Kroll Ontrack™

Peter Böhret

„Daten auf der Spur“

Handbuch zur Datenrettung und Computer Forensik

Die Informationen im vorliegenden Buch werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autor können daher für fehlerhafte oder veraltete Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Bei konkreten Vorhaben der Datenrettung oder Computer Forensik empfiehlt sich die Kontaktaufnahme mit der Kroll Ontrack Kundenberatung.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Verwendung und Speicherung in elektronischen Medien.

Die gewerbliche Nutzung der Inhalte dieses Buches ist nicht zulässig. Texte und Abbildungen können jedoch nach vorheriger schriftlicher Freigabe durch die Kroll Ontrack GmbH im Zusammenhang mit Veröffentlichungen über IT-Sicherheit, Datenrettung oder Computer Forensik unentgeltlich genutzt werden.

Copyright (c) 2004 by Kroll Ontrack GmbH

Kroll Ontrack GmbH
Hanns-Klemm-Straße 5
71034 Böblingen
Tel. 07031/644-0
Internet: www.krollontrack.de; www.ontrack.de
E-Mail: info@krollontrack.de

1. Auflage

Printed in Germany

Produktmanagement und Layout:
Trimedia Communications Deutschland GmbH
Ina Brendt, Alexandra Schwarz

Druck: Digital PS Druck AG

Inhaltsverzeichnis

Vorwort

Im digitalen Zeitalter sind die Gefahren durch Datenverlust und Computerkriminalität stets gegenwärtig. Jahr für Jahr wächst die Menge an elektronisch gespeicherten Daten. Unternehmen, Organisationen, Behörden und Privatleute kommunizieren per E-Mail und nutzen elektronische Speichermedien, um kritische Daten, aus Kundenverwaltung, Buchhaltung, Kalkulation, Planung und Konstruktion zu speichern. Digitale Daten sind daher von entscheidender Bedeutung: Sie sind das wirtschaftlich wichtigste Gut eines jeden Unternehmens. Doch mit der Zunahme an gespeicherten Daten wächst auch die Gefahr, Daten zu verlieren oder Opfer von Computerkriminalität zu werden – beides kann im Ernstfall die Existenz eines Unternehmens gefährden.

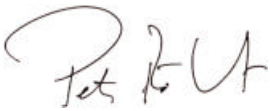
Mit diesem Handbuch möchten wir, die Kroll Ontrack GmbH, führender Anbieter von Services und Software im Bereich von Datenrettung und elektronischer Beweissicherung, die besondere Bedeutung von Datensicherung und Datensicherheit aufzeigen. Erfahren Sie auf den folgenden Seiten, wie elementar Datenrettung und Computer Forensik heutzutage sind, welche Präventionsmaßnahmen ergriffen werden können und müssen und wie Kroll Ontrack betroffenen Unternehmen, Institutionen oder Privatleuten im Krisenfall schnell und effizient helfen kann.

Im Anhang finden Sie Checklisten, die Ihnen im Schadensfall eine schnelle und sichere Orientierung geben. So schützen Sie sich vor gut gemeinter aber unsachgemäßer erster Hilfe und meistern Krisen

schon von Anbeginn. Sollten Sie Interesse an immer aktuellen Informationen von Kroll Ontrack haben - ein Anruf, eine E-Mail oder ein Brief an uns genügt. So sind Sie topaktuell informiert und stets auf der sicheren Seite!

Ich freue mich, von Ihnen zu hören!

Ihr



Peter Böhret
Geschäftsführer
Kroll Ontrack GmbH

Datenrettung

Was sind Daten eigentlich wert?

Buchhaltung, Kalkulation, Kundenverwaltung, interne und externe Kommunikation, Entwürfe, Konzepte, Patente – Fundament, Wissen und Visionen eines Unternehmens finden sich heute in Computern. Dabei überschreitet der Informationsgehalt der gespeicherten Daten bei weitem das Potenzial, das einst in Aktenschränken gelagert wurde. Hierzu tragen nicht zuletzt die beliebige Verknüpfbarkeit verschiedener Prozesse, der universelle Zugriff und die ständige Verfügbarkeit des gesamten Wissensschatzes bei.

Tatsächlich ist sich aber kaum ein Unternehmen des Wertes seiner Daten bewusst. Mittlerweile kann zwar nicht mehr nur die Hardware versichert werden, sondern auch der Datenbestand, die Wertbestimmung von Daten ist jedoch recht willkürlich. Ob der Versicherungsschutz tatsächlich die Kosten abdeckt, die bei einem Datenverlust entstehen, bleibt damit fraglich. Versicherungsgesellschaften, die dieses Risiko abdecken, rechnen nach der Formel: 1 MByte Daten entspricht einem Wert von € 1.000.[1] Dass eine solche Absicherung nicht ausreicht, kann leicht an zwei Beispielen errechnet werden:

1. Eine versierte Schreibkraft (durchschnittlich 300 Anschläge/min) kann Text mit einem Umfang von 1 MByte optimal in ca. 55 Ar-

[1] Quelle: TELA Versicherungs AG

beitsstunden erfassen – vorausgesetzt, die Daten liegen als Ausdruck vor. Nimmt man einen Stundenlohn inkl. aller Nebenkosten von € 40 an, dann kostet die ‚Datenwiederherstellung' auf diesem Weg ca. € 2.200.

2. Ein Team aus drei Personen hat insgesamt 2,5 Arbeitstage an einer Kundenpräsentation gearbeitet; die Powerpoint-Präsentation ging bei einem Festplattencrash verloren. Um die Präsentation aus den vorhandenen Brainstorming-Notizen und dem Recherchematerial zu rekonstruieren, braucht das Team noch einmal einen vollen Arbeitstag. Setzt man den Tag mit € 800 pro Person an, kostete diese ‚Datenrettung' das Unternehmen € 2.400.

Unternehmer zum Thema „Wert von Daten"

Rainer Maassen – Geschäftsführer bei maassen & partner, Hersteller von Datenbanklösungen:

„Der Wert von Daten hängt zunächst davon ab, inwieweit diese Daten unternehmenskritisch sind oder nicht. Davon hängt ab, wie weit ein vorübergehender Verlust der Daten bis zur Wiederherstellung Kosten verursacht. Außerdem spielt die Größe des Unternehmens eine Rolle. Die Daten eines Ein-Mann Betriebs können nicht so wertvoll sein wie die Daten eines Konzerns. Deshalb würde ich als Vergleichswert den Jahresumsatz nehmen.
Kategorie 1: Alle Daten aus der Buchhaltung, Auftragsverwaltung und Lohnbuchhaltung sind besonders unternehmenskritisch. Ein Fehlen verursacht sofort erhebliche Kosten, mindestens in Höhe des Umsatzes, der in der Zeit vom Verlust bis zur Wiederherstellung gemacht würde und jetzt nicht gemacht werden kann. Dazu kommen Image-Nachteile usw. Mit anderen Worten: Die Daten sind unentbehrlich. Können Sie gar nicht wiederhergestellt werden, wird Ihr Wert auf bis zu 50% des Unternehmenswertes angesetzt, und der liegt üblicherweise beim 3 - 5fachen des Jahresumsatzes.
Kategorie 2: Daten aus Vertrieb und Marketing, Kundendaten, Projektdaten usw. Deren Wert liegt bei 0,1 bis 0,5 Jahresumsätzen, je nachdem, wie wichtig die Daten für die Kundenbetreuung und die Außenkontakte sind.
Kategorie 3: Interne Daten, die nicht für die Leistungserbringung wesentlich sind. Auch ihre Kosten können erheblich sein."

Frank Brandenburg – Geschäftsführer Clearswift, Anbieter von Lösungen für die Sicherheit digitaler Kommunikation:

„Besonders als Softwareunternehmen wickelt man (fast) alles elektronisch ab. Ein gutes Beispiel dafür ist unsere Support-Datenbank. Wenn diese Daten nicht vorhanden wären, wüssten wir nicht,

1. welche unserer Kunden einen Support-Vertrag haben (und dafür auch bezahlt haben),
2. welche Produkte beim Kunden eingesetzt werden,
3. welche Historie (Updates, bisherige Probleme) der Kunde hat.

Diese Informationen liegen nur elektronisch vor, nicht zu sprechen von ‚banalen' Dingen wie Mailadressen, Telefon-Nummern etc.
Unser gesamtes Renewal- und Support-Geschäft käme damit zum Erliegen. Wenn man dabei gängige Umsatzgrößen bei Softwareherstellern betrachtet, beträgt der Supportanteil zwischen 30 - und 50%.

Diese Aussagen betreffen zunächst einmal Unternehmensdaten, die – wie allgemein üblich – auf einem Fileserver gespeichert und von dort aus auch gesichert werden.

Folgen von Datenverlust

Die Anzahl an Fällen von Datenverlust in Unternehmen und die Schwere der davon ausgelösten finanziellen Folgen nehmen seit Jahren massiv zu. Das liegt daran, dass

- immer mehr Unternehmen immer mehr Daten ausschließlich elektronisch speichern und keine Sicherung in Form von Ausdrucken mehr durchführen;

  Die Gesetzgeber in vielen europäischen Ländern fördern diesen Trend: Sie schreiben die Archivierung von Daten in Papierform nicht

mehr für alle relevanten Wirtschaftsdaten zwingend vor, sondern akzeptieren die elektronische Archivierung. Entsprechende Gesetze sind bereits in Kraft getreten (z.B. in Deutschland) oder liegen zur Verabschiedung vor.

- elektronische Daten immer wichtiger für Unternehmen werden, da viele Geschäftsprozesse inzwischen zu hundert Prozent auf Daten und deren Verknüpfungen beruhen;
- zwar immer bessere Backup-Systeme und -Methoden existieren, diese aber selbst in großen Unternehmen oft nicht konsequent oder unzureichend eingesetzt werden.

  Kroll Ontrack-Recherchen haben ergeben, dass in 80% der Datenverlustfälle scheinbar ordnungsgemäß erstellte Backups existieren, dass sich aber herausstellt, dass sich die Backups in einem nicht verwertbaren Zustand befinden. Backup-Systeme gehen immer davon aus, dass die Hardware und die Speichermedien sich zum Zeitpunkt der Datensicherung in einem intakten Zustand befinden und die gesicherten Daten nicht beschädigt sind. Lagen beim Fahren des Backups aber bereits Beschädigungen an Daten vor, dann wird das Backup diese einfach widerspiegeln. Die benötigten Daten können nicht wie gewünscht restauriert werden.

Man muss kein Schwarzseher sein, um die möglichen Folgen eines Datenverlustes für ein Unternehmen in düsteren Farben zu schildern:

- 93% der Unternehmen, deren Data Center für zehn oder mehr Tage ausfielen, überlebten das folgende Geschäftsjahr nicht.[2]

  Datenverlust ist nicht einfach nur ein Schreckgespenst, mit dem Hersteller von Backup-Systemen ihren Umsatz steigern, sondern bittere Realität. Können Daten tatsächlich einmal nicht von einem Backup restauriert werden, drohen einem Unternehmen massive Folgen bis hin zum Konkurs.

Wie kommt es zu Datenverlust?

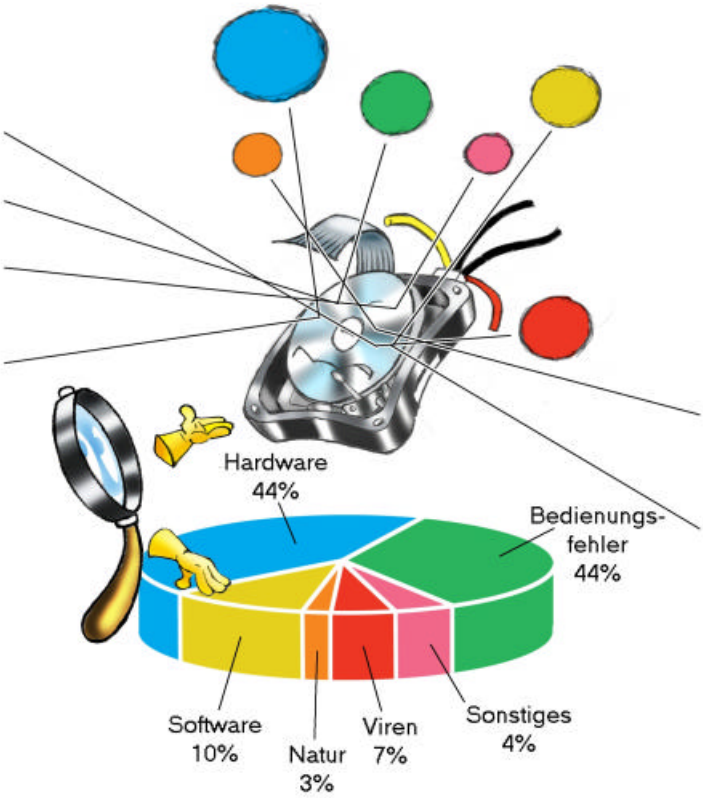
Im Gegensatz zu der in den Medien oft verbreiteten Meinung spielen Naturkatastrophen als Ursache für Datenverlust nur eine untergeordnete Rolle. Tatsächlich beruhen drei Viertel aller Schadensfälle auf Störungen an der Hardware oder auf Bedienungsfehlern.

Die fünf wichtigsten Ursachen für Datenverlust im Überblick:[3]

- Funktionsstörungen der Hardware oder des Systems 44%

  Mögliche Symptome:
  Fehlernachricht, die besagt, dass das Gerät nicht erkannt wird;
  zuvor zugängliche Daten sind plötzlich nicht mehr auffindbar;
  kratzende oder klappernde Geräusche;
  Festplattenlaufwerk dreht sich nicht;

[2] Quelle: National Archives and Records Administration U.S.A, Washington
[3] Quelle: Kroll Ontrack-Studie, 2002



Gründe für Datenverlust

Festplattenlaufwerk des Computers arbeitet nicht.

Gegenmaßnahme:

Schalten Sie den PC nicht immer wieder aus und an, da bei jedem Vorgang noch mehr wichtige Daten verloren gehen können, da dies die Magnetschicht zusätzlich beschädigt.

Vorsorgemaßnahmen:

Schonen Sie elektrische Komponenten, indem Sie Ihren Computer vor Nässe, Licht und Staub schützen.

Vermeiden Sie Spannungsschwankungen durch Verwendung einer unterbrechungsfreien Stromversorgung (USV).

Schütteln Sie Festplattenlaufwerke oder Bänder nicht bzw. entfernen Sie die Abdeckungen nicht.

Stellen Sie sicher, dass Ihr Rechner – und damit auch die Festplatte – ausreichend Kühlung erhält. Überhitzungen können sowohl den Prozessor als auch die Festplatte schädigen.

- Bedienungsfehler 32%

Mögliche Symptome:

Zuvor zugängliche Daten sind plötzlich nicht mehr auffindbar;

Meldungen wie „Datei nicht gefunden" werden angezeigt.

- *es wurde partitioniert*
- *es wurde formatiert*

Vorsorgemaßnahmen:

Führen Sie grundsätzlich keine Aktionen wie Installationen oder Reparaturen durch, mit denen Sie keine Erfahrung haben.

- Software-Fehler o. Funktionsstörungen von Software 10%

  Mögliche Symptome:
  Systemnachrichten mit Bezug auf Speicherfehler;
  Softwareanwendung lädt nicht;
  Fehlernachricht, die besagt, dass Daten beschädigt oder unzugänglich sind.
  Vorsorgemaßnahmen:
  Sichern Sie regelmäßig Ihre Daten;
  verwenden Sie Diagnose-Tools mit besonderer Vorsicht.

- Computerviren 7%

  Mögliche Symptome:
  Leerer Bildschirm;
  seltsames und unvorhersehbares Verhalten der Anwendung;
  Anzeige der Fehlernachricht „Datei nicht gefunden", die einen Virenbefall andeutet;

  Vorsorgemaßnahmen:
  Arbeiten Sie mit einem guten Anti-Virus-Softwarepaket;
  kaufen Sie Software nur bei seriösen Anbietern;
  überprüfen Sie alle eingehenden Daten, einschließlich verpackter Software, auf Viren.

- Sonstiges 4%

- Höhere Gewalt (Naturkatastrophen, Brände etc.) 3%

Gefährdete Speichermedien

Grundsätzlich sind elektronisch gespeicherte Daten stärker gefährdet als Informationen, die auf Papier aufbewahrt werden. Zwar kann auch ein Aktenordner versehentlich weggeworfen werden oder einem Brand zum Opfer fallen – es gibt aber viel mehr mögliche Ursachen für den Verlust digitaler Daten. Hinzu kommt, dass digitale Informationen bis auf wenige Ausnahmen entweder in einem sogenannten flüchtigen Speicher liegen, dessen Inhalt verloren geht, sobald die Stromzufuhr unterbrochen wird, oder auf Medien, die Daten magnetisch (Diskette, Festplatte, Magnetband) oder optisch (CD, DVD) aufzeichnen. Die Struktur solcher Medien kann durch eine Reihe von äußeren Einflüssen verändert werden (mechanisch, thermisch, magnetisch). Geschieht dies, so werden auch die gespeicherten Daten verändert. Darüber hinaus besteht die Gefahr von Datenverlust auch bei mobilen Daten, da Daten von mobilen Geräten, z.B. Laptops, oder mobilen Datenträgern selten so gesichert werden wie die von stationären Systemen.

Magnetisch und optisch gespeicherte Daten auf stationären Systemen

Bei der magnetischen Speicherung von Daten wird jedes einzelne Bit durch eine definierte Menge an Partikeln eines magnetisierbaren Materials dargestellt. Diese Menge ergibt sich aus der Fläche auf dem Datenträger, der wiederum als kleinste physikalische Speicher-

Analyse im Reinraum

einheit definiert wird. Ausgerichtet werden die Partikel (heutzutage in der Regel aus Kristallen von Edelmetalloxiden bestehend) durch elektrische Spannung. In einer Festplatte ist dafür der Schreib-/Lesekopf zuständig, der in Mikrosekundengeschwindigkeit die Polung von Partikeln verändert. Gelesen werden solche Daten auf induktivem Weg: Je nach der Polung wird im Schreib-/Lesekopf negative oder positive Spannung erzeugt. Die Datendichte liegt aktuell bei Werten oberhalb von 6.500 Bytes pro mm². Das veranschaulicht, wie verletzlich magnetisch gespeicherte Daten eigentlich sind.

Beeinflusst werden Magnetpartikel übrigens nicht nur durch magnetische Einwirkung. Der klassische ‚Headcrash', bei dem ein Schreib-/Lesekopf die Oberfläche der Festplatte berührt, führt zu einer physikalischen Beschädigung und damit zu Datenverlust. Hitze und Feuchtigkeit, die im Katastrophenfall einwirken, verändern meist die Struktur des Trägermaterials, so dass sich entweder die Magnetschicht teilweise ablöst oder aber der Träger (die ‚Platte') nicht mehr eben ist, was einen Headcrash zur Folge haben kann.

Die Daten eines Unternehmens werden heutzutage in der Regel zentral gelagert. Der so genannte ‚File Server' muss dabei aber nicht unbedingt ein Rechner mit einem Festplattensystem sein. Die Datenspeicherung kann durchaus auch verteilt stattfinden – z.B. auf mehreren Festplattensystemen an verschiedenen Orten oder in einem eigenen oder angemieteten Data Center. Zum Einsatz kommen dabei meist sogenannte ‚Raid-Systeme', die aus einer beinahe belie-

big ausbaubaren Anzahl einzelner Festplattensysteme bestehen und entsprechend große Datenmengen speichern können.

Für das Backup, sprich die Sicherheitskopie eines Datenbestandes, werden in den meisten Unternehmen nach wie vor Magnetbänder eingesetzt. Magnetbänder haben prinzipiell den Vorteil, dass für die Speicherung einer Informationseinheit mehr Fläche zur Verfügung steht, sodass die Daten magnetisch und mechanisch weniger gefährdet sind als auf einer Festplatte. Die Schreib-Lese-Methode unterscheidet sich nicht grundsätzlich, ist aber bei Magnetbändern insgesamt robuster. Trotzdem sind natürlich auch Magnetbänder – gleich welchen Typs: Streamerkassetten, Minikassetten, DAT etc. – empfindlich gegenüber magnetischen, mechanischen und thermischen Einflüssen.

Als optische Medien werden – besonders im Bereich Datensicherung und mobile Daten – zunehmend auch CDs, DVDs oder magneto-optische Träger (MOs) eingesetzt. Diese sind zwar unempfindlich gegenüber externem Magnetismus, aber vor Datenverlust durch mechanische Beschädigung oder Hitze nicht gefeit.

Mobile Daten[4]

Solange die Informationen zentral gelagert werden, lassen sie sich auch zentral schützen und kontrollieren. Doch wer schützt die Da-

[4] Im Anhang (S. 80) finden Sie eine Auflistung von mobilen Geräten und Datenträgern, die sensible Daten beinhalten können.

ten, die im Umlauf sind, zum Beispiel auf Notebooks, Palm Organizern und Disketten?

Natürlich empfiehlt es sich zunächst, Daten von mobilen Geräten und mobilen Datenträgern genauso zu sichern wie Daten von stationären Systemen. Im Idealfall wird die IT eines Unternehmens entsprechende Mechanismen und Richtlinien einsetzen, damit die Mitarbeiter dies auch tun können und müssen. So setzen sich langsam Lösungen durch, mit denen Außendienstmitarbeiter beispielsweise die Daten von ihrem Laptop über das Internet im Data Center des Unternehmens sichern können. Das Backup von Daten auf PDAs oder Mobiltelefonen bleibt aber in der Regel dem einzelnen Mitarbeiter überlassen, sodass die Datensicherheit hier vom individuellen Verhalten abhängt.

Speichermethoden

Grundsätzlich unterscheiden sich die Speichermethoden bei Platten und Bändern voneinander. Während bei Platten (einschließlich CD-ROMs, DVDs und MOs) die Daten wahlfrei geschrieben und gelesen werden können, sind sie auf Bändern sequenziell gespeichert. Das bedeutet, dass einzelne Datenbereiche bzw. ganze Dateien auf einem Band nur durch Vor- und Rücklauf angesteuert werden können. Bei einer Festplatte sorgt das jeweilige Betriebssystem dafür, dass die Adresse des physikalischen Aufbewahrungsortes eines Da-

tenpartikels in Tabellen abgelegt wird. Diese Information wird dann beim Zugriff auf die gewünschten Daten genutzt.

Bei einer ‚klassischen' Festplatte ist das Betriebssystem dafür verantwortlich, eine solche Tabelle (in der DOS-/Windows-Welt File Allocation Table = FAT genannt) zu erzeugen und zu verwalten. Was PC-Anwender möglicherweise als ‚Formatieren' kennen, ist eigentlich der Vorgang, bei dem eine solche Tabelle angelegt wird. Vereinfacht dargestellt kann man sagen, dass sie zunächst dem jeweils kleinstmöglichen Aufbewahrungsort für ein mindestmöglich abbildbares Datenstück (in der Regel: 1 Byte) eine feste Adresse zuschreibt. Die kleinsten adressierbaren Einheiten einer FAT Dateizuordnungstabelle sind die Cluster.

Wird bei dem populären FAT-Dateisystem, das den meisten Anwendern aus dem täglichen Umgang mit der Windows-Welt vertraut ist, eine Datei gespeichert, sucht das Betriebssystem nach einem freien genauer - freigegebenen Cluster – und schreibt die Bytes der Datei dort hinein. Wird eine Datei gelöscht, gibt das Betriebssystem diesen Cluster wieder frei. Aber die physikalische Datenspeicherung, also die Polung der Magnetpartikel, wird dabei nicht verändert!

Tatsächlich umfasst eine Datei nicht nur einen Cluster, sondern ist i.d.R. um ein Vielfaches größer, d.h. sie belegt mehrere Cluster. Daher ist es meist so, dass der Rest einer Datei den letzten Cluster nicht ausfüllt. Es bleibt Platz (der so genannte ‚Slack') übrig, der noch physikalische Daten von einer alten – bereits gelöschten Datei - enthalten kann, da der Speicherbereich durch das Löschen wieder

freigegeben wurde. Diese Daten können im Dateisystem nicht mehr zugeordnet werden, da sie zu keiner aktuell genutzten Datei gehören.

Diese „versteckten“ Restdaten und der Umstand, dass beim Löschen von Dateien die Daten nicht wirklich entfernt werden, sondern nur aus dem „Inhaltsverzeichnis“ der Festplatte gelöscht werden, damit der benutzte Speicherplatz überschrieben werden kann, bieten der Datenrettung große Chancen, da diese Daten immer noch auf der Festplatte abgespeichert sind. Dies gilt auch für optisch gespeicherte Daten. Auch von überschriebenen Magnetbändern kann man Daten wiederherstellen.

Backup

Methoden der Datenrettung

Eines bleibt festzuhalten: Die einzige und beste Prophylaxe gegen Datenverlust ist ein konsequent durchgeführtes Backup! Aber selbst wenn diese Vorbeugungsmaßnahme in einem Unternehmen optimal verwirklicht wird, bleibt ein Restrisiko. Mit den modernen Methoden der Datenrettung lassen sich jedoch auch Daten wiederherstellen, die nicht aus einem Backup restauriert werden können.

Die Aufgaben der Datenrettung liegen nicht nur in der aufwändigen Wiederherstellung von Datenfragmenten auf beschädigten Datenträgern. Neben dem komplexen Finden und Auslesen von Magnetpartikeln und „Datensplittern“ gibt es zahlreiche Fälle, bei denen es ausreicht, redundante Daten auf gespiegelten Systemen, sogenannten Backups, zu identifizieren oder aus dezentral gesicherten Informationen zusammenzusetzen. Mit der genauen Kenntnis des Betriebssystems, der vorhandenen Netzstruktur und der für diesen Fall geeigneten Werkzeuge zur Datenrettung kann durch einen professionellen Eingriff oft eine rasche und erfolgreiche Datenrecherche eingeleitet werden.

Wiederherstellung der Daten

Aufgrund genauer Systemkenntnisse wissen die Experten, welche Daten in welchen Verzeichnissen, Sektoren oder Segmenten von Datenträgern zu finden sind und was eine rasche und effiziente Wiederherstellung gelöschter Dateien möglich macht. Gelöschte

Daten lassen sich relativ leicht wiederherstellen, sofern mit dem entsprechenden Rechner nicht allzu lange weiter gearbeitet wurde und somit Daten überschrieben wurden. Darüber hinaus lassen sich Datei-Fragmente in freigegebenen Clustern und im Slack-Bereich (von Dateien nicht ausgenutzte Bereiche) der Festplatte auffinden.

Viele verloren geglaubte Informationen lassen sich zudem aus gelöschten E-Mails oder über die Wiederherstellung von Meta-Daten retten. Das sind Informationen, die die Eigenschaften von Datensätzen beschreiben und den inhaltlichen Kontext herstellen. Hier wird deutlich, wie wichtig die genaue Kenntnis von Betriebssystemen und deren Eigenheiten ist.

Daher ist es von großer Bedeutung, dass der Experte genau weiß, wie Dateien, die Lücken haben, aufgefüllt werden können, so dass sie logisch als vollständig 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, sprich deren Dateiinformationsköpfe, beschädigt sind, restaurieren und wieder öffnen, was bei korrupten Dateien sonst vom Betriebssystem verweigert wird.

In rund 60 Prozent aller Fälle ist die Hardware so schwer beschädigt, dass die Festplatte in den Reinraum muss. In einem hochspezialisierten Prozess werden hier die auf der Festplatte gespeicherten Daten wieder verfügbar gemacht und anschließend ausgelesen. Danach werden die geretteten Daten auf ein Backupmedium gespei-

chert (CD, DVD, Bänder) und dem Kunden wieder zur Verfügung gestellt.

Datenrettungsprozess[5]

Der erste Schritt bei der Datenrettung im Labor ist immer der Versuch, alles, was physikalisch auf dem beschädigten Datenträger gespeichert ist, auf ein intaktes Speichersystem zu übertragen. Im einfachsten Fall bedeutet dies, mit einem geeigneten Softwaretool die Daten eins-zu-eins auf ein neues Speichermedium zu übertragen, so dass ein physikalisch vollständig identisches Abbild entsteht.

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 Datenbestandes zu machen. Hier ist dann die gute Zusammenarbeit zwischen Analytiker und Mechaniker gefragt, denn von außen betrachtet sind alle Daten gleich. Nur bei der perfekten Suche nach vorgegebenen Mustern in den logisch als relevant erachteten Sektoren lässt sich zielgerichtet vorgehen. Anders ist eine Recherche auf gigabyte-großen, gelöschten und oft stark beschädigten Datenträgern kaum effizient durchführbar.

[5] Im Anhang (S. 81) finden Sie eine Auflistung der einzelnen Schritte bei der Datenrettung im Labor.

Wenn ein Harddisk-System mechanisch so beschädigt ist, dass sich die Platten nicht mehr drehen oder die Schreib-/Leseköpfe defekt sind, dann muss das Gerät im Reinraum geöffnet werden. In einem solchen – wie bei Kroll Ontrack in Böblingen – herrschen ähnliche Bedingungen wie an den Produktionsstätten der Festplatten. Hier wird dafür gesorgt, dass sich Staubpartikel nicht auf der empfindlichen Plattenoberfläche ablagern können und eine zu hohe Luftfeuchtigkeit nicht zu Kondenswasser auf dem Material führt. Beides könnte zu weiterem Datenverlust führen. Oft werden beschädigte Systeme komplett demontiert, die einzelnen Platten entnommen und in einem neuen Gehäuse mit neuen Schreib-/Leseköpfen und einer neuen Platine wieder zusammengesetzt.

Danach werden im Labor von den Datenrettungsingenieuren die Strukturen des Dateisystems so wiederhergestellt, dass auf die verlorenen, korrupten oder beschädigten Daten wieder zugegriffen werden kann. Je nach Beschädigung kann ein solcher Lesevorgang durchaus einige Stunden, in Ausnahmefällen auch mehrere Tage, dauern.

Remote Datenrettung[6]

Eine andere Möglichkeit bei logischen Fehlern ist die Remote Datenrettung (RDR™) über Modem oder Internet, eine ausschließlich von Kroll Ontrack angebotene und patentierte Lösung. Diese Form der Datenrettung kann in Fällen von Datenverlust genutzt werden, die nicht aufgrund einer Beschädigung des Speichermediums entstanden sind, sondern durch logische Fehler, wie z.B. korrupte Dateisysteme, Fehlbedienung oder Viren ausgelöst wurden.

Grundsätzlich möglich ist die Remote Datenrettung immer dann, wenn ein Laufwerk physikalisch gesund ist. Dann können die Daten auf diesem Laufwerk über eine gesicherte Verbindung direkt bearbeitet und wiederhergestellt werden. Dabei wird ein Verfahren eingesetzt, bei dem eine Maske über die Kundendaten gelegt wird und so die darunter liegenden Daten nicht noch mehr beschädigt oder überschrieben werden können. Auf dieser Maske arbeitet der Datenrettungs-Ingenieur. Die geretteten Daten können danach entweder auf die Harddisk oder auf ein separates Medium beim Kunden kopiert werden, so dass dieser sofort wieder direkten Zugriff darauf hat. Dabei ist es egal, ob es sich um einen Server, Desktop oder Laptop handelt. Kroll Ontrack setzt ein eigenes (geheimes) Übertragungsprotokoll ein, das durch Datenverschlüsselung auf Paketbasis zusätzlich optimiert wird. Bei dieser Art der Datenverschlüsselung

[6] Im Anhang (S. 82) finden Sie die Schritte, wie eine Remote-Datenrettung abläuft.

Arten der Datenrettung

wird die Gesamtdatenmenge in einzelne Dateien kodiert, so dass die Sicherheit gewährleistet ist.

Für die Kunden hat dies erhebliche Vorteile, insbesondere, was den Zeitaufwand für die Datenrettung angeht. Schließlich muss bei einer Standard-Datenrettung im Labor – abgesehen von der Zeit für Einsenden und Zurückschicken der Medien – oft mit drei bis fünf Tagen gerechnet werden. RDR™ steht dagegen 24 Stunden am Tag zur Verfügung und ist die schnellste Form der Datenrettung. Möglich ist die Remote Datenrettung derzeit für folgende Betriebssysteme:

- DOS
- Windows 3.x, 95, 98, Me, 2000, NT und XP
- Linux
- Sun Solaris
- Novell NetWare

sowie für

- Microsoft SQL
- Microsoft Exchange Server
- Outlook pst. Files

Logische Problemfälle können fast immer mit der Remote Datenrettung gelöst werden. Es gibt sehr oft eine Reihe typischer Situati-

onen, in denen dieses Verfahren die schnellste und kostengünstigste Variante darstellt wie zum Beispiel bei der Wiederherstellung:

- von RAID-Systemen
- von MS Exchange Servern
- von MS SQL Servern
- nach einem Virusangriff
- versehentlich gelöschter Daten.

Datenrettung mit Software-Tools

Es gibt auch Software Tools mit denen der Anwender selbst verloren gegangene Daten wiederherstellen kann.

Do-it-yourself-Datenrettung ist möglich bei:

- Versehentlich gelöschten Daten
- Korrupten Daten nach Virenbefall
- Nichtzugreifbaren Daten aufgrund von Partitionierungsproblemen.
- Formatierten Datenträgern

Selbst die einfachste Datenrettungs-Software ist in der Lage, versehentlich gelöschte Dateien auf einem DOS- oder Windows-PC wiederherzustellen, so lange kein Schreibvorgang nach dem Datenverlust durchgeführt wurde. Der Einsatz solcher Tools ist nur dann

ratsam, wenn ganz sicher ist, dass die verschwundenen Dateien tatsächlich gelöscht wurden und nicht durch andere Ursachen verloren gegangen sind.

Datenrettungsunternehmen wie Kroll Ontrack setzen inzwischen auf eine Mischung von Do-it-yourself-Verfahren und Datenrettungs-Services. Mit der Softwarefamilie Ontrack EasyRecovery™ stehen dem Anwender einige der Tools zur Verfügung, die auch bei der professionellen Datenrettung im Labor zum Einsatz kommen. Bei der Anwendung in Eigenregie gelten jedoch diverse Vorsichtsmaßnahmen. Die Software darf beispielsweise nicht auf der betroffenen Partition installiert werden.

Erfolgreich gerettete Daten

Tipps & Tricks für den Ernstfall

1. Zunächst gilt es Ruhe zu bewahren. Egal was passiert ist, gehen Sie davon aus, dass die Daten in 80% aller Fälle wiederherstellbar sind. Tätigen Sie keine übereilten Handlungen!

2. Defekte Hardware führt oft zu Fehlverhalten der Datenträger. Schalten Sie den PC deshalb nicht ein, wenn Sie vermuten, dass es – zum Beispiel bei einem Blitzeinschlag – zu Überspannung in Ihrem Netz gekommen ist. Lassen Sie den PC ausgeschaltet.

3. Bei einem Festplattencrash hören Sie oft ungewöhnliche Geräusche, z.B. Klackern oder hohe Töne. In diesem Fall gilt es, keinesfalls selbst Hand an die Hardware zu legen. Lassen Sie das System ausgeschaltet. Ein Neustart könnte die Festplatte endgültig zerstören.

4. Verwenden Sie keine Datenträger, die Hitze, Feuchtigkeit oder Verrußung ausgesetzt waren, da die Daten unwiderruflich verloren gehen können, wenn der Datenträger nicht in der staubfreien Umgebung eines Reinraums behandelt wird.

5. Unterlassen Sie das Schütteln des Datenträgers und öffnen Sie bei Festplatten nicht das Gehäuse.

6. Durch Wasser beschädigte Datenträger sollten feucht gehalten (im Wasser lassen oder in feuchte Tücher einwickeln) und sofort ins Labor gebracht werden.

7. Beschädigte Datenträger können bei einem weiteren Betrieb unwiederbringliche Schäden erleiden, auch wenn Sie noch einige Datensätze kopieren können. Diese Datenträger sollten nicht weiter verwendet werden.

8. Probieren Sie niemals, Datenträger selbst zu säubern. Am besten senden Sie den Datenträger an ein Datenrettungs-Labor.

9. In vielen Fällen lassen sich die verlorenen Daten mit speziellen Software-Programmen (z.B. Ontrack EasyRecovery™) in Eigenregie wiederherstellen. Setzen Sie solche Tools jedoch nicht ein, wenn die Anzeichen auf einen Hardware-Defekt deuten und der Computer beispielsweise ungewöhnliche Geräusche von sich gibt.

10. Wenden Sie sich unbedingt an ein Fachunternehmen für Datenrettung, wie z.B.:

    Kroll Ontrack GmbH
    Hanns-Klemm-Straße 5
    71034 Böblingen
    Telefon: +49 (0)7031/644-150
    kostenlose Hotline: 0800/10121314 (D); 0800/644150 (A); 0800/880100 (CH)
    Fax: +49 (0)7031/644-144
    E-Mail: info@krollontrack.de; info.suisse@krollontrack.ch; info@krollontrack.at
    Internet: www.krollontrack.de; www.ontrack.de;

www.krollontrack.ch; www.krollontrack.at

11. Geben Sie folgende Informationen an:
    - eingesetztes Betriebssystem;
    - Art, Hersteller und Modell des betroffenen Speichermediums;
    - Speicherkapazität des Mediums;
    - Art des Problems, Symptome, Umstände des Datenverlustes;
    - Was wurde bisher unternommen?
    - Wurde ein Virenscanner eingesetzt?
    - Hatten Sie in letzter Zeit ein Virenproblem?
    - Haben Sie bereits selbst versucht, mit einem Tool die Daten zu retten?
    - Welche Daten sind wichtig?

Datenmissbrauch unter der Lupe

Elektronische Beweismittelsicherung auf der Basis von Computer Forensik

Einführung: Daten und Datenmissbrauch[7]

„Die Bedeutung des PCs 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, Bundesminister des Innern.

Mit diesen Worten würdigte Otto Schily anlässlich des 20. Jahrestags der Gründung von Microsoft einerseits die rasante Entwicklung des PCs und seiner Möglichkeiten, warnte aber andererseits gleichzeitig vor den Risiken. Das Speichern und Abrufen allzeit verfügbarer Informationen, das Aufbewahren und Übermitteln von Daten in Sekundenschelle 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

[7] Im Anhang (S. 83) finden Sie eine Auflistung von Indizien, die ein Unternehmen zur Vorsicht mahnen sollte.

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 nachvollziehbar. 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.

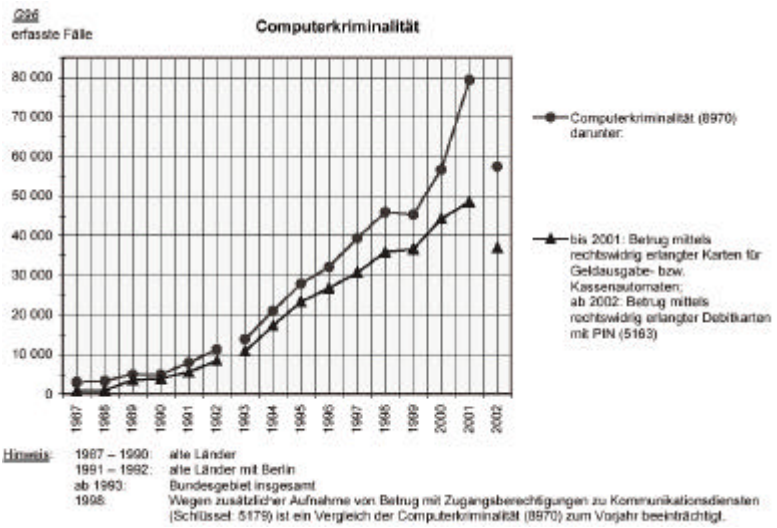
Gefahren erkennen, Fehler vermeiden

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 Vorsichtmaßnahme 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 Schadensbegrenzung und Täterermittlung.
Computer Forensik ist das zentrale Element für gerichtsfeste Beweissicherung und fundierte Analyse des verfügbaren Materials. 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 auch die Pflicht, sich 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.

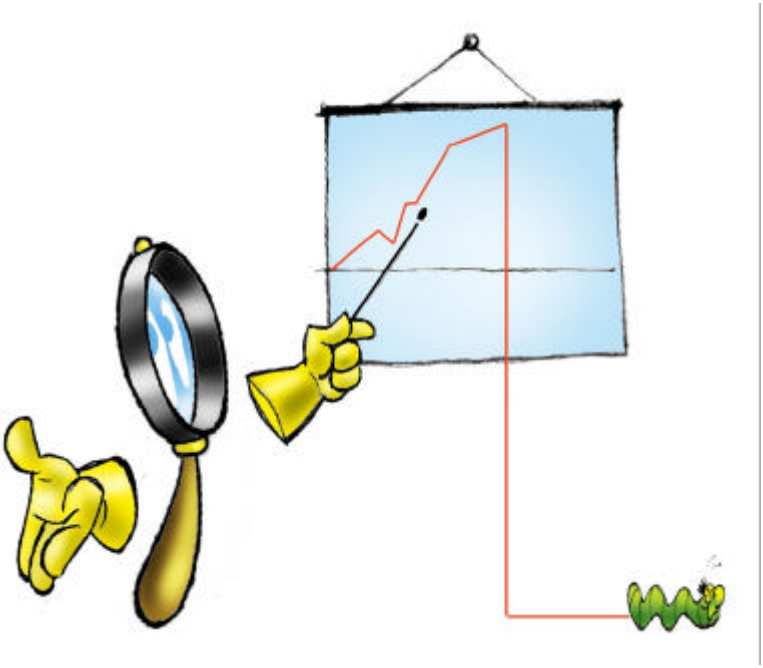
Statistische Bewertung[8]

Die Computer Forensik als Instrument der Wiedergewinnung beweiskräftiger Daten und der Identifikation von Beweismaterial auf Computersystemen ist bei der hohen Computerkriminalität in Deutschland ein zentrales Ermittlungsinstrument. 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 2002, Bundeskriminalamt Wiesbaden, Seite 238 unter http://www.bka.de/pks/pks2002/index2.html

[8] Im Anhang (S. 84) finden Sie eine Auflistung über Varianten der Wirtschaftskriminalität mittels Computer.



Wirtschaftliche Folgen von Datenverlust

Die Kriminalstatistik dokumentiert das rasante Wachstum der Computerkriminalität von 1987 bis 2001. Trotz des Rückgangs im Jahr 2002 kann nicht von einer Entwarnung gesprochen werden, da es eine hohe Dunkelziffer gibt, die in keiner Statistik auftaucht. Darüber hinaus hat von 2001 auf 2002 die Datenveränderung und Computersabotage um 53,9 Prozent zugenommen. Gründe hierfür sind unter anderem die steigende Anonymität der PC-Nutzer und die Angst vor einem Jobverlust. Nur ein kleiner Bruchteil der Delikte kommt tatsächlich zur Anzeige, die eigentliche Dunkelziffer der Computerkriminalität liegt um ein Vielfaches höher.

Fallentwicklung und Aufklärung (Tabelle 01)

Bereich: Bundesgebiet insgesamt

7232

Schlüssel	Straftaten(gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2002	2001	absolut	in %	2002	2001
8970	Computerkriminalität	57 488	79 283	-(21 795)	-(27,5)	50,0	56,8
	davon:						
5163	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	38 969	-	x	x	40,5	41,7
5175	Computerbetrug -§263a StGB-	9 631	17 310	-7 779	-44,9	57,0	77,9
5179	Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	5 902	8 039	-2 137	-26,6	77,1	84,2
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	228	920	-692	-75,2	80,7	95,8
6742	Datenveränderung, Computersabotage -§§ 303a, 303b StGB-	1 327	862	465	53,9	38,1	45,4
6780	Ausspähen von Daten	806	1 463	-657	-44,9	64,4	82,6
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	1 947	1 672	275	16,4	96,1	99,2
7152	Softwarepiraterie in Form gewerbsmäßigen Handelns	780	410	370	90,2	95,1	96,1

Hinweis: Durch eine inhaltliche Änderung des Schlüssels '5163' ist ein Vergleich des Summenschlüssels Computerkriminalität (8970) mit dem Vorjahr nur eingeschränkt sinnvoll.

Quelle: Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, PKS Berichtsjahr 2002, Bundeskriminalamt Wiesbaden, Seite 238 unter http://www.bka.de/pks/pks2002/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[9] und einem Rahmenbeschluss über Angriffe auf Kommunikationsnetze und Informationssysteme[10].

Im Europarat wurde Ende 2001 von den 44 Mitgliedsländern des Europarates und ihren Partnern USA, Kanada, Japan und Südafrika eine internationale Konvention über Cyberkriminalität verabschiedet. Auch der Praxis der Strafverfolgung nimmt sich die Europäische Union an, beispielsweise im geförderten Projekt CTOSE (Cyber Tools Online Search for Evidence)[11], das versucht, die manipulationssichere Speicherung und gerichtstaugliche Aufbereitung von Beweisen bei computerbasierten Verbrechen im Internet einheitlich zu definieren.

[9] A5-0284/2001, Quelle: http://www.europarl.eu.int/meetdocs/ committees/libe/20020708/472956de.pdf
[10] A5-0328/2002, Quelle: http://www2.europarl. eu.int/omk/sipade2?PUBREF=//EP//NONSGML+REPORT+A5-2002-0328+0+DOC+PDF+V0//DE&L=DE&LEVEL=3&NAV =S&LSTDOC=Y
[11] Quelle: http://www.ctose.org/

Aufgabenbereiche der Computer Forensik[12]

Die neue Dimension und die Geschwindigkeit, die Kriminalität durch Computer und weltweite Netzwerke erhält, zeigen wie anfällig unsere Informationsgesellschaft gegen kriminelle Attacken ist. Gleichzeitig ist sie wenig vorbereitet bei der Strafverfolgung und der dazu notwendigen Beweiserhebung. Das Gebiet der Sicherung und Wiederherstellung von Daten, der Recherche und Analyse von Indizien in vornehmlich digitaler Form sowie ihre gerichtsfeste Dokumentation, ist Fokus der Computer Forensik, die somit zu einem der wichtigsten Beweisermittlungsinstrumente 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.

Ein Großteil aller PC-Dokumente – immerhin werden 90% 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

[12] Im Anhang (S. 86) finden Sie eine Auflistung, wann die Computer Forensik helfen kann.

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 wiederherstellen 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.

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

Computerkriminalität ist nicht auf Konzerne und Großunternehmen beschränkt, sondern findet ebenso wie andere Wirtschaftsverbrechen - Betrug und Spionage - immer und überall statt. Somit bleibt auch Computer Forensik als Maßnahme zur Beweissicherung nicht allein Großunternehmen 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, Geschäftsführern sowie Anwälten, Richtern, Staatsanwälten und Ermittlern vorhanden sein, lange bevor es um konkrete Verdachtsmomente oder gar Strafverfolgung geht. Zur

frühzeitigen Kontrolle von Entwicklungen, die für ein Unternehmen kritische Folgen haben könnten und zur Ergreifung entsprechender Sicherheitsmaßnahmen, sind Unternehmen und Geschäftsführungen durch das KonTra-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 um die 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. 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 sind nur einige Beispiele.

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 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.

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 Beweiskraft des vorhandenen Materials darf hierbei nicht beeinträchtigt werden. 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.

Mobile Daten[13]

Informationen, die zentral gelagert werden, lassen sich auch zentral schützen und kontrollieren, doch bei Daten, die im Umlauf sind, ist die Sicherung schwieriger. 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 verbreitet, 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 wiederherstellbar sein sollen, bieten ein großes, weil unsichtbares Sicherheitsrisiko.

[13] Im Anhang (S. 80) finden Sie eine Auflistung aller mobilen Geräte und Datenträger, die sensible Daten beinhalten können.

Computer-forensische Untersuchung

Schon die Beschreibung eines durchaus üblichen Ablaufs – wie die Vorbereitung einer Präsentation - macht transparent, wo die kritischen Punkte der Datensicherheit liegen. Beinahe selbstverständlich, dass kein Mensch den integren Mitarbeiter daran hindert, Dokumente, die er zur Vorbereitung seines Vortrags auf dem Arbeitsplatzrechner gespeichert hat, 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 ihm die neuen Informationen 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 vorliege 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.

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 relevan-

ten 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 leiden – Chemie, Bio- und Gentechnologie, Elektronik, Automobil und Telematik – 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.

Bei der Wirtschafts- und Industriespionage liegt der geschätzte jährliche Schaden zwischen 5 und 10 Milliarden Euro mit steigender Tendenz. Betroffen von der Wirtschaftspionage 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 % 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 sind, die per E-Mail diskutiert wurden. Sowohl die Mails als auch die verworfenen Geschäftberichte 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 sind, 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 es nötig, das sich das Unternehmen gegen Computerspionage, -sabotage und andere kriminelle Handlungen schützt. Dies 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 wie 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% 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 kon-

kretem 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. Teledienstegesetzes. 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."[14]

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

[14] Quelle: http://www.bfd.bund.de/information/DS-Konferenzen/oh_email.pdf

von Arbeitnehmer und Arbeitgeber unterzeichnet ist und welche kontrolliert und geahndet wird.

Es ist im Interesse aller Arbeitnehmer und trägt zur Sicherung der Arbeitsplätze bei, dass ein Unternehmen sensibel 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 unbedingt 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 mehr als 17 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 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 Plattenhersteller (Fujitsu, IBM, Maxtor, Quantum, Samsung, Seagate, Toshiba und Western Digital) setzen auf den Ontrack Disk Manager® als optionales Installations-Werkzeug. Solch 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.

Leitfaden der Computer Forensik

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, Daten eines Datenträgers wiederherzustellen, da sich die relevanten Daten des Datenträgers im Netzwerk auf anderen Rechnern, wie 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.

Erste Schritte

Vor dem Eintreffen eines Computer Forensik Experten ist es wichtig, die Situation ganz nüchtern in Augenschein zu nehmen, allerdings nur in Augenschein. Die betroffenen Rechner sollten 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 Arbeitspeichers 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 lau-

fenden Programme auf einem externen, neuen Datenträger sichern. Auch sollte 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.

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 stehen die Ingenieure von Kroll Ontrack mit dem zuständigen Projektmanager stets in Verbindung.

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 der Datenspeicher ohne Veränderung der Meta-Daten bitgenau gesichert 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 Laufwerktechniken 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. Hier-

für 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, also ein Abbild einer Festplatte oder Partition, 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 Compu-

ter Forensik Experten selbst dann mit überzeugenden Erfolgsquoten, wenn Täter versucht haben, belastende Daten zu vernichten, und zunächst der Zugriff auf beschädigten Speicher-Medien wiederhergestellt werden muss.

Für die Authentizität des Datenmaterials ist entscheidend, dass physikalisch fehlende Daten – beispielsweise Worte in einem Dokument oder einer E-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%. 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 Löschversuchen 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 geradezu 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 Deduplikation, bei der Informationen, die mehrfach in identischer Form gespeichert sind, zur Reduktion der Datenmenge ausgefiltert werden. Vervielfältigungen liegen vor, wenn Programme Daten in identischer Form in verschiedenen Verzeichnissen speichern. So können zum Beispiel E-Mails als Entwürfe und an mehrere Adressaten versandte Objekte oder leere Seiten in Dokumenten gespeichert werden. Diese Daten bieten keinerlei Information, liefern aber Speicher- und Untersuchungsbedarf. 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 ElectronicDataInverstigator eine eigene Dokumentationsmethode bereit, mit der sich die Ergebnisse der Untersuchung online am Bildschirm abrufen, durchsuchen und präsentieren lassen. Mittels eines weiteren Tools, des Kroll Ontrack ElectronicDataViewer, kann auch im Gerichtssaal die Betrachtung des vorsortierten, markierten Datenmaterials online und live erfol-

gen. Darüber hinaus lassen sich alle Daten zur Unterstützung der Prozessführung auch in adäquater, vollständiger Form ausdrucken und – zum schnelleren Rückgriff – in eine Datenbank importieren.

Die Computer Forensik Experten von Kroll Ontrack erstellen bei Rechtsfällen spezielle Berichte über die ermittelten und analysierten Daten. 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.

Hilfe im Krisenfall

Tipps & Tricks im Krisenfall

Sofortmaßnahmen bei Verdacht.

Wenn Sie den Verdacht haben, dass in das Netz Ihres Unternehmens eingebrochen wurde, 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, hektische 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 bestätigen können, dass keine Daten verändernden Eingriffe vorgenommen wurden.
- Verschließen 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 durch falsche Behandlung der Daten und Geräte und falsche Einschätzung beziehungsweise Nicht-Erkennen der Situation verloren geht. 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 Schadens 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

Telefon: +49 (0)7031/644-150;
kostenlose Hotline: 0800/10121314 (D);
0800/644150 (A) 0800/880100 (CH)
Fax: +49 (0)7031/644-144
E-Mail: info@krollontrack.de; info.suisse@krollontrack.ch;
info@krollontrack.at

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?

Porträt Peter Böhret

Geboren 1959 in Göppingen studierte Peter Böhret Informatik in München und Betriebswirtschaft mit den Schwerpunkten Marketing und Computer in Stuttgart. Er begann seine Karriere als Software Ingenieur, Projekt-Manager und Sales-Manager bei Stark Systemstechnik und als Sales-Manager bei der Hengstler GmbH, bevor er 1996 zunächst als Sales Manager und dann als European Business Development-Manager bei der Ontrack DataRecovery GmbH tätig wurde. Im März 1999 wurde er Managing Director. Mit der Umfirmierung zur Kroll Ontrack GmbH wurde die GmbH einer von fünf Geschäftsbereichen der Kroll Inc., die verschiedene Sicherheitsdienstleistungen bis hin zu umfassenden Lösungen für Unternehmen in der gesamten Welt bereitstellen. Peter Böhret nimmt auch bei der neufirmierten Kroll Ontrack GmbH den Posten des Managing Directors wahr.

Neben seiner Tätigkeit als Geschäftsführer machte sich Böhret mit zahlreichen Veröffentlichungen im Bereich IT-Sicherheit und Software u.a. als Co-Autor des Buches ‚Der Mensch in der Software-Entwicklung' einen Namen.

Unternehmensporträt Kroll Ontrack GmbH

Die Kroll Ontrack GmbH mit Sitz in Böblingen ist das deutsche Tochterunternehmen der international tätigen Kroll Ontrack Inc., die als 100% Tochtergesellschaft von Kroll Inc. in den Bereichen Datenrettung und elektronische Beweissicherung (Computer Forensik) tätig ist.

Als führender Anbieter im Bereich Datenrettung hilft die Kroll Ontrack GmbH mit zahlreichen Service- und Software-Lösungen, in denen Hunderte selbst entwickelter Werkzeuge und Methoden zum Einsatz kommen, sowohl Unternehmen als auch Privatpersonen, wichtige Daten zu sichern und wiederherzustellen.

Im Zuge der Fusion mit Kroll Inc. im Juni 2002 operiert Kroll Ontrack nun als Technology Services Group von Kroll und ist damit einer von fünf Geschäftsbereichen, die mit Dienstleistungen im komplexen Geschäft der Bereitstellung von umfassenden Sicherheitslösungen für Unternehmen in der ganzen Welt befasst sind. Momentan beschäftigt Kroll Ontrack weltweit etwa 400 Mitarbeiter – davon rund 40 in Deutschland. Aufgrund der hohen Nachfrage nach professioneller Datenrettung expandierte das Unternehmen in den vergangenen sechs Jahren stark und eröffnete zusätzlich zum Hauptsitz in Minneapolis Niederlassungen und Labore in Los Angeles, New York, Washington D.C., Tokio, London, Paris, Böblingen, Berlin, Wien, Mailand und Lugano. In Polen ist Kroll Ontrack über den Lizenzpartner MBM Ontrack vertreten.

Kroll Ontrack Computer Forensik Dienstleistungen – Beratung, Sicherstellung und gerichtstaugliche Ermittlung von Daten

Das Gebiet der Wiederherstellung und Sicherung von z.B. gelöschten 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 Beweisermittlungsinstrumente 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.

In Zusammenarbeit mit Unternehmensmanagement, Anwälten oder Strafverfolgungsbehörden suchen die Computer Forensik Spezialisten nach elektronischen Beweisen (elektronischen Fingerabdrücken) innerhalb der EDV. Hierbei kommt der professionellen Vorgehensweise eine besondere Bedeutung zu, da schon kleinste Fehler zur Vernichtung von elektronischen Spuren führen können. Jeder einzelne Schritt, angefangen bei der Beratung über die Erfassung der relevanten Daten bis hin zur Erstellung des Abschlussberichts, wird nachvollziehbar dokumentiert, so dass die gefundenen und reproduzierten elektronischen Dokumente als Beweismittel (Augenscheinsobjekte, Sachverständigenbeweis) auch vor Gericht und vor jedem gerichtlichen Sachverständigen jederzeit standhalten.

‚Ontrack Datenrettung Services' – In rund 80% Prozent aller Fälle kann geholfen werden

Die Wiederherstellung von Daten, die durch mechanische und elektromagnetische Defekte, Bedienungsfehler, Viren, Naturkatastrophen oder Computerkriminalität beschädigt oder zerstört worden sind, ist eine Kernkompetenz des Unternehmens. Dabei gelingt es den Experten von Kroll Ontrack, in rund 80% Prozent aller Fälle – unabhängig vom Speichermedium und dem eingesetzten Betriebssystem – alle wichtigen Kundendaten wiederherzustellen. Eine Erfolgsquote, die für sich spricht und bisher in der Branche unerreicht ist.

Weltweit wurden bislang weit mehr als 165.000 erfolgreiche Datenrettungen bei Kunden aller Branchen durchgeführt. Da die Fälle oft sehr unterschiedlich sind, bietet Kroll Ontrack, in Abstimmung auf den Sachverhalt und die Bedürfnisse des Kunden, mehrere Service-Varianten an:

Die traditionelle Datenrettung findet im Kroll Ontrack Labor statt. Hier bearbeiten Datenrettungsingenieure den Datenträger mit eigens entwickelten Instrumenten und Werkzeugen, um dessen ursprüngliche Struktur wiederherzustellen. Physikalische Schäden im Inneren der Festplatte werden in hauseigenen Reinräumen bearbeitet.

Als einziges Unternehmen bietet Kroll Ontrack bei nahezu 50% der Fälle von Datenverlust die patentierte Remote DataRecovery™ an,

die über Modem- oder Internetverbindung direkt im System des Kunden erfolgt. Sie ist die derzeit schnellste und bequemste Methode der Datenrettung, da sie ohne Ausbau der Festplatte durchgeführt werden kann. Dadurch werden teure und unnötige Ausfallzeiten reduziert, denn in den meisten Fällen ist der Rettungsvorgang schon nach wenigen Stunden erfolgreich abgeschlossen.

Für dringende Fälle stehen der 24-Stunden-Notfall-Service und der Express-Service zur Verfügung. Für weniger zeitkritische Fälle bietet Kroll Ontrack den Standard-Service an.

Ontrack PowerControls™ - Die Mailbox Management Software

Mit Ontrack PowerControls™ gibt Kroll Ontrack Microsoft Exchange Administratoren ein einfaches und zugleich leistungsstarkes Softwaretool an die Hand, mit dem aus .edb-Files einzelne E-Mails oder ganze Mailboxen schnell und unkompliziert wiederhergestellt werden können. Mit Ontrack PowerControls™ können Mailboxen und Ordner aber auch jede beliebige Anzahl von Nachrichten und Anhängen wiederhergestellt werden. Mit einer leicht bedienbaren Benutzeroberfläche kann mit den Dateien genauso interaktiv gearbeitet werden, wie der Administrator dies von Microsoft® Outlook® gewohnt ist. Durch eine Suchfunktion kann zudem mailboxübergreifend nach Stichworten oder Daten gesucht werden. Mit Ontrack PowerControls™ spart der Administrator viel Zeit, da er

nicht, wie beim herkömmlichen Restore, einen zweiten Exchange-Server aufsetzen muss, sondern direkt von einem Client auf das .edb-File zugreifen kann. Auch bei System-Abstürzen kann – ohne großen Aufwand – auf jede einzelne E-Mail seit dem letzten Backup zugegriffen werden. Ontrack PowerControls™ erübrigt so ein Single-Mailbox-Backup. Mit dem integrierten Extract Wizard hat der Administrator die Möglichkeit, direkt aus einem vorhandenen Backup die .edb auf einen Rechner ohne Exchange Umgebung zu extrahieren und dann mit Ontrack PowerControls™ ausgewählte Inhalte aus einer Datenbank in einen Live Server einzuspielen.

Ontrack EasyRecovery™ Serie: Unterstützung bei Datenverlust

Mit der Ontrack EasyRecovery™ Serie bietet Kroll Ontrack eine Software für die Datenrettung und -reparatur an. Diese stellt eine ökonomische Lösung für solche Fälle von Datenverlust dar, die nicht der Expertise eines Datenrettungsingenieurs bedürfen. Der größte Teil der auftretenden Schadensfälle bei strukturellen Problemen kann mit der Ontrack EasyRecovery™ Software schnell und kostengünstig behoben werden. Die Repair-Funktion widmet sich dem Problem, wenn nicht mehr auf Dateien zugriffen werden kann, weil eine Datei beschädigt ist. Die Software repariert beschädigte Microsoft® Office-Dateien und stellt sie als neue, lesbare Dateien wieder her.

Zuverlässiges Löschen von Daten mit Ontrack DataEraser™

Die Software Ontrack DataEraser™ löscht sicher firmeninterne und vertrauliche Daten. So sind zum Beispiel bei der Rückgabe von Leasing-Geräten, einem User-Wechsel oder bei der Weitergabe eines PCs die ursprünglichen Daten vor dem Zugriff Dritter geschützt. Mit diesem Programm lassen sich Daten schnell und effizient durch mehrfaches Überschreiben der Festplatten löschen, so dass eine Wiederherstellung der Daten unmöglich ist.

Ontrack Data Advisor™ - ein leistungsfähiges Diagnose-Tool!

Ontrack Data Advisor™ ist ein einfach anzuwendendes und zugleich leistungsfähiges Diagnose-Tool für Computersysteme. Durch die Identifikation von Problemen, die zu einem Datenverlust führen können, stellt Ontrack Data Advisor™ schnell fest, ob das Festplattenlaufwerk, die Dateistrukturen und der Computerhauptspeicher in Ordnung sind. Ontrack Data Advisor™ bootet automatisch, eine Diagnose wird auch dann ausgeführt, wenn das System nicht läuft.

Anhang

Mobile Geräte und Datenträger, die sensible Daten beinhalten können:

- Notebooks, Laptops und Präsentationssysteme
- Pocket PCs, Palm Organizer, Psion Handheld Computer (EPOC) und andere PDAs
- Mobiltelefone, Diktiergeräte und Fotoapparate
- Disketten
- Magneto-Optische Platten (MOs)
- CD-Rs und CD-RWs
- DVD-Rs und DVD-RWs, DVD+Rs und DVD+RWs
- Streamerkassetten und Magnetbänder
- Wechselplatten (Harddisk, ZIP, JAZ, u.a.)
- Compact-Flash-Speicher oder Microdrives
- Smart Medias
- Memory Sticks
- Secure Digital oder Multi Media Cards

Die Schritte bei der Datenrettung im Labor

- Wenden Sie sich an ein Datenrettungsunternehmen (z.B.: Kroll Ontrack GmbH, +49 (0)7031/644-150 oder 0800/10 12 13 14 (D); 0800/644150 (A); 0800/880100 (CH)
- Verpacken Sie das betroffene Speichermedium entsprechend den Anweisungen und schicken Sie es an das Labor des Datenretters.
- Der Datenrettungsspezialist führt eine Diagnose durch und informiert Sie über das Ergebnis.
- Nach der Auftragserteilung durch Sie wird die Datenrettung vorgenommen.
- Die rekonstruierten Daten werden auf CD/DVD, Magnetband o.ä. gesichert.
- Die Daten werden Ihnen zugeschickt, und Sie können diese wieder in Ihr System einspielen.

Und so läuft eine Remote-Datenrettung ab:

Sie stellen eine Verbindung zu einem der RDR™-Server her; dazu benutzen Sie den speziellen Client, der Ihnen mit dem RDR™-QuickStart-Paket zur Verfügung gestellt wird. Diese Software können Sie in der zu Ihrem Betriebssystem passenden Version bekommen. Für den Fall, dass Ihr System nicht mehr hochfährt sogar auf einem bootfähigen Datenträger.

Über diese Verbindung treten Sie in Kontakt mit einem der Kroll Ontrack-Ingenieure.

Dieser RDR™-Ingenieur kann mit einer speziell entwickelten Software eine Analyse Ihrer Daten durchführen; zuvor wird ein Tool installiert, das alle Veränderungen an den Daten aufzeichnet und veränderte Daten sichert, so dass Ihr System im Zweifelsfall komplett in den Ausgangszustand versetzt werden kann. Die Analyse durchläuft üblicherweise die folgenden Schritte:

- Test auf physische Integrität des betroffenen Systems;
- Einschalten des Track-/Backup-Tools;
- Ermittelte Probleme werden behoben und Veränderungen geschrieben;
- der RDR™-Ingenieur beendet die Verbindung, Sie booten das System neu;
- Sie haben wieder Zugriff auf Ihre Daten!

Ziel der RDR™ ist es, dass der Rechner wieder booten kann und wieder Zugriff auf die Daten besteht.

Alle Achtung! Hier sollten Sie aufpassen.

Indizien, die ein Unternehmen zur Vorsicht mahnen sollten, sind,

- wenn der Mitbewerber 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, Geschäftpartner, Kunden, Behörden mitunter sogar Mitbewerber 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.

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 Passworterschleichung
- Computerspionage – Ausforschung von Patenten, Forschung und Entwicklung, Buchhaltung, Vertriebs- und Kundendaten durch Hacking, Kopien oder unrechtmäßige 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 Programmkopien (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.

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 aufwändig 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 ihren 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.

Glossar

Authentizität

Mit Hilfe der Authentizität wird sichergestellt, dass eine Meldung tatsächlich von derjenigen Person oder Institution stammt, welche sich als Absender ausgibt.

Authorization

Auch: "Berechtigung" - Das Recht eines Anwenders, auf bestimmte Daten (nur) mit definierten Funktionen wie Lesen, Ändern, Einfügen oder Löschen zuzugreifen. Diese Rechte werden von einem Administrator vergeben.

Backup

Sicherheitskopie eines Datenbestandes.

Benchmark

Maßstab für einen Leistungsvergleich - sei es für Hard- und Software oder eine Dienstleistung.

Beta-Version

Eine lauffähige, aber noch nicht endgültige Version eines Programms. Solche Programmfassungen werden von Fachhändlern und ausgesuchten Testpersonen ausprobiert, um letzte Fehlerquellen zu finden.

Betriebssystem

Betriebssysteme sind die derzeit wichtigsten PC-Programme. Ohne Betriebssystem läuft kein Computer: Sie verarbeiten vom Benutzer eingegebene Daten, verwalten die gespeicherten Dateien und kontrollieren angeschlossene Geräte wie Drucker und Festplatten. Gleichzeitig dienen sie als Basis für Anwenderprogramme wie Text- und Dateiverarbeitung, die ohne den Unterbau des Betriebssystems nicht laufen können.

Mit der Entwicklung von MS-DOS und WINDOWS gelang Microsoft der Durchbruch auf dem Markt. Während DOS sich noch weitgehend auf die Eingabe von Programmbefehlen über die Tastatur beschränkte, kann der Nutzer bei Windows den Computer über eine graphische Oberfläche mit Hilfe der Maus steuern. Beispiele für gängige Betriebssysteme:

die Anfänge: MS-DOS, Novell, Novell-DOS, DR-DOS

die Massenware: Windows (die wichtigsten Versionen 3.11, 95, 98, Millennium)

die Ableger: Windows NT (die wichtigsten Versionen NT4, 2000, XP) für die Kleinen: Windows Powered (Windows CE). PalmOS, EPOC ambitionierte Versuche: OS/2, BeOS
die Alternativen: Linux oder Mac OS von Apple

Bildschirmschoner

Ein Programm, das in Arbeitspausen auf dem Bildschirm erscheint und die Darstellung ständig verändert. Dadurch wird verhindert, dass sich ein unverändertes Bild in den Bildschirm "einbrennen" kann. Besser - weil energiesparend - sind Mechanismen, die den Bildschirm nach einer einzustellenden Zeit in einen Stromsparmodus schalten.

Bit

Abkürzung für "Binary Digit" die kleinste Informationseinheit im binären Zahlensystem, die einer Speicherzelle entspricht. Ein Bit kann entweder den Wert 0 oder 1 annehmen. 8 Bit werden zu einem Byte zusammengefasst.

Bitmap

Bild oder Grafik auf der Basis von Bits.

Booten

Bezeichnet das Laden des BIOS und des Betriebssystems nach einem Kalt- oder Warmstart.

Buffer

Englische Bezeichnung für Puffer - ein Zwischenspeicher, der zur Zwischenlagerung von Daten dient (siehe auch *Cache*).

Bug

Englische Bezeichnung für "Wanze" oder "Käfer" umgangssprachliche Bezeichnung für einen Programmfehler (siehe auch *Debug*).

Byte

Ein Byte ist die kleinste adressierbare Speicherstelle. Es besteht aus 8 Bits. Da ein Bit zwei Zustände einnehmen kann, ermöglicht ein Byte (2 hoch 8) 256 Kombination und damit die Darstellung von 256 verschiedenen Zuständen oder Zeichen. Außerdem: 1 KByte = 1024 Byte, 1 Megabyte = 1024 KByte.

Cache

Ein schneller Puffer, der Daten zwischenspeichert und diese immer wieder sehr schnell zur Verfügung stellen kann. Es gibt mehrere Cache-Arten:

- solche, die Daten aus dem Arbeitsspeicher in CPU-Nähe (im First- oder Second-Level-Cache) puffern
- solche, die Daten von der Festplatte im Arbeitsspeicher zwischenlagern (z.B. Smartdrive bzw. smartdrv.exe),
- oder Daten vom langsamen CD-ROM-Laufwerk auf der Festplatte "cachen".

Der Festplatten-Cache puffert hardwareseitig Schreib- und Lesezugriffe. Da die Algorithmen unterschiedlich effektiv arbeiten, steigert ein größerer Cache nicht zwangsläufig das Plattentempo. Werden die im Cache befindlichen Daten erneut benötigt, tritt die beschleunigende Wirkung des Cache voll zu Tage, da diese nicht mehr von dem langsameren Medium geholt werden müssen.

CD-ROM

Als "CD-ROM" (Abk. f. "**c**ompact **d**isk **r**ead **o**nly **m**emory", "Compact-Disk-Festwertspeicher") werden die von den Audio-CDs abgeleiteten Datenträger bezeichnet.

Client

Begriff aus dem Netzwerkbereich: ein Client nimmt Dienste in Anspruch, deshalb wird eine an den Server angeschlossene Arbeitsstation als Client bezeichnet. Der Client schickt Anfragen des Benutzers in einem speziellen Protokoll an den Server und stellt dessen Antworten in lesbarer Weise auf dem Bildschirm dar.

Cluster

Die kleinstmögliche Speichereinheit auf einem Datenträger. Bei Festplatten beispielsweise hat ein Cluster eine Größe von mindestens 2048 Byte.

CPU

Abkürzung für "Central Processing Unit" - englische Bezeichnung für Prozessor.

Data Mining

So wie ein Minenarbeiter im Bergwerk nach verborgenen Schätzen sucht, so werden beim Data-Mining aus dem Datenwust verborgene Informationen ans Tageslicht befördert. Das soll beispielsweise zu besseren Prognosen, differenzierteren Segmentierungen, Klassifizie-

rungen und Bewertungen von Kundengruppen oder Märkten führen.

Datei

Zusammengehörende Daten, die mit einem Anwendungsprogramm erstellt und unter einem eindeutigen Namen auf dem Datenträger gespeichert werden.

Datenbank

Im allgemeinen ist mit einer Datenbank eine Sammlung von Daten gemeint, die miteinander in Beziehung stehen. Über Datenbanken werden Aufträge, Kundenadressen, Bilder oder Archivinformationen verwaltet. Dazu werden spezifische Informationen in Tabellen zusammengefasst die wiederum aus einzelnen Feldern bestehen.

Datenkonvertierung

Texte, Grafiken u.a. werden in bestimmten Datenformaten gespeichert. Um mit "fremden" Daten umgehen zu können, müssen diese dem eigenen Format angepasst werden - also durch Übersetzung konvertiert werden.

Datensicherung

Datensicherung ist Pflicht. Das Oberlandesgericht Karlsruhe entschied, dass EDV-Anwender für die Sicherung ihrer Daten selber verantwortlich sind (Aktenzeichen 10 U 123/95).

Datenträger

Medium zum dauerhaften Speichern von Daten. Darunter fallen Disketten, CD-ROMs, Festplatten, Magnetbänder u.a.

Debug, Debugging

Kommt aus dem Englischen (Bug = Wanze) und bedeutet soviel wie Fehlersuche.

Defragmentierer / Defragmentierung

Ein Programm, das die Position von Datenelementen auf einem Datenträger verändert, damit Dateien zusammenhängend abgespeichert werden und schneller bearbeitet werden können (siehe auch *Fragmentierung*).

Desktop

Allgemeine Bezeichnung für die Arbeitsoberfläche in Windows.

Desktop Publishing

Erstellen von druckfertigen Dokumenten mit dafür speziell entwickelter Software. Desktop Publishing - abgekürzt DTP - ist der Oberbegriff für das Verfahren, mit Hilfe eines Personal Computers und ergänzender Hard- und Software Texte zu erfassen, layoutmäßig zu bearbeiten und für eine Vervielfältigung vorzubereiten.

Dialer

sind kleine Programme, die dem Computer-Anwender helfen, eine gewünschte Onlineverbindung herzustellen. Immer häufiger wird diese Technik von 'Gaunern" aber auch dazu verwendet, Online-Verbindungen ungewollt herzustellen und über teure Mehrwertdienste-Nummern abzurechnen. Die notwendigen Software-Routinen fängt sich der User zuvor quasi als Computervirus ein.

Directory

Englische Bezeichnung für "Verzeichnis". Gemeint ist in der Regel ein Dateiverzeichnis.

Diskette

Disketten sind die einfachste Form austauschbarer Datenträger, die gelesen und beliebig oft gelöscht und erneut beschrieben werden können.

Download / Downstream

Bezeichnung für das (Herunter-)Laden von Daten aus einem Kommunikationssystem wie dem Internet. Bei einem Download werden Programme oder Dateien auf den eigenen Computer übertragen.

Drag and Drop

Wörtlich: Ziehen und Fallen lassen. Technik in Windows (ursprünglich von Apple entwickelt), um einzelne Teile von Dokumenten (z.B. eine Textpassage aus WinWord) mit der Maus markieren, mit gedrückter linker Maustaste in das Fenster einer anderen Anwendung ziehen und dort fallen lassen zu können. Der Text wird dann genau an der Stelle eingefügt, an dem sich der Mauszeiger befindet. Diese Methode nennt sich "Drag & Drop" und ist der einfachste Weg, Daten zwischen zwei Anwendungen auszutauschen (siehe auch OLE, Einbetten und Verknüpfung).

Editor

Dienstprogramm zum Bearbeiten (Eingeben, Ändern) von Daten.

EDV

Abkürzung für "Elektronische Datenverarbeitung".

Ereignisprotokoll

Spezielle Datei eines Betriebssystems wie Windows NT oder Windows für Workgroups, in der wichtige Systemereignisse festgehalten werden.

Explorer

Englische Bezeichnung für "Forscher" oder "Erforscher". Im EDV-/IT-Bereich wird der Begriff gerne für Software verwendet, die z.B. die Festplatte erkundet (Windows-Explorer von Microsoft) das WorldWideWeb erforschen lässt (Internet-Explorer von Microsoft).

FAQ

Abkürzung für 'Frequently Asked Questions" (= häufig gestellte Fragen). Sie enthalten kurze und klare Antworten auf die am meis-

ten gestellten Fragen zu einem Thema. FAQs gibt es zu Computerthemen ebenso wie über Autoren oder Musiker.

FAT

Abkürzung für "File Allocation Table". Dateizuordnungstabelle auf Festplatten, Disketten und CD-ROMs, die die Positionen von Dateien und Verzeichnissen auf dem Datenträger enthält (siehe auch NTFS).
FAT bezeichnet sowohl die Dateizuordnungstabelle selbst, die den Platz auf der Festplatte verwaltet und die freien, belegten sowie defekten Cluster protokolliert, als auch das Dateisystem. Die FAT folgt direkt nach dem Bootsektor. Im Anschluss daran liegt eine Kopie der FAT.

Fehlermeldung

Meldung vom Betriebssystem oder dem Anwendungsprogramm an den Benutzer, wenn ein Fehler aufgetreten ist. Dabei kann es sich beispielsweise um einen Eingabe-, einen Programm- oder auch einen Hardwarefehler handeln.

Festplatte

Datenträger, der fest im Rechner eingebaut ist und eine größere Datenmenge aufnehmen kann.

File

Englische Bezeichnung für "Datei".

File Server

Zentraler Rechner (Server) im Netzwerk, auf dem die Netzwerksoftware geladen ist und auf dem sich zentrale Daten befinden, die für die angeschlossenen Arbeitsstationen zugänglich sind.

Firewall

Englische Bezeichnung für "Feuermauer" / "Brandmauer". Technik in Form von Hard- und/oder Software, die den Datenfluss zwischen einem privaten und einem ungeschützten Netzwerk (also LAN und Internet) kontrolliert bzw. ein internes Netz vor Angriffen aus dem Internet schützt. Dazu vergleicht eine Firewall z.B. die IP-Adresse des Rechners, von dem ein empfangenes Datenpaket stammt, mit einer Liste erlaubter Sender - nur deren Daten dürfen passieren.

Floppy / Floppy Disk

Flexibles Speichermedium für Daten, auch "Diskette" genannt.

Fragmentierung

Normalerweise werden alle Daten einer Datei direkt hintereinander auf der Festplatte gespeichert. Allerdings funktioniert das nur, wenn ein genügend großer zusammenhängender Speicherbereich zur Verfügung steht. Ist das nicht der Fall, werden Dateien zerstückelt (auf einzelne Cluster aufgeteilt) auf die Festplatte geschrieben. Man spricht hier von fragmentierten Dateien.

Da der Lesekopf der Festplatte für das "Anfahren" der einzelnen Fragmente mehr Zeit braucht, verzögert sich das Laden von Dateien. Deshalb ist es sinnvoll, die Festplatte in regelmäßigen Abständen aufzuräumen und die Dateien wieder in einem Stück dort abzulegen. Dieser Vorgang heißt Defragmentierung und sollte mindestens einmal monatlich durchgeführt werden, falls der Computer täglich benutzt wird.

Handheld

Ein Handheld ist ein (kleiner) Computer ohne Tastatur, den man in der Hand halten kann daher "Handheld". Die Eingabe erfolgt meist unter Zuhilfenahme eines Eingabestiftes oder über einen Touch-Screen (berührungsempfindlicher LCD-Bildschirm).

Hardware

Alle harten Bestandteile des Computers und seiner Peripherie, d.h. alle Geräte und Geräteteile vom Prozessor über Speicher und Datenträger bis zum Drucker oder Modem.

Hauptverzeichnis

Oberstes Verzeichnis auf einem Datenträger. In diesem Verzeichnis müssen sich bestimmte Systemdateien befinden, die das Betriebssystem benötigt und dort sucht.

Headcrash

Englische Bezeichnung für den Aufprall des Schreib-/Lesekopfes einer Festplatte auf die Oberfläche des Datenträgers - das Schlimmste, was einer Festplatte passieren kann. Dabei wird das Laufwerk beschädigt, und Daten gehen verloren.

Header

Ein Bereich am Anfang (am Kopf) von Dateien, in dem grundsätzliche Informationen über die Datei gespeichert sind oder der Teil einer E-Mail oder einer Usenet-Nachricht, die Informationen über Inhalt, Absender und Datum gibt.

Hypertext

Hypertext zeichnet sich gegenüber normalem Fließtext durch Querverweise (Hyperlinks) zu andern Dokumenten oder Textstellen aus. Durch Anklicken einer markierten Textstelle oder anderer in den Text eingefügter Objekte wird automatisch das referenzierte Dokumente bzw. die entsprechende Textstelle angezeigt, eine Datei heruntergeladen oder ein anderes Programm gestartet.

Image

Englisch für Bild bzw. Graphik. Der Begriff wird auch verwendet, wenn ein Abbild eines Speichermediums oder auch nur einer Partition hergestellt wird.

Image Backup

Englische Bezeichnung für die komplette Datensicherung (z.B. auf einem Streamer), die spurweise und nicht Datei für Datei durchgeführt wird (siehe auch *Datensicherung*).

Image-File / Image-Datei

Das Image-File besteht aus den Daten, die auf eine CD oder DVD gespeichert werden sollen. Die Brenn-Software kann ein solches File anlegen. Das ist dann nützlich, wenn eine langsame Festplatte ver-

wendet wird, die dem Brenner ansonsten keinen kontinuierlichen Datenstrom liefern kann (siehe Buffer-Underrun, On-The-Fly). Vorteil: Alle Daten, die auf die CD-ROM übertragen werden sollen, befinden sich in einer Datei - unfragmentiert und bestens vorbereitet. Allerdings braucht das Image-File entsprechend viel Platz auf der Festplatte - im ungünstigsten Fall 650 MByte und mehr.

Implementation

Integration zusätzlicher Funktionen in vorhandene Anwendungen. Auch als Bezeichnung für das Installieren weiterer Software verstanden.

Inkompatibilität

Unverträglichkeit von Hardware- oder Softwarekomponenten.

Installation

Einbau und Einrichten von (weiteren) Hardwarekomponenten eines Computersystems.
Kopieren von Software auf die Festplatte eines Computers und gleichzeitige Anpassung an das Betriebssystem.

Installationsprogramm

Spezielles Programm, das in der Regel mit der Software mitgeliefert wird und zuständig für das Kopieren von Software auf die Festplatte eines Computers ist. Außerdem nimmt es notwendige Anpassungen an die vorhandenen Komponenten des Systems vor.

Interface

Englische Bezeichnung für Schnittstelle:
Anschlussmöglichkeit für Peripheriegeräte des Computers.
Schnittstelle zwischen Protokollen, Programmen, Diensten etc..

Kompatibilität

Verträglichkeit unterschiedlicher Hardware- und Softwarekomponenten.

Komprimieren / Kompression

Verfahren, um Datenaufkommen unterschiedlicher Art zu reduzieren.

Konfiguration

Zusammenstellen eines PC-Systems.

Anpassung von Hardware und Software an die Gegebenheiten des vorliegenden Systems.

Konvertierung

Umformung / Umwandlung zwischen unterschiedlichen Dateiformaten, damit diese von anderen Programmen gelesen oder bearbeitet werden können.

Kopierschutz

Vorrichtung, die das unbefugte Kopieren von Programmen oder Daten unterbindet. Ein Kopierschutz kann durch spezielle Software oder Hardware (Dongle) realisiert werden.

LAN

Abkürzung für "Local Area Network": lokal angelegtes Netzwerk. Im Gegensatz zu WAN, das überregional die Arbeitsstationen und Netzwerke verbindet. "Lokal" bezieht sich in diesem Sinne auf einen gemeinsamen Standort, wie beispielsweise ein Firmengelände oder einen Raum.

Laptop

Wörtlich: Auf dem Schoß. Computer, der so klein und leicht konzipiert ist, dass er wie eine Aktentasche transportiert und auf dem Schoß bedient werden kann. Der besonders flache Bildschirm bei den Laptops wird durch LCD-, DSTN-, HPA-, TFT-Technik oder Plasmabildschirm realisiert. Zwischenzeitlich wurde der Laptop durch das noch handlichere Notebook ersetzt.

Laufwerk

Gerät, das Speichermedien wie Disketten oder Festplatten beschreiben und lesen kann.

Lesekopf

Schreib-/Lesekopf zum Schreiben und Lesen von Daten auf Datenträgern.

(Hyper-)Link

Englische Bezeichnung für Verknüpfung oder Verbindung - Verbindung zu Daten, die sich in einem anderen Programm oder Dokument befinden. Diese interne Verknüpfung der Daten sorgt dafür, dass die Daten mit der Anwendung, in der sie ursprünglich erzeugt

wurden, weiterbearbeitet oder automatisch aktualisiert werden können.

Link

Englische Bezeichnung für Verknüpfung oder Verbindung.
Bestandteil (Linker) des Kompilierens.
Interne Verbindung einer Arbeitsstation zum Server, damit ein Datenaustausch stattfinden kann.

Lizenz

Berechtigung zur Nutzung von Software. In der Regel wird die Lizenz mit dem rechtmäßigem Kauf von Software erworben.

Logfile

Datei, in der die Aktivitäten eines Computers protokolliert werden.

Login

Das Anmelden und das Authentisieren eines Anwenders in einem Netzwerk oder einem anderen Kommunikationssystem wie einem Online-Dienst: Die Login-Prozedur umfasst dabei den gesamten Vorgang vom Wählen der Telefonnummer des Online-Dienstes oder Internet-Providers über diverse Passwort-Abfragen bis hin

zum geschlossenen Verbindungsaufbau. Gegenteil: Das Verlassen des Systems geschieht meist mit dem Befehl Logoff oder Logout- manchmal auch mit Quit.

Lokal

"Lokal" bezieht sich in diesem Sinne auf einen begrenzten Netzwerkstandort, wie beispielsweise ein Firmengelände oder ein Gebäude. Die Arbeitsstationen sind noch so nah am Server, dass die Verbindung über übliche elektrische Leitungen realisiert werden kann und nicht über das Telefonnetz oder über Satellit hergestellt werden muss.

Magnetische Speicher

Datenträger, der das Speichern von Informationen über eine Magnetisierung ermöglicht.

(Computer-)Maus

Eingabegerät, das von Hand auf dem Tisch geführt wird und entsprechend der Bewegung der Hand auf dem Bildschirm einen Cursor bewegt. An entsprechenden Positionen können mit den zusätzlich angebrachten Tasten Aktionen ausgelöst werden.

Menü

Eine mit Hilfe von Listen oder Schaltflächen dargestellte Ansammlung von Programmfunktionen.

Motherboard

Englische Bezeichnung für die Hauptplatine im Computer. Sie ist quasi die zentrale Bühne, auf der die weitere Hardware aufgebaut wird: die Speicherbausteine, die Grafikkarte, die CPU usw.

Netz / Netzwerk

Verbund von Computern, die über verschiedene Leitungen verbunden sind und sich gemeinsame Ressourcen wie Daten und Peripheriegeräten teilen. Häufig steht in einem Netzwerk ein spezieller Rechner (Server) nur zur Datenverwaltung zur Verfügung, auf den alle anderen Arbeitsstationen Zugriff haben.
Man unterscheidet im Wesentlichen LANs, die "unter einem Dach" innerhalb von Firmen und Behörden eingesetzt werden, sowie WANs, die beispielsweise mehrere Filialen in verschiedenen Städten oder Ländern verbinden.

Notebook

Tragbarer Computer mit fast der Leistungsfähigkeit eines PCs. Notebooks haben eine Grundfläche von etwa einer DIN A4-Seite, ei-

nen flachen LCD-Monitor, ein Gewicht von weniger als 3 kg und können bei Bedarf auch über einen Akku betrieben werden. Das Notebook ist der Nachfolger des Laptops.

Operation

Englische Bezeichnung für "Anweisung" oder "Befehl".

Overhead

Englische Bezeichnung für die Überlastung eines Systems mit Aktionen, die die Produktivität verhindern.

Partition

Einheit eines definierten Speicherbereichs einer Festplatte, die als eigenständiges Laufwerk angesprochen und behandelt werden kann.

Patch

Ein Patch (englische Bezeichnung für "Flicken", manchmal auch "Bug fix" genannt) ist ein kleines Programm, das z.B. Bugs (Fehler) von in der Regel großen Anwendungsprogrammen repariert. Die meisten Patches werden von den Software- Herstellern auf ihren Webseiten kostenlos zum Download angeboten. Da Patch-Programme nur in einen kleinen Teil des fehlerhaften Programm-

codes eingreifen und kein komplettes Update sind, sind sie in der Regel nicht sehr umfangreich und somit auch in sehr kurzer Zeit downzuloaden. Oftmals werden Patches aber auch in die nächsten Versionen eines Programms eingebaut, damit fehlerhafte Programme, die nicht gepatcht wurden, auch repariert werden.

Peripherie

Englische Bezeichnung für Umgebung. Gemeint sind an einen Computer angeschlossenen Geräte, wie Bildschirm, Tastatur, Scanner, Drucker u.a.

Pfad

Ein Pfad zeigt die Stelle an, an der eine Datei auf der Festplatte gespeichert ist.

Platine

Kunststoffplatte, die mit elektronischen Bauteilen bestückt ist und deren Leitungen und Schaltkreise mit Hilfe eines speziellen Verfahrens aufgedruckt wurden.

Programmabsturz

Fehler in einem Programm, der dazu führt, dass ein Arbeitsschritt nicht zu Ende ausgeführt werden kann und auch keine weiteren Eingaben möglich sind. Das Programm kann nicht mehr ordnungsgemäß verlassen werden und gegebenenfalls zur Instabilität des Systems führen.

Protokoll

Ein Protokoll bezeichnet die Sammlung von Regeln für Formate und Arten der Datenübermittlung zwischen unterschiedlichen Rechnersystemen.

Prozessor

Auch Central Processing Unit oder CPU - zentrale Recheneinheit im Computer, die alle Rechen- und Steueroperationen übernimmt.

RAID-System

Abkürzung für "Redundant Array of Independent Disks" oder "Redundant Array of Inexpensive Disks". Bei RAID-Systemen steht die Sicherheit von Festplatten-Daten im Vordergrund. Ein RAID-System ist in der Lage, Daten redundant zu speichern, also auf mindestens einer weiteren Festplatte nochmals abzulegen.

Redundanz

Mehrfach vorhandene Informationen - (Nicht nur) in Netzwerken kann das Vorhandensein derselben Daten in unterschiedlichen Dateien bzw. der selben Dateien in unterschiedlichen Verzeichnissen oder Datenträgern schnell dazu führen,

- dass nicht alle Daten / Dateien aktuell sind,
- dass auf die falschen Daten zugegriffen wird,
- dass neuere Informationen an verschiedenen Stellen eingetragen werden.

Auf jeden Fall sind redundante Daten zu vermeiden. Es sei denn, kontrollierte bzw. strukturierte Redundanz wird zu einem Bestandteil der Datensicherung - siehe auch: RAID (Redundant Array of Inexpensive Disks).

Remote

Englische Bezeichnung für z.B. "räumlich fern, (weit) entfernt; abgelegen, entlegen". Als Form der Datenrettung existiert die Remote DataRecovery™, die von Kroll Ontrack patentierte Form der Datenrettung bei der die beschädigten Dateien über das Internet oder 1:1 Modemverbindung repariert werden.

ROM

Abkürzung für "Read Only Memory" - englische Bezeichnung für Nur-Lese-Speicher.

Schreib- / Lesekopf

Lesekopf bei Laufwerken zum Lesen oder Schreiben von Daten.

Sicherheitskopie / Sicherungsdiskette / Sicherungskopie

Kopien von Daten, Datenträgern oder Teilen von Datenträgern

Sicherungsdateien

Spezielle Dateien, die von Anwendungsprogrammen automatisch hergestellt werden und den Stand vor dem letzten Sichern einer Datei beinhalten. In solchen Fällen verfügt der Anwender über die aktuelle Version seiner Arbeit und die Vorversion. Sehr häufig haben Sicherungsdateien die Dateierweiterung BAK.

Software

Sammelbegriff für alle Arten von Computerprogrammen - also für Betriebssysteme, Utilities und Anwendungsprogramme.

Spiegeln

Herstellen einer kompletten Festplatten-Kopie.

Tape

Englische Bezeichnung für "Magnetband".

temporäre Dateien

Zeitweilig nötige Dateien, in denen Daten bis zum Ende der Bearbeitung zwischengespeichert werden. Temporäre Dateien werden meist automatisch entfernt, sobald der Vorgang ordnungsgemäß beendet werden kann.

temporäres Verzeichnis

Verzeichnis für temporäre Dateien. Kann durch die Umgebungsvariable TEMP festgelegt werden.

Transfer

Englische Bezeichnung für Datenübertragung.

Übertragungsprotokoll

Regelsystem für die korrekte Übertragung von Daten in der Datenfernübertragung und in Netzwerken (siehe auch Protokoll). Die einfachste Übertragungsart sendet / empfängt ASCII-Zeichen mit einem "Return" am Zeilenende. Das ist aber bei einer schlechten

Leitung sehr störanfällig. Für die Übertragungen, die fehlerfrei sein müssen, gibt es Übertragungsprotokolle. Dabei werden die zu übertragenden Daten in Blöcke unterteilt, für die Prüfsummen gebildet werden, die wiederum auch an den Empfänger geschickt werden. Anhand dieser Prüfsummen wird der korrekte Datenfluss kontrolliert. Wenn Fehler auftreten, regelt das Übertragungsprotokoll zudem, wie der Fehler behoben wird.

Update

Englische Bezeichnung für Aktualisierung - neuere Version eines Programms / einer Software.

ZIP (Kompression)

Häufig verwendetes Format für gepackte bzw. komprimierte Dateien.