkehr aus dem lokalen Netzwerk heraus oder in es hinein, eventuell gepaart mit gehäuften Meldungen der Firewall und
- wenn Mitarbeiter, Geschäftspartner, Kunden, Behörden mitunter sogar Mitbewerb oder andere sie vor „undichten Stellen“ warnen. Nehmen Sie solche Warnungen niemals auf die leichte Schulter

In diesen Fällen sollten alle Unternehmen den Wunsch haben, auf Nummer sicher zu gehen. Es steht viel auf dem Spiel. Suchen Sie zumindest eine Beratung bei einem Experten und erarbeiten Sie gemeinsam eine effiziente Strategie für die Überprüfung der Datensicherheit ihres Unternehmens.

Das größte Schadensfeld der Wirtschaftskriminalität macht die Werkspionage aus, sofern die digitale Entwendung und Weitergabe von Patenten, Daten, Konstruktionszeichnungen, Plänen, Ideen, Adressdatenbanken und Kundenkonditionen unter diesem Begriff subsumiert werden kann.

Unbenommen von der ungenauen, aber exorbitanten Schadenssumme belegt die hohe Dunkelziffer, dass der indirekte Schaden, der aus einer öffentlichen Verfolgung des erfolgten Angriffs resultieren würde, von vielen Beteiligten noch viel höher eingeschätzt wird, als der direkte Schaden. Zur Dunkelziffer der nicht zur Anzeige gebrachten Computerstraftaten kommt noch das dunkle Feld der kriminellen Handlungen, die nie entdeckt werden, da keine Kontrolle stattfindet. Durch solche unentdeckten Sicherheitslöcher können jahrelang Daten fließen, deren wirtschaftlicher Schaden überhaupt nicht mehr einzuschätzen ist.

*Die Dunkelziffer gibt die Gefahr an. Was wir nicht wissen, ist die kritische Größe. Der Unwissenheit zu begegnen heißt somit, Sicherheit schaffen.*

Selbst die Überprüfung, welche Informationen durch wen die internen Netze verlassen haben oder wer an welcher Stelle unberechtigt ändernden Zugriff auf Datenbestände des Unternehmens genommen hat, ist im Nachhinein nur durch eine sorgfältige Untersuchung von Netzen, Rechnern und Datenträgern zu erhalten, die die Beweiskraft des vorhandenen Materials nicht beeinträchtigen darf. Solche Nachforschungen sind Aufgabe eines Computer Forensik Experten, der sich sowohl mit den Gegebenheiten von Betriebssystemen, Anwendungen, Netzstrukturen und Computerhardware auskennt, als auch seine Vorgehensweise so abstimmt, dass seine Ermittlungen die Beweiskraft des vorliegenden Materials nicht beschädigen.

## **Gefährliche Irrtümer!**

Hier sollten Sie nicht irren:

- Unsere Mitarbeiter sind alle zufrieden
- Wir haben die volle Kontrolle über den Informationsfluss
- Das Netzwerk unseres Unternehmens ist sicher geschützt
- Jeder kann nur die Informationen öffnen und speichern, die für ihn bestimmt sind.
- Interne Daten unseres Hauses dringen nicht unkontrolliert nach außen
- Jedem im Unternehmen ist die Problematik der Geheimhaltung bewusst
- Unberechtigter Daten- und Informationstransfer geschieht immer böswillig

## Flexible Daten

Buchhaltung, Kalkulation, Kundenverwaltung, interne und externe Kommunikation, Ideen, Konzepte, Patente – Fundament, Wissen und Phantasie eines Unternehmens finden sich heute in Firmencomputern. Dabei überschreitet der Informationsgehalt der gespeicherten Daten das Potential, das einst in Aktenschränken gelagert wurde bei weitem. Hierzu tragen nicht zuletzt die beliebige Verknüpfbarkeit verschiedener Prozesse, der universelle Zugriff und die ständige Verfügbarkeit des gesamten Wissensschatzes bei. Solange die Informationen zentral gelagert werden, lassen sie sich auch zentral schützen und kontrollieren, doch wer schützt die Daten, die im Umlauf sind.

Schon die Beschreibung eines durchaus üblichen Ablaufs – beispielsweise die Vorbereitung einer Präsentation – macht transparent, wo die kritischen Punkte der Datensicherheit liegen. Beinahe selbstverständlich, dass kein Mensch den integren Mitarbeiter daran hindert, Dokumente mit internen technischen Analysen, die er zur Vorbereitung seines Vortrags auf dem Arbeitsplatzrechner gespeichert hat, samt der Powerpoint-Dateien, die im gleichen Verzeichnis liegen, auf das Firmennotebook zu übertragen. Am Wochenende setzt er sich zu Hause an seinen privaten Desktop-Rechner, lädt die aktuellsten Daten aus dem Internet und verfeinert mit ihnen die Präsentation. Da die neuen Informationen ihm wichtig erscheinen, lädt er auch gleich die Dokumentation, integriert die Daten als Anmerkungen und schickt das aktualisierte Dokument zur Info per Mail an seinen Kollegen. Am Vorabend der Präsentation loggt er sich mit dem Notebook aus dem Hotel noch einmal im Firmennetz ein, holt die neusten Mails ab, in denen sein Vorgesetzter ihn bittet, eine Wertetabelle aus der Präsentation zu entfernen, da anscheinend ein Messfehler vorliegt und ihr Inhalt „non disclosure“ sei. Selbstverständlich hält er sich an diese Anweisung löscht die Tabelle und überträgt den gesamten Vortrag auf sein PDA mit dessen Hilfe er am nächsten Tag vorträgt. Ohne bösen Willen hat dieser Mitarbeiter Tür und Tor zu den Daten seines Unternehmens geöffnet. Schuld tragen hier Faktoren wie Mobilität gepaart mit Effizienz und selbstverständlich fehlende Information und Schulung.

### Geräte, auf die Sie achten sollten!

Folgende mobile Geräte beinhalten sensible Daten:

- Notebooks, Laptops und Präsentationssysteme
- Pocket PC, Palm Organizer, Psion Handheld Computer (EPOC) und andere PDAs
- Mobiltelefone, Diktiergeräte und Fotoapparate

Neben den an Geräte gebundenen Datenspeichern – und viele interne Informationen finden sich heute ganz selbstverständlich an ganz anderen Orten, beispielsweise die Adressen aller wichtigen Kunden auf dem Mobiltelefon – ist ein anderer Weg, der Informationen die große weite Welt öffnet, die Kopie auf mobile Datenträger: Von traditionellen Disketten über Speicherkarten, beschreibbare CDs oder DVDs, Magnet-Bänder bis zu Wechselplatten, sie alle verlassen das Haus beinahe unbemerkt per Post, Boten oder Mitarbeiter. In den wenigsten Fällen ist sichergestellt, welche Daten die Datenträger enthalten dürfen, welche sie darüber hinaus enthalten, vor allem aber, welche sie zuvor enthalten haben. Gerade Dateien, die auf den ersten Blick nicht mehr sichtbar sind, sich aber oft ohne großen Aufwand wiederherstellen lassen, mitunter sogar wieder herstellbar sein sollen, bieten ein großes, weil unsichtbares Sicherheitsrisiko.

Folgende mobile Speicher können sensible Daten beinhalten:

- Diskette
- Magneto-Optische Platte (MO)
- CD-R und CD-RW
- DVD-R und DVD-RW, DVD+R und DVD+RW
- Streamerkassetten und Magnetband
- Wechselplatten (Harddisk, ZIP, JAZ, u.a.)
- Compact-Flash-Speicher oder Microdrive
- Smart Media
- Memory Stick, USB Stick
- Secure Digital oder Multi Media Card

## Beispiele konkreter Vorfälle:

Ein Mitarbeiter eines Bankinstituts, dem vorgeworfen wurde, er habe interne Kreditberechnungen auf seinen Pocket PC übertragen und einem Kreditnehmer zugänglich gemacht, gab seinen vollständig entladenen Pocket PC zur Kontrolle ab. Selbstverständlich ließen sich im flüchtigen Speicher des Geräts keine Daten wiederherstellen. Allerdings konnte durch eine forensische Untersuchung des Arbeitsplatzrechners dem Arbeitnehmer nachgewiesen werden, dass die relevanten Daten auf der Festplatte des Arbeitsrechners im Ordner „Eigene Dokumente“ gespeichert und automatisch mit dem Pocket PC synchronisiert worden waren.

Bei der Spionage von Patenten, unter der besonders die Branchen mit Zukunftstechnologien – Chemie, Bio- und Gentechnologie, Elektronik, Automobil und Telematik, um nur einige zu nennen – leiden, ist der Angriff in der Regel von außen initiiert. Dass sich die Spione der Mittäterschaft von Beschäftigten des angegriffenen Unternehmens bedienen, um Passwörter zu erfahren, Daten zu kopieren oder an andere Betriebsgeheimnisse zu gelangen, ist eine gängige Spionagetechnik, die auch im digitalen Zeitalter den raschen Weg zu den Daten ebnet.

Unachtsamkeit öffnet Eindringlingen Tür und Tor in Netzwerke. Passwörter, die sich auf Klebezetteln am Bildschirmrand verteilen, können von jedem Besucher gelesen werden. Noch unabsehbarer sind die Konsequenzen, wenn nach dem Besuch eines Filmteams – und wem ist Publicity nicht willkommen – solcherart dokumentierte Kennwörter dann im Fernsehen ausgestrahlt werden oder nach einem Fototermin in der Zeitung erscheinen. In beiden Fällen ist keine Böswilligkeit die Ursache des Problems, wobei unbenommen ist, dass manche Aufnahmen im Haus genau mit dem Ziel gemacht werden, dem Auftraggeber die Zugangsschlüssel preiszugeben.

Bei der Wirtschafts- und Industriespionage liegt der geschätzte jährliche Schaden zwischen 5 und 10 Milliarden Euro mit eher steigender Tendenz. Betroffen von der Wirtschaftsspionage sind alle Unternehmen, die sich mit zukunftsweisenden Entwicklungen beschäftigen. Hier bietet die Computer Forensik die Chance, einem Anfangsverdacht nachzugehen, den Diebstahl von Patenten und Entwicklungen auf digitalen Medien zu verfolgen und die Computerspionage nachzuweisen.

Innentäter sind oft nur unwissend. Dennoch gehen rund 85 Prozent aller Attacken auf sie zurück. Die Bedrohung von außen ist leider oft auch eine Bedrohung von innen.

Dass ein großer Teil des Datenmissbrauchs tatsächlich nicht in krimineller Absicht geschieht, sondern von gutwilligen Mitarbeitern in Unkenntnis der Sachlage und Problematik erfolgt, macht den Schaden nicht kleiner. Neben dem Ausspähen von Daten hat die Datenfälschung – beispielsweise im Zusammenhang mit Bilanzfälschungen bei Fusionierungen oder Firmenübernahmen – eklatant zugenommen. Hier sehen Unternehmen und beteiligte Steuer- und Wirtschaftsprüferbüros erhöhten Handlungsbedarf. Der Nachweis, der durch eine forensische Untersuchung der verfügbaren Datenträger geführt wird, kann zu einer gravierenden Wertberichtigung und – wie die jüngste Vergangenheit gezeigt hat – zu Strafverfahren führen.

Einem Unternehmen der IT-Branche wurde nach der Übernahme nachgewiesen, dass mit der Aufnahme der Verhandlungen, verschiedene Geschäftsberichtvarianten entstanden, die per E-Mail diskutiert wurden. Sowohl die Mails als auch die verworfenen Geschäftsberichte wurden zwar sorgfältig gelöscht, ließen sich aber aus alten Backups fast vollständig rekonstruieren, so dass sich der Nachweis des Betrugs führen ließ. Die Konsequenz der Recherche war, dass die Bewertung des Unternehmens um mehr als die Hälfte reduziert wurde

## Alles was Recht ist

Die Diskussion über die Computer Forensik rückt immer wieder den Schutz der Daten in den Vordergrund. Selbstverständlich müssen neben dem vertraulichen und oft hypersensiblen Datenbestand des Unternehmens auch alle persönlichen Daten der Mitarbeiter, ob sie nun von der Personalabteilung, von ihnen selbst oder als E-Mails gespeichert seien, geschützt werden.

Es versteht sich, dass bei prophylaktischen stichprobenartigen Kontrollen ebenso wie bei – durch einen konkreten Verdacht angeregten - umfassenden Recherchen alle Daten in die Suche einbezogen werden können. Dies macht den Schutz des Unternehmens gegen Computerspionage, -sabotage und andere –kriminelle Handlungen nötig und es dient nicht zuletzt der Wettbewerbsfähigkeit und dem Bestand des Unternehmens, der Sicherheit des Arbeitsplatzes sowie der dauernden Integrität des Datenbestandes.

Um dem Unternehmen Handlungssicherheit zu geben und für die Computer Forensik die rasche Kontrolle ohne Umwege und Diskussionen offen zu halten, haben viele große Unternehmen – beispielsweise Banken – die Policy „keine Privatsphären auf Firmenrechnern und im Firmennetz“. So ist gewährleistet und in einer Vereinbarung eindeutig festgehalten, dass jederzeit eine Kontrolle der Geschäftsdaten erfolgen kann. Ein für das Unternehmen positiver Nebeneffekt besteht darin, dass zeitlich intensive „Privatausflüge“ ins Internet ausfallen. Dies bringt erfahrungsgemäß Reduktionen der Verbindungszeiten von über 50 Prozent, teilweise bis zu 90 Prozent mit sich.

Die private Nutzung von E-Mail und Internet sollte ausdrücklich im Arbeitsvertrag geregelt sein. Eine Alternative hierzu bietet eine offizielle Betriebsvereinbarung. Auf jeden Fall sind bei Bestehen eines Betriebsrats die Regularien mit ihm abzustimmen. Um späteren Problemen vorzubeugen ist – vor allem bei der noch immer rechtlich unklaren Situation dringend angeraten, die Problematik in konkretem Hinblick auf das eigene Haus mit einem Fachanwalt zu beraten.

Generell kann gesagt werden, dass der Arbeitgeber nur dann umfassende Kontrollmöglichkeiten hat, wenn gewährleistet ist, dass E-Mails und Dateien keine persönlichen Inhalte haben, die Internetnutzung nur dienstlich initiiert ist und alle Speichermedien lediglich Firmendokumente enthalten. Dies setzt voraus, dass eine private Nutzung der Onlinemedien ausdrücklich untersagt wurde, sämtliche im Unternehmen eingesetzten PCs Firmeneigentum sind und keine privaten Speichermedien im Unternehmen verwendet werden dürfen.

Dadurch, dass private E-Mails nicht versandt und empfangen werden dürfen und private Dokumente nicht gespeichert werden, kann das Unternehmen davon ausgehen, dass sämtliche gespeicherten Inhalte sich auf Firmenbelange beziehen. Darüber hinaus ist der Arbeitgeber, der die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken erlaubt, kein Telekommunikationsanbieter im Sinne des Telekommunikations- (TK-) bzw. Teledienstrechts. Der Arbeitskreis Medien schreibt hierzu in seiner Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, die sich an öffentliche Stellen des Bundes und der Länder richtet, deren dargestellte Grundsätze aber ausdrücklich auch auf den nicht-öffentlichen Bereich übertragen werden können:

*„Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine vollautomatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.“ (Quelle: [http://www.bfd.bund.de/information/DS-Konferenzen/oh\\_email.pdf](http://www.bfd.bund.de/information/DS-Konferenzen/oh_email.pdf))*

Prinzipiell sollten im Verdachtsfall auf allen Geräten und Medien, auf denen sensible Daten das Unternehmen verlassen können oder über die Zugriff auf das Unternehmen erfolgen kann, auch Nachforschungen angestellt werden können. Auf jedem Speichermedium können rechtserhebliche Daten gefunden werden und daher ist auch jedes Speichermedium bei der Kontrolle und Recherche einzuschließen. Damit dies ohne Schwierigkeiten umgesetzt werden kann, muss gewährleistet sein, dass im Unternehmen nur Speichermedien verwendet werden dürfen, die Firmeneigentum sind.

Durch das Eigentum an Hard- und Software hat das Unternehmen das Recht, auf alle Geräte, Speichermedien und Protokolle zuzugreifen. Voraussetzung hierfür ist eine schriftliche Vereinbarung, die von Arbeitnehmer und Arbeitgeber unterzeichnet ist, kontrolliert und geahndet wird.

Es ist im Interesse aller Arbeitnehmer und trägt zur Sicherung der Arbeitsplätze bei, dass ein Unternehmen sensibler und rasch auf Merkmale reagieren muss, die auf Spionage oder Sabotage schließen lassen. Früherkennung hilft Schaden zu begrenzen, bevor er virulent wird. Diesem Argument wird sich der Betriebsrat schwerlich bei den nötigen Vorvereinbarungen verschließen. Da innerhalb eines Unternehmens vertrauliche und geheime Informationen in der Regel auch per E-Mail weitergeleitet werden, muss die Möglichkeit eines Mechanismus gegeben sein, der das Versenden der sensiblen internen Daten und Nachrichten nach außen kontrolliert und stichprobenartige Untersuchungen über die Integrität des Datenverkehrs erlaubt.

Die Problematik unkontrollierter Speichervorgänge lässt sich durch den Verzicht auf Diskettenlaufwerke und andere Geräte für beschreibbare Medien deutlich reduzieren. Allerdings verfügen heute beinahe alle Geräte über Möglichkeiten, externe Laufwerke anzuschließen. Dazu kommt, dass viele Computer heute mobil außerhalb des Unternehmens eingesetzt werden. Hier ist ein Ausschluss des Missbrauchs nahezu unmöglich. Umso wichtiger ist es, dass die Möglichkeiten der Kontrolle durch Computer Forensik im Vorfeld durch entsprechende Vereinbarungen gewährleistet werden.

Wenn die Recherche durch einen unbeteiligten Dritten erfolgen soll, muss dessen Integrität vom auftraggebenden Unternehmen sichergestellt sein. Der lückenlose Einblick in die Geschäftsdaten, der mitunter erforderlich ist, um beispielsweise Veränderungen und Fälschungen im Datenbestand historisch nachzuweisen, erfordert ein besonderes Vertrauensverhältnis.

Sicherheit schafft eine rückverfolgbare Firmenhistorie, die gewährleistet, dass der Auftragnehmer nicht nur seine Kompetenz und sein handwerkliches Geschick, sondern auch seine Vertrauenswürdigkeit bereits unter Beweis gestellt hat. Ähnlich eines Fonds, der den prognostizierten Wert seiner künftigen Entwicklung nicht zuletzt aus seinen historischen Daten herleitet, ist auch bei der Übergabe sensibler Daten – vor allem solcher, die der Auftraggeber nicht kennt, deren Gehalt er oft nur vermutet, deren Inhalt er mitunter gar fürchtet – absolut darauf zu achten, dass sie niemals in die falschen Hände geraten.

Seriöse Unternehmen wie Kroll Ontrack garantieren Verschwiegenheit, solange sie keine Kenntnis von meldepflichtigen Straftatbeständen erlangen. In dieser Vorsicht liegt auch begründet, dass sich gute Computer-Forensik-Unternehmen sehr wohl für die Rekonstruktion der Daten interessieren, nicht aber – solange es nicht ausdrücklich vom Auftraggeber gewünscht wird – für ihren Inhalt.

### **Seriosität als Entscheidungskriterium**

Eine lückenlose seriöse Firmengeschichte, wie beispielsweise die Historie der KROLL ONTRACK GmbH, die 15 Jahre zurückreicht, ist ein überzeugendes Argument. Auf dem Gebiet der Datenrettung hat Kroll Ontrack inzwischen über 200.000 erfolgreiche Wiederherstellungen durchgeführt. Die langjährig Erfahrung und permanente Weiterentwicklung auf dem neusten Stand der Technik bilden die Basis für eine Datenrettung, die neben traditionellen Speichermedien auch innovative Datensicherungsformen mit einbezieht. Wie hoch der Qualitätsstandard, die Zuverlässigkeit und die fachliche Kompetenz im Bereich Festplatten und Festplattenmanagement ist, beweist unter anderem der Kroll Ontrack Disk Manager®. Das weltweit verbreitete Tool wird seit Mitte der achtziger Jahre vertrieben – rund 150 Millionen Lizenzen – und schafft auch in älteren PCs Zugriff auf neue, große Platten (momentan bis zu 137 Gigabyte). Beinahe alle namhaften Plattenherstellern (Fujitsu, IBM, Maxtor, Quantum, Samsung, Seagate, Toshiba und Western Digital) setzen auf den Kroll Ontrack Disk Manager als optionales Installations-Werkzeug. Solche millionenfach geprüfte und bewährte Praxis zeugt von Solidität in einem Bereich, in dem gerade in kritischen Situationen größtes Fachwissen ad hoc verfügbar sein muss. Nur wer die Festspeicher so präzise wie die Hersteller kennt, weiß ohne Zeitverlust und zusätzliche Recherche worauf auf jeden Fall zu achten ist und wie er sich von der Seite des Betriebssystems auf sicherste Weise der beweisträchtigen Hardware nähert und ihre Indizien sichert.

## Vorgehen der Computer Forensik

Ein wichtiges Entscheidungskriterium bei der Wahl des Computer Forensik Experten ist, dass nicht nur die handwerkliche Expertise im Haus vorliegt, sondern dass sich diese Kompetenz aus dem grundlegenden Verständnis des gesamten Systems bildet. Nur so ist gewährleistet, dass Probleme, die sich bei der Wiederherstellung von Daten immer wieder ergeben können, nicht rein mechanisch behoben werden müssen, sondern im Gesamtzusammenhang verstanden, eingeordnet und gelöst werden. Nur wer die Details sowohl auf Software- als auch auf Hardwareebene kennt, kann aufwendige Recherchen auf das Wesentliche und das Machbare eingrenzen und auf diese Weise Kosten sparen, ohne Informationsverluste zu riskieren.

So macht es unter gewissen Umständen keinen Sinn, eine Platte zu restaurieren, da sich die relevanten Daten der Platte im Netzwerk auf anderen Rechnern, beispielsweise Servern oder Backupsystemen lückenlos rekonstruieren lassen. Mit genauer Kenntnis des Betriebssystems, der vorhandenen Netzstruktur und der für diesen Fall geeigneten Werkzeuge zur Datenrettung kann oft mit deutlich reduziertem Aufwand eine rasche und erfolgreiche Datenrecherche eingeleitet werden. Wenn absehbar ist, dass System- und Strukturanalyse auf dem Weg zu den gesuchten Daten nicht weiterkommen, ist es Zeit für den Reinraum-Ingenieur, seinen weißen Kittel überzustreifen und sich mit Feinmechanik und Fachwissen auf die Spur des Datenbestands zu machen. Hier ist dann die perfekte Zusammenarbeit zwischen Analytiker und Mechaniker gefragt, denn von außen betrachtet sind alle Daten gleich. Nur in der perfekten Kombination von der Suche nach vorgegebenen Mustern in den logisch als relevant erachteten Sektoren lässt sich zielgerichtet vorgehen. Anders ist aber eine Recherche auf gigabytegroßen, gelöschten und oft stark beschädigten Datenträgern kaum effizient darstellbar.

Je nach Beschädigung kann ein Lesevorgang durchaus einige Tage dauern, eine Spanne, die für den Auftraggeber nicht nur sehr teuer, sondern bei zeitkritischen Daten auch deutlich zu lange ausfallen kann. Hier lässt sich zumindest mit der genauen Kenntnis des Installationsverhalten von Betriebssystemen und Programmen, der automatischen Verwaltung von temporären und Auslagerungsdateien und der Vorgehensweise von Tools wie beispielsweise Festplattenoptimierern der Einsatz von Energie am falschen Platz sparen.

## Erste Schritte

Vor dem Eintreffen eines Computer Forensik Experten ist es wichtig, die Situation ganz nüchtern in Augenschein zu nehmen, allerdings nur in Augenschein. Kroll Ontrack bittet darum, dass die betroffenen Rechner nicht berührt werden, solange es nicht absolut notwendig ist – beispielsweise zum Abbruch einer laufenden Mailübertragung, die vielleicht durch das Abziehen des Netzwerk- oder Telefonkabels gestoppt werden kann. Schon das Verschieben der Maus kann dazu führen, dass sich nicht mehr Verifizieren lässt, ob der letzte Mitarbeiter an diesem Computer ein Rechts- oder Linkshänder war. Auf seine Identität können aber auch andere Details wie Kaffeetasse, Aschenbecher, Stift usw. hindeuten. Mögen diese Informationen auch in vielen Fällen unerheblich sein, so gehen doch in den wenigen entscheidenden Situationen durch Unachtsamkeit wichtige Indizien verloren.

Dass ein laufender Rechner, auf dem Beweismaterial vermutet wird, nicht ausgeschaltet werden soll, versteht sich von selbst, geht hierdurch doch der gesamte flüchtige Inhalt des Arbeitsspeichers verloren.

Ein schwarzer Bildschirm kann das Ergebnis eines Bildschirmschoners sein und sollte nicht darüber hinwegtäuschen, dass im Hintergrund Programme laufen.

Je nach Situation und vermutetem Delikt wird der Computer Forensik Experte zunächst die Situation aufnehmen, den Bildschirm abfotografieren, den Inhalt des Arbeitsspeichers und die Daten der laufenden Programme auf einem externen, neuen Datenträger sichern, bevor er den PC abschaltet. Auf keinen Fall wird er auf den internen Laufwerken des Rechners Daten speichern oder den PC ordnungsgemäß herunterfahren, eventuell sogar neu starten, da bei allen diesen Vorgängen je nach Betriebssystem Daten auf die Festspeicher geschrieben und Dateien gelöscht oder überschrieben werden können. Aus diesem Grunde darf ein ausgeschalteter PC bei Vorlage eines Verdachts auch niemals einfach eingeschaltet werden, um eigenhändige Ermittlungen anzustellen, da beim Startvorgang wichtige Information durch Überschreiben verloren gehen könnten.

## To Do! Das müssen Sie im Vorfeld einer Untersuchung beachten.

Handelt es sich um einen Rechner oder sind mehrere Computer betroffen?

(Die folgenden Fragestellungen gelten für jeden betroffenen PC)

- PC ist eingeschaltet, -> dann bleibt er eingeschaltet, bis er untersucht wurde.
- PC ist ausgeschaltet, -> dann bleibt er ausgeschaltet, bis mit den geeigneten Hilfsmitteln eine bitgenaue Kopie der Originaldatenträger angelegt und die Datenträger als Beweismittel unverändert sichergestellt wurden.
- Kleben Sie ein Schild auf den Bildschirm: Achtung! Mit diesem PC nicht mehr weiter arbeiten!

Die Umgebung und Konfiguration des/der Rechner muss auf Details geprüft werden und die Ergebnisse dokumentiert werden:

- Ist es ein unverbundener PC oder wie ist der PC in ein Netzwerk integriert?
- Hat der PC einen Internetanschluss und ist die Verbindung aktiv?
- Welchen Datenspeicher-Medien sind im PC integriert und auf welche Datenspeicher hat der PC Zugriff?
- Sind alle Wechselmedien verfügbar, die mit dem PC eingesetzt wurden und wurden sie sichergestellt?
- Welche Peripheriegeräte, die in der Lage sind, Daten zu speichern (PDAs, Mobiltelefone, Digitalkameras, MP3 Player etc.) wurden an den Rechner angeschlossen und sind sämtliche Peripheriegeräte inklusive ihrer Medien sichergestellt?

Die Behandlung, die digitalem Beweismaterial im Rahmen von fiktionalen Geschichten – beispielsweise Fernsehkrimis und Romanen – zukommt, ist absolut kein Beispiel für die Realität. Während in der Regel Polizeiaktionen durch fachkundige Beratung möglichst realistisch gestaltet werden, ist die Darstellung von der kriminalistischen Recherche an den digitalen Geräten des Tatorts oder der Tatverdächtigen oft unprofessionell umgesetzt. Da werden Computer ausgeschaltet, gebootet, Programme gestartet und lediglich die offen zugänglichen Dateien rasch mit einfachsten Suchfunktionen gescannt – oft direkt am Tatort oder am Schreibtisch des bearbeitenden Beamten, stets aber auf der Originalhardware, als einem leicht veränderlichen Indiz, das somit alle Beweiskraft verliert und zuvor nicht gesichert wurde –, so dass kein Tatverdächtiger sich eigentlich die Mühe machen müsste, gespeichertes Beweismaterial selbst zu vernichten. Dies erledigen in diesen Spielhandlungen stets die Ermittler selbst, zumindest entheben sie die recherchierten Daten der Beweiskraft.

## Protokollierung

Der Computer Forensik Experte wird aus allen relevanten Speichermedien die Daten erfassen. Eine Eins-zu-eins-Kopie (Image) kann an den sichergestellten Medien im Labor stattfinden, wobei der Computer Forensik Experte ab dem Zeitpunkt der Übergabe die Gewähr übernimmt.

Alternativ hierzu kann die Erfassung der Daten auch direkt vor Ort beim Kunden stattfinden. Dabei sollte der Ablauf des Vororteinsatzes genauestens protokolliert werden. Hierfür setzen sich beispielsweise die Ingenieure von Kroll Ontrack mit dem zuständigen Projektmanager in Verbindung

- bei der Ankunft,
- beim Zutritt auf Kundengelände,
- beim Zugriff auf Daten(träger),
- beim Antritt der Rückreise
- bei ihrer Ankunft und
- bei der Übergabe der Medien ins Labor, wo die Originaldatenträger im Tresor gesichert werden.
- Sie geben während der Arbeit laufend Zwischenbescheide,
- vermerken jede Pause und jedes Vorkommnis während ihres Vororteinsatzes und
- den Zeitpunkt der Beendigung ihres Einsatzes.
- Sie stellen sicher, bzw. vereinbaren mit Vorortpersonal, dass während Pausen oder z.B. über Nacht kein Zutritt und Zugriff Dritter möglich ist.

Bei dieser Vorgehensweise übernimmt Kroll Ontrack die Gesamtverantwortung für den ordnungsgemäßen Ablauf und gewährleistet bei Zugriff und Lagerung der Datenträger auch bei der Wiederherstellung und Analyse der gespeicherten Daten eine durchgängig protokollierte Historie. Dies ist die Grundlage für die Gerichtsfestigkeit der ermittelten Daten.

## Sicherung der Daten

Nach einer ersten Bestandsaufnahme werden die verfügbaren Daten gespeichert. Hierbei entscheiden Relevanz und Empfindlichkeit über die Reihenfolge. Läuft der verdächtige Rechner noch, werden mit geeigneten Tools zunächst Inhalte des flüchtigen Speichers und die Informationen des Systemstatus gesichert, sofern dies für diesen Fall von Bedeutung ist. Hierbei stehen alle Daten im Vordergrund, die durch ein Ausschalten des Systems gelöscht oder verändert werden könnten; sofern dies auch Daten betrifft, die auf Festplatten temporär zwischengespeichert werden, werden auch diese einbezogen.

Anschließend muss eine bitgenaue Sicherung der Datenspeicher ohne Veränderung der Meta-Daten vorgenommen werden. Auch für die sektorweise 1:1 Kopie des Datenträgers mit Erfassung aller einzelnen Bits verfügt der Computer Forensik Experte über die professionellen Werkzeuge. Die bitgenaue Kopie kann beim Kunden oder im Labor erstellt werden. Sollte der Datenträger beschädigt oder defekt sein, ist es in der Regel erforderlich, ihn unter Laborbedingungen zu kopieren, da hier ein Reinraum und Laufwerk-techniken für die temporäre Inbetriebnahme oder Reparatur des Datenträgers zur Verfügung stehen.

Wie und auf welchen Datenträger die Sicherung erfolgt, wird ebenso wie alle anderen Aktionen protokolliert. Diese 100%ige und lückenlose Protokollierung der „Chain of Custody“ macht aus den dokumentierten Daten Beweise, die auch vor Gericht Stand halten. Hierfür werden die Original-Datenträger bei Kroll Ontrack in einem eigenen Safe gelagert, auf den nur autorisiertes Personal Zugriff hat.

Niemals wird ein Computer Forensik Experte Untersuchungen der Daten direkt an den Original-Datenträgern in einem PC durchführen. Bei Kroll Ontrack wird zudem aus Sicherheitsgründen ein zweites Image erstellt, an dem dann die weiteren Untersuchungen und Analysen erfolgen. Alle weiteren Aktivitäten erfolgen an dem zweiten Image. Der Originaldatenträger oder das erste Image, dienen lediglich als Beweismaterial. Die genau festgelegten und protokollierten Prozesse prädestinieren die Kroll Ontrack Computer Forensik Experten, auch als Sachverständige vor Gericht aufzutreten.

## Wiederherstellung der Daten

Voraussetzung für eine genaue Beweismittelrecherche ist, dass alle relevanten Daten zum Zugriff verfügbar sind. Daher ist die Kompetenz im Bereich Datenrettung eine grundlegende Voraussetzung für erfolgreiche Computer Forensik. Die Computer Forensik Experten kooperieren durchgängig mit den Datenrettungsexperten von Kroll Ontrack. Eigene Werkzeuge, Labors und selbstentwickelte Techniken ermöglichen die Rettung von Daten auch von stark beschädigten Datenträgern und aus gelöschten Dateien, Datenbanken und E-Mail-Archiven. Dank genauer Systemkenntnis, die auch die Hardware und Software alter Systeme umfasst, arbeiten die Computer Forensik Experten selbst dann mit überzeugenden Erfolgsquoten, wenn Täter versucht haben, belastende Daten zu vernichten, und zunächst der Zugriff auf beschädigten Speicher-Medien wieder hergestellt werden muss.

Durch genaue Systemkenntnisse, wissen die Experten, welche Daten in welchen Verzeichnissen, Sektoren oder Segmenten von Datenträgern zu finden sind, was eine rasche und effiziente Wiederherstellung gelöschter Dateien möglich macht. Gelöschte Dateien lassen sich relativ leicht wieder herstellen, sofern mit dem entsprechenden PC nicht allzu lange weiter gearbeitet wurde und somit Dateien überschrieben wurden. Darüber hinaus lassen sich Datei-Fragmente in freigegebenen Clustern und im Slack-Bereich (von Dateien nicht ausgenutzten Bereichen) der Festplatte auffinden.

Selbst aus formatierten Festplatten und beschädigten Datenträgern lassen sich Daten gezielt wiederherstellen, wobei auch zunächst nicht mehr lesbare, korrupte Dateistrukturen kein dauerhaftes Hindernis bieten. Und auch wenn sich durch physische Zerstörungen – beispielsweise fehlende Stücke des Magnetbandes – nur Teile des Datenträgers wiederherstellen lassen, so kann dies durchaus genügen, da eventuell dieser Teil wichtige Informationen, den verlangten Nachweis oder das fehlende Indiz enthält.

Viele verloren geglaubte Informationen lassen sich zudem aus gelöschten Emails oder über die Wiederherstellung von Meta-Daten retten. In diesem Zusammenhang wird deutlich, wie wichtig die genaue Kenntnis von Betriebssystemen und deren Eigenheit ist. So können beispielsweise aus alten temporären Dateien Informationen gerettet und Zusammenhänge belegt werden, um deren Verschleierung und Löschung sich Kriminelle an anderer Stelle des Datenträgers erfolgreich bemüht haben.

In diesem Zusammenhang ist wichtig, dass der Experte genau weiß, wie Dateien, die Lücken haben, aufgefüllt werden können, so dass sie mathematisch als vollständige Datei erkannt werden. Korrupte Dateien werden über Software-Werkzeuge lesbar gemacht, so dass alles, was außerhalb des korrupten Bereiches liegt, wieder gelesen werden kann. So lassen sich auch Dokumente, deren Header beschädigt ist, restaurieren und wieder öffnen, was sonst vom Programm bei korrupten Dateien verweigert wird. Für die Authentizität des Datenmaterials ist entscheidend, dass physikalisch fehlende Daten – beispielsweise Worte in einem Dokument oder einer Mail – niemals ersetzt, sondern als Lücke freigehalten werden. Unter forensischen Gesichtspunkten gilt es, das Original ohne Verfälschung und Ergänzungen eigener Hand so weit wie möglich zu restaurieren. Nur so bleibt der Beweischarakter erhalten.

Bei beschädigten Datenträgern liegt die Quote der erfolgreichen Datenwiederherstellung bei rund 80 Prozent. Die Möglichkeiten bei der Datenwiederherstellung im Bereich der Beweismittelrecherche ist höher, da hier weniger defekte, statt dessen meist gelöschte Datenträger zu analysieren sind. Hinzu kommt, dass Verursacher selbst bei böswilligen Löschanversuchen meist nicht professionell vorgehen, was die Chance auf eine effiziente Datenrettung erhöht.

Stets sollten die Geschädigten sich darüber im Klaren sein, dass teilweise oder ganz gelöschte oder nicht ansprechbare Datenträger sehr wohl rekonstruierbares Beweismaterial enthalten können. Gelöschte oder defekte Datenträger, selbst mutwillig zerstörte Speichermedien lassen sich meist „reparieren“. Auch wenn der Schieber oder das ganze Gehäuse einer Diskette entfernt wurde, und nur noch die Speicherfolie vorliegt, die Festplatte durch Aussetzen des Schreib-/Lesekopfes auf der Magnetplatte (Headcrash) unlesbar ist, oder die Oberfläche der beschreibbaren CD-ROM oder DVD zerkratzt wurde, – dies nur als drei Beispiele aus dem Spektrum der denkbaren Zerstörungen die von systemimmanenten Eingriffen bis zu brachialer Gewalt reichen – besteht berechtigte Hoffnung, durch manuelle Eingriffe in speziell ausgerüsteten Werkstätten wieder Zugriff auf die gespeicherten Daten zu erhalten. Daher muss gerade in Fällen, in denen ein Verdacht vorliegt, der sich nicht ad hoc durch Einblick in ein möglicherweise beweisrelevantes Medium erhärten lässt, keine vorschnellen Schritte unternommen werden dürfen, sondern der Datenträger als möglicherweise entscheidendes Beweismittel sichergestellt und einer professionellen Untersuchung zugeführt werden muss. Völlig falsch und nachgerade fahrlässig wäre es, diesen Datenträger – beispielsweise den Computer einer verdächtigten Person – dem normalen Geschäftsbetrieb wieder zuzuführen, indem die Festplatte formatiert und mit einer Standardkonfiguration überschrieben wird. Der Schaden, der durch die Zerstörung möglicherweise noch bestehenden, lediglich nicht direkt einsehbaren Beweismaterials entstehen kann, ist zu diesem Zeitpunkt und ohne fachgerechte Analyse nicht absehbar.

## Eingrenzung des Datenmaterials

Nun liegt der Fokus der Computer Forensik – anders als bei der Datenrettung – auf der gezielten Eingrenzung der Daten. Wenn die regenerierten Datenmengen so groß werden, dass sie nicht mehr überschaubar sind, kommen Filterfunktionen zum Einsatz, die mit gezielter Schlüsselwortsuche und der Sortierung nach gewünschten Kriterien die Flut der Daten kanalisiert und auf die für die Beweisfindung relevanten Daten konzentriert.

Zu dieser Eingrenzung des verfügbaren Datenmaterials gehört auch die Deduplication, bei der Informationen, die mehrfach in identischer Form gespeichert sind, zur Reduktion der Datenmenge ausgefiltert werden. Solche Vervielfältigungen liegen beispielsweise vor, wenn Programme Daten in identischer Form in verschiedenen Verzeichnissen speichern beispielsweise E-Mails als Entwürfe, Postausgang und an mehrere Adressaten versandte Objekte oder wenn in Dokumenten leere Seiten gespeichert wurden, die keinerlei Information, wohl aber Speicher- und Untersuchungsbedarf liefern. Solche redundanten Informationen lassen sich mit entsprechenden Tools herausfiltern, was die Reduktion und Transparenz der für die Beweisführung notwendigen Datenmenge gewährleistet.

Letztendlich sollten die erzielten Ergebnisse in der für die Zielgruppe am besten verständlichen und bearbeitbaren Art aufbereitet werden. So werden in den allermeisten Fällen Richter, Staatsanwälte und Anwälte weder an die technischen Hardwarekomponenten noch den entsprechenden Software Applikationen Interesse haben. Sie erwarten mit Recht, dass Ihnen die Erkenntnisse, die aus dem Datenmaterial resultieren, in einer gut verständlichen, rasch zu bearbeitenden Form präsentiert werden. Hierfür hält Kroll Ontrack mit seinem selbstentwickelten ElectronicDataViewer eine eigene Dokumentationsmethode bereit, mit der sich die Ergebnisse der Untersuchung Online am Bildschirm abrufen, durchsuchen und präsentieren lassen. Mittels des Kroll Ontrack ElectronicDataViewer kann auch im Gerichtssaal die Betrachtung des vorsortierten, markierten Datenmaterials online und live erfolgen. Darüber hinaus lassen sich alle Daten zur Unterstützung der Prozessführung auch in adäquater, vollständiger Form ausdrucken und – zum schnelleren Rückgriff – in eine Datenbank importieren.

Darüber hinaus stellen die Computer Forensik Experten von Kroll Ontrack bei Rechtsfällen spezielle Berichte über die ermittelten und analysierten Daten zur Verfügung. Sie stehen für eidesstattliche Erklärungen zur Verfügung, liefern das erforderliche Material und erstellen rechtserhebliche Berichte. Selbstverständlich ist das gesamte Beweismaterial nach wie vor im ursprünglichen Format (Originaldateityp) und zur gerichtsfesten Beweisführung auf den Originaldatenträgern verfügbar.

### Hier hilft die Computer Forensik

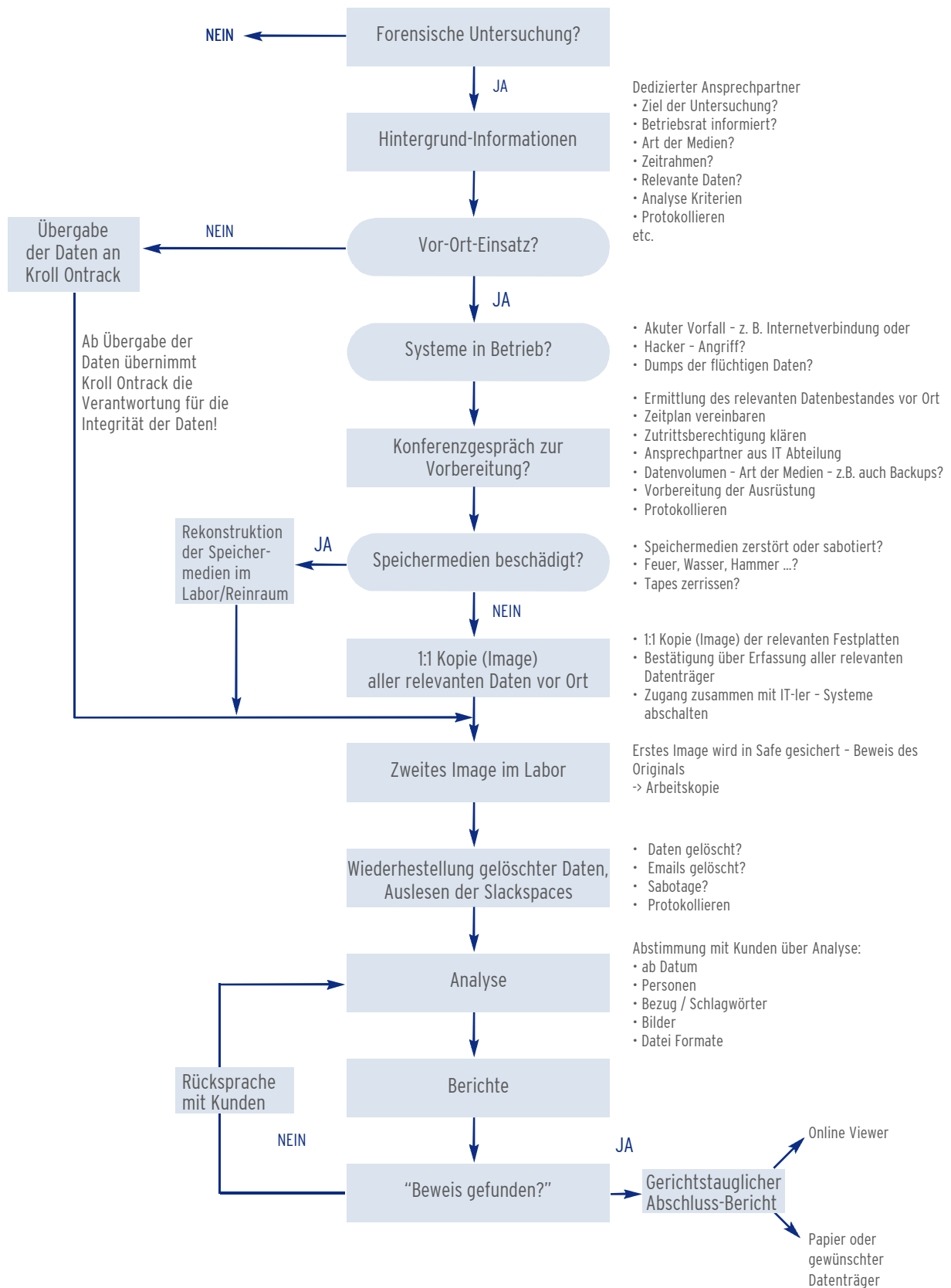
Computerkriminalität geht alle an, denn auch wenn

- Backup-Strategien akribisch durchgehalten werden, können Daten gestohlen oder vernichtet werden
- das lokale Netzwerk aufwendig gegen Angriffe von außen geschützt ist, können von außen und innen durch Spamming, Viren und Trojaner gefährliche Angriffe erfolgen
- die Mitarbeiter gut ausgesucht und geschult sind, können sie unbedarft oder korrupt sein und absichtlich oder unabsichtlich Daten nach außen tragen.

Computer Forensiker bieten vor und während der Krise Vorständen, Geschäftsführern oder ihre Rechtsbeiständen die Chance, sich durch professionelle Hilfe zu entlasten.

- So können sie sich im Alltag auf ihre wesentlichen Arbeitsbereiche konzentrieren,
- erhalten – sofern das Material es erfordert und zulässt – gerichtsfeste Beweise in der gewünschten Form,
- können selbständig entscheiden, welche Vorgehensweisen Ihnen angemessen erscheinen
- und vermeiden, dass Unruhe im Umfeld der nötigen Ermittlungen sich direkt auf Ihre Person fokussiert.

# Normaler Prozessablauf



**Kroll Ontrack GmbH**  
**Hauptsitz Böblingen**  
Hanns-Klemm-Str. 5  
71034 Böblingen  
Fon +49 (0)7031 644-0  
Fax +49 (0)7031 644-100  
Datenrettungs-Hotline:  
0800 10 12 13 14  
  
info@krollontrack.de  
[www.ontrackdatarecovery.de](http://www.ontrackdatarecovery.de)

**Kroll Ontrack S.a.g.l.**  
Piazza Boffalora, 4  
P.O. Box 191  
6830 Chiasso 3 Boffalora  
Fon +41 (0)91 68286-92  
Fax +41 (0)91 68286-94  
Datenrettungs-Hotline:  
0800 880 100  
  
info@krollontrack.ch  
[www.ontrackdatarecovery.ch](http://www.ontrackdatarecovery.ch)

**Kroll Ontrack GmbH**  
**Zweigniederlassung Österreich**  
Landstraßer Hauptstraße 71/2  
1030 Wien  
Fon +43 (0)1 71728-380  
Fax +43 (0)1 71728-110  
Datenrettungs-Hotline:  
0800 644 150  
  
office@krollontrack.at  
[www.ontrackdatarecovery.at](http://www.ontrackdatarecovery.at)

Copyright © 2008 Kroll Ontrack Inc.  
All Rights Reserved.

All other brands and product names are  
trademarks or registered trademarks of

**KROLL ONTRACK®**

**Vertrauen Sie auf die Besten.**