Zugriff auf archivierte Daten - ein Glücksspiel für Ihr Unternehmen?

Maximaler Zugriff auf gespeicherte Unternehmensdaten – bei minimalem Risiko

Kroll Ontrack

Gespeicherte Daten effizient verwalten: Maximaler Zugriff, minimales Risiko

Vor dem Hintergrund einer zunehmend komplexeren technischen Infrastruktur, einer enormen Datenmenge und gleichbleibender oder sinkender Budgets ist die kosteneffiziente und sichere Verwaltung von Informationen weiterhin eine Herausforderung für alle Unternehmen. Bei effizienter Verwaltung erfüllt ein klar definiertes Information Life Cycle Management die Anforderungen des Unternehmens, der Sicherheit, der Compliance sowie der gesetzlichen Bestimmungen. So werden Risiken verringert, wertvolle Informationen geschützt und eine kontinuierliche Zugriffsmöglichkeit auf die Daten sichergestellt. Bei einer mangelhaften Datenverwaltung werden alle Daten „für den Fall des Falles“ gespeichert und damit das IT-Budget unnötig belastet. Außerdem steigen die Risiken und Kosten, wenn – im Falle eines Audits, eines Rechtsstreits oder einer Übernahme – gespeicherte Daten offengelegt werden müssen. In diesem Whitepaper informieren wir Sie über die Best Practices beim Life Cycle Management und geben Tipps zur Verringerung der mit der Speicherung und Konvertierung wichtiger Daten verbundenen Risiken.

Information Life Cycle Management

Die Storage Networking Industry Association (www.SNIA.org) definiert Information Lifecycle Management (ILM) wie folgt:

- Richtlinien, Prozesse, Praktiken, Dienstleistungen und Tools, die dazu verwendet werden, den Wert der Informationen mit der am besten geeigneten und kosteneffektivsten Infrastruktur zu kombinieren – von dem Zeitpunkt, an dem die Informationen erstellt werden, bis zu deren endgültiger Vernichtung.

- Informationen und geschäftliche Anforderungen werden mit Hilfe von Unternehmensrichtlinien koordiniert.

Interessanterweise kommt der Begriff Speicherung in der Definition der SNIA nicht vor. Neben ihrer Relevanz für technische Fachgebiete wie Informationsspeicherung, Sicherheit, Unternehmensarchitektur usw. zielt diese Definition auch darauf ab, Unternehmen auf Strategien, Taktiken und Methoden des Informationsmanagements hinzuweisen.

Obwohl immer mehr Unternehmen für die interne Datensicherung Festplatten verwenden, wird dennoch eine Zunahme der externen Sicherung auf Band erwartet.

Information Life Cycle Management

Der Begriff des Informationsmanagements in Unternehmen beinhaltet zahlreiche grundlegende Fragen: Welche Inhalte werden gegenwärtig von dem Unternehmen gespeichert? Befinden sich die gespeicherten Inhalte am Unternehmensstandort oder bei einem Speicherplatzanbieter? Welche Daten sind für die Geschäftskontinuität oder rechtliche Zwecke tatsächlich notwendig, und welche Daten sollten entsorgt werden, weil sie doppelt vorhanden oder nicht relevant sind? Manche Informationen verlieren nie ihre Gültigkeit - wie proprietäre Zeichnungen, Prototypen oder Formeln - und sind möglicherweise bereits gespeichert. Wenn bestimmte Daten immer länger vorgehalten werden müssen, benötigt das Unternehmen einen Plan, um den Zugriff auf die Daten sicherzustellen – auch dann, wenn die gegenwärtige Technologie veraltet ist und es sich nicht lohnt, Altsysteme nur zu Wiederherstellungszwecken weiter zu betreiben.

Wenn ein Unternehmen diese Fragen nicht mit Hilfe eines klar umrissenen ILM-Prozesses klärt, lautet die Standardlösung sowohl für gespeicherte Daten als auch für ältere technische Systeme automatisch „behalten“. Meist werden Informationen über die Verwaltung verschiedener Arten von Inhalten oder Daten nur selten durch ein Service Level Agreement (SLA) erfasst und kommuniziert – ein Umstand der unnötige Kosten und Risiken zur Folge hat.

Eine kürzlich durchgeführte Untersuchung der Enterprise Strategy Group (ESG) hat ergeben, dass „82 % der Unternehmen Bänder für alle oder einen Teil ihrer Sicherungsprozesse vor Ort verwenden“ (siehe Abbildung 1). Der Bericht bestätigt, dass hier eine Verlagerung stattfindet, weil in Zukunft mehr Unternehmen für interne Sicherungsprozesse Festplatten verwenden werden – die extern gespeicherte Datenmenge auf Bändern soll den Erwartungen zufolge aber dennoch steigen. Dies liegt hauptsächlich an der Zunahme primärer Daten, so dass noch mehr Daten gespeichert und gesichert werden müssen.

Obwohl dem Band schon lange sein Verschwinden vorrausgesagt wird, ist es nach wie vor ein intensiv genutztes Speichermedium für neu generierte Daten. Bänder sind die meist genutzte Speichertechnologie für historische Informationen – insbesondere auch für unverzichtbare Geschäftsaufzeichnungen.

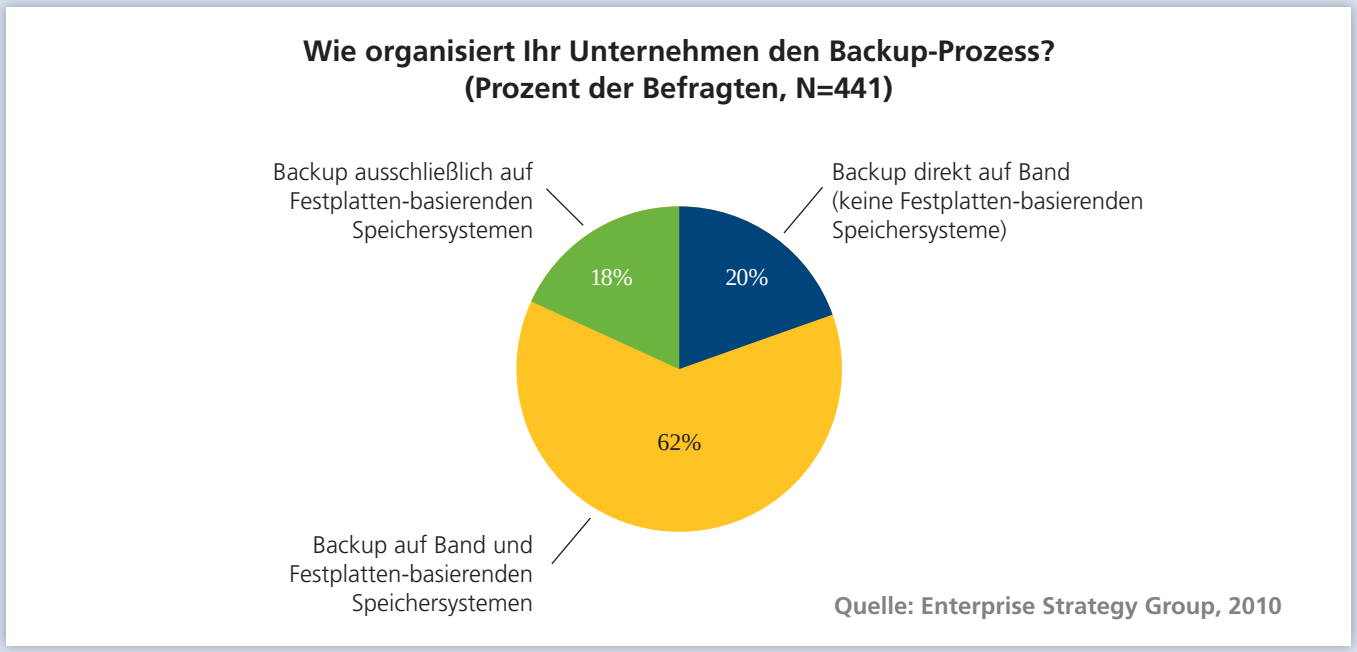

Abbildung 1: Bänder sind in den meisten Unternehmen Teil des Datensicherungs-Prozesses

Datenzugriff – ein Glücksspiel

Unternehmen sichern und speichern routinemäßig Informationen und sind davon überzeugt, dass die von ihnen verwendeten Verfahren zuverlässig und die gesicherten Daten intakt sind. Der problemlose Abruf dieser Daten kann jedoch durch verschiedene Faktoren beeinflusst werden. Einige dieser möglichen Probleme fallen erst dann auf, wenn sich das Unternehmen in einer kritischen Situation befindet, in der es nur noch reagieren kann und schnell nach Alternativen suchen muss. Ungeachtet der technischen Probleme sind Unternehmen verpflichtet, spezifische relevante Daten aufzubewahren und im Falle eines Rechtsstreits fristgerecht vorzulegen. Darüberhinaus entbindet eine Datenverwaltung, die den Zugriff auf die Daten schwierig oder unmöglich macht, Unternehmen nicht von dieser Pflicht. Einige Unternehmen verlassen sich blind darauf, dass ihre älteren Daten problemlos zugänglich und verwendbar sein werden, falls man sie benötigt. Die folgende Tabelle zeigt die Faktoren, durch die der Zugriff auf die Daten häufig gefährdet wird.

Bänder bleiben das vorherrschende Speichermedium für langzeitarchivierte Informationen – insbesondere auch für unverzichtbare Geschäftsaufzeichnungen.

Wann kann Datenverfügbarkeit gefährdet sein

Fehler der Backup Software	Die Sicherungssoftware ist korrekt eingerichtet, und der Prozess wurde gestartet. Die gesicherten Daten selbst werden jedoch nie überprüft.
Korruption der Speichermedien	Versagen des Bandlaufwerks; beschädigte Bänder oder Bänder, auf die nicht zugegriffen werden kann; die auf dem Band gespeicherten Informationen sind nicht lesbar (logische Datenfehler). Es besteht ein wesentlicher Unterschied zwischen den Daten der letzten Sicherung und den Daten vom Zeitpunkt der Medien-Korruption.
Menschliche Fehler	Häufig werden Bänder versehentlich gelöscht, neu initialisiert oder überschrieben.
Datenmenge und Auffindbarkeit von Informationen	Dies bezieht sich auf die reine Datenmenge und die Möglichkeit, spezifische Inhalte im Unternehmensspeicher wiederzufinden. Wie erfahren Sie von fehlenden oder verloren gegangenen Daten? Bei einer Unternehmensfusion müssen die operativen Daten sowie die Buchführungs- und Kundendaten beider Unternehmen weiterhin zur Verfügung stehen. Die unterschiedlichen Sicherungslandschaften müssen aufeinander abgestimmt werden (z. B. proprietäre Sicherungssysteme in Windows-Umgebungen).
Ältere und veraltete Systeme	Ältere Daten müssen vorgehalten und alte statische Systeme auf ein anderes Format oder eine neuere Technologie umgestellt werden. Prüfer können eventuell das Einreichen alter Datensätze verlangen – wie im Fall einer Bank, die 17 000 Datensätze aus den 1980er Jahren vorlegen musste. Die Bänder standen zwar zur Verfügung, aber Software und Laufwerke funktionierten nicht mehr.
Naturkatastrophen	Feuer, Wasserschäden, Schlamm, außergewöhnliche Kälte, Hitze oder andere Naturkatastrophen führen häufig dazu, dass Bänder verschmutzt und/oder beschädigt werden und mit den üblichen Mitteln nicht mehr lesbar sind.
Nicht einwandfreie Methoden	Die Daten können zwar von Menschen „gelesen“ werden, aber durch fehlerhaftes Verschieben/Verlagern der Daten können die für Untersuchungs- und E-Discovery-Zwecke benötigten Datei- oder Systemmetadaten verändert werden.

Vier Tipps für einen verbesserten Datenzugriff

Unternehmen erwarten von Datenmanagementexperten, dass diese ihnen zu einer effizienteren Verwaltung der gespeicherten Daten und einer geringeren Belastung von IT-Personal und -Infrastruktur verhelfen. Die folgenden vier Tipps könnten Ihnen dabei helfen:

1: Projekt definieren

Der Erfolg eines Projekts zur Bearbeitung gespeicherter Daten hängt von dem KnowHow und der Erfahrung der Projektleiter ab. Sie müssen in der Lage sein, den Umfang und die Herausforderungen des Projekts genau zu erkennen, um die Projektplanung daran auszurichten. Wichtig sind zum Beispiel folgende Punkte:

- Wie sieht die Datenlandschaft aus? Sind alle Speichersysteme und -medien bekannt?
- Liegen Erfahrungen mit der Realisierung von Lösungen für verschiedenartige Systeme vor?
- Was sind die Beweggründe für das Projekt und welches Budget steht zur Verfügung?

Es ist ebenso wichtig, die Art der Medien und ihren Zustand festzuhalten, wie abzuklären, welches Zielmedium geeignet ist. Selbst bei offensichtlich verheerenden Schäden (beispielsweise durch Feuer und Wasser) ist normalerweise eine Wiederherstellung in einem gewissen Ausmaß möglich. Dabei lassen sich dann die langfristig zu sichernden Unternehmensdaten auch gleich noch besser organisieren. Bei Naturkatastrophen muss besonders schnell gearbeitet werden, bevor die Medien durch Verkleben oder Korrosion endgültig unbrauchbar werden.

Es gilt auch zu klären, welche Datenschutzanforderungen bestehen. Wenn beispielsweise Daten unbedingt im Unternehmen bleiben müssen, ist die Konvertierung vor Ort vorzunehmen. Vielleicht müssen auch veraltete Server so wiederhergestellt werden, dass sich die früheren Zugangsrechte ebenfalls wiederherstellen lassen.

Das Definieren des Projekts und seines Umfangs sowie das Festlegen der erforderlichen technischen und personellen Ressourcen – schon im Vorfeld – ist ein wichtiger Schritt.

2: Daten analysieren

Ein Unternehmen muss die Inhalte seiner Speichermedien kennen, um später die richtigen Entscheidungen treffen zu können, welche Daten zu erhalten, zu zerstören oder auf Grund von Aufbewahrungspflichten oder Compliance zu speichern sind. Ein exaktes Katalogisieren oder Indizieren der Medien kann ein Unternehmen dabei unterstützen, sich auf die relevanten Medien zu konzentrieren. Allerdings ist Backup-Software für die Verwaltung großer Datenmengen ausgelegt, und nicht für das Auffinden und den Zugriff auf spezifische Inhalte. Eine solche Software ist komplex und erfordert eine relationale Datenbank zur Verwaltung von Sicherungsparametern, Sitzungen, Zeitplänen, Fehlern und anderen statistischen Daten.

Die Sicherungssoftware erfasst zwar systematisch, was gesichert wird, aber es kann schwierig sein, Angaben über den tatsächlichen Inhalt der Sicherungskopie zu erhalten.

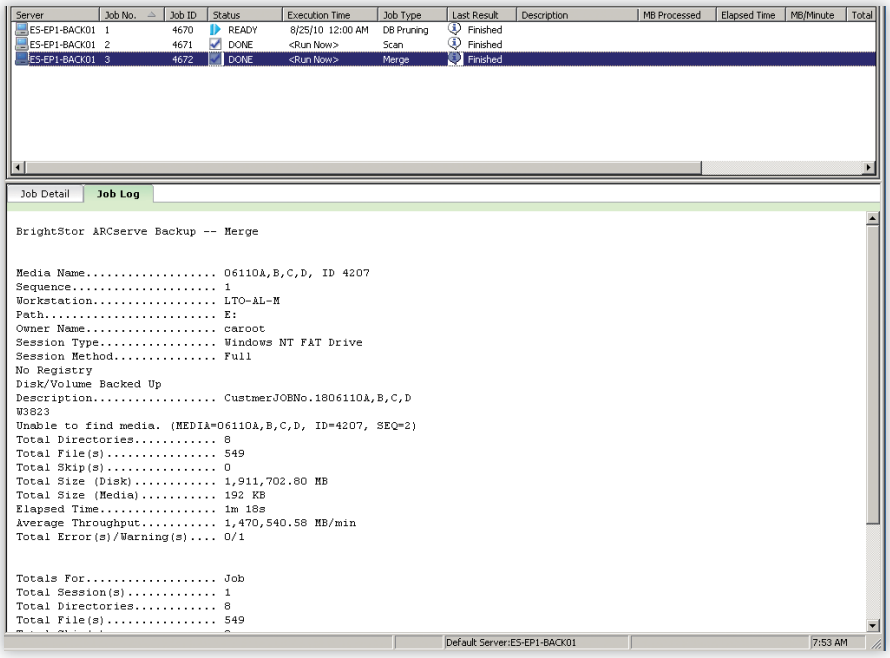

Abbildung 2: Die Backup-Software zeichnet die Metadaten des Backups auf - aber nicht die spezifischen Medien-Inhalte.

Vier Tipps für einen verbesserten Datenzugriff

Unternehmensübernahmen sind dafür ein klassisches Beispiel. Alle Sicherungskopien des übernommenen Unternehmens werden zu Assets des Mutterunternehmens. Beide Unternehmen haben bis zur Übernahme meist unterschiedliche Sicherungssoftware verwendet. Wenn einige Jahre nach der Übernahme ein Rechtsstreit beginnen würde, müssten im Verlauf des Beweiserhebungsverfahrens durch einen Verfahrensbevollmächtigten alle langfristigen Datenspeicher des Unternehmens geprüft und Auszüge erstellt werden. Würde diese Forderung nicht erfüllt, kann die Vorlage aller Sicherungsbänder angeordnet werden.

Die Begriffe „Katalogisieren“ und „Indizieren“ haben bei Anbietern von Software für die Langzeit-Datensicherung unterschiedliche Bedeutungen. Der Katalog einer Sicherungskopie zur langfristigen Sicherung bezieht sich normalerweise auf die auf einem Medienset gespeicherten Sicherungssitzungen. Bei einigen Anbietern werden diese Identifikationsmetadaten auf dem Band selbst gespeichert. Eine wachsende Zahl von Sicherungs-Software-Anbietern speichert jedoch die Medien-, Sicherungs- oder Sitzungs-ID auf demjenigen Medium, das zu der relationalen Datenbank der Software zurückverweist. Außerdem sind die wenigsten gespeicherten Sicherungssitzungen in Bezug auf Umfang und Aufzeichnung linear. Um die Sicherungs-IOPs (Input/Output-Operations pro Sekunde) und die Systemleistung beizubehalten, arbeiten viele Sicherungs-Plattformen mit verteilten Aufzeichnungen und Datenrotation. In diesem Fall werden mehrere Datenströme oder Prozesse gleichzeitig ausgeführt. Damit die Medienhardware mit mehreren Sicherungen mithalten kann, speichert die Software eine Sitzung mit einer spezifischen Größe in MB oder GB und wechselt dann zu einem anderen Sicherungsstream. Das einzige Unterscheidungsmerkmal der auf dem Medium aufgezeichneten Daten ist die Medien-, Sicherungs- oder Sitzungs-ID – der Rest der zugehörigen Metadaten wird in der relationalen Datenbank gespeichert.

Beim Zugriff auf die Sicherungsmedien über die Befehlseingabeaufforderung erhalten Speicheradministratoren unter Umständen mehrdeutige Informationen (siehe Abbildung 3).

Welche Daten sind auf den Medien gespeichert? Diese Frage kann zum Problem werden:

- Wenn ein Update der Backup-Software durchgeführt wird.
- Wenn die Datenbank, die zur Verwaltung aller Medien- und Sitzungsinformationen dient, korrupt ist oder gelöscht wurde.
- Wenn die Metadatensammlung möglicherweise nicht den Projektanforderungen entsprechen. Beispiel: In der Unternehmens-Datenbank sind die Sicherungs-Datensätze als „Mediensets“ gekennzeichnet – mit dieser ungenauen Bezeichnung ist nicht klar, welche Daten genau gesichert wurden (siehe Abbildung 3).

```
Up since: Wed Aug 18 16:24:46 2010  Version: Networker 7.5.1.Build.360 Eval
Saves: 1 session(s), 588 MB total   Recovers: 0 sessions(s)
Device                    type        volume
  /backup              adv_file    (none)
  /backup2             adv_file    (none)
  /dev/nst0    (J) sdlt600      80084553    mounted sdslt600 tape 80084553
  /dev/nst1    (J) sdlt600      80084653    mounted sdslt600 tape 80084653
  /dev/nst2    (J) sdlt600      80084753    mounted sdslt600 tape 80084753
  /dev/nst3    (J) sdlt600      80084853    mounted sdslt600 tape 80084853
  /dev/nst4    (J) sdlt600      80084453    mounted sdslt600 tape 80084453
  /dev/nst5    (J) sdlt600      80084353    mounted sdslt600 tape 80084353
d=fawn:backup        adv_file    (none)
fawn:/dev/nst0(J) sdlt600      90084353    writing, done (full)
fawn:/dev/nst1(J) sdlt600      90084453    writing, done
fawn:/dev/nst2(J) sdlt600      90084553    mounted sdslt600 tape 80084553
fawn:/dev/nst3(J) sdlt600      90084653    mounted sdslt600 tape 80084653

Sessions



Messages
Wed 04:45:51 PM fawn:/root saving to pool 'Default'  (90084353)
Wed 04:46:05 PM media warning: rd=fawn:/dev/nst0 writing: No space left on device,
Wed 04:46:05 PM media notice: sdlt600 tape 90084353 on rd=fawn:dev/nst0 is full
Wed 04:46:05 PM media notice: sdlt600 tape 90084353 used 510 MB of 40 GB capacity
Wed 04:46:06 PM media info: verification of volume "90084353", volid 4110649123 suc
Wed 04:46:07 PM write completion notice: Writing to volume 90084353 completed
Wed 04:46:09 PM fawn:root saving to pool 'Default" (90084453) 508 MB
Wed 04:46:11 PM 588 MB are saved to pool 'Default" (90084453) of fawn:/root
Wed 04:45:43 PM write completion notice: Writing to volume 90084453 completed
Pending:
```

Abbildung 3: Der Command-Line Output der Backup-Software Storage Engine

Vier Tipps für einen verbesserten Datenzugriff

Verschiedene Bedeutungen und unterschiedlicher Terminologiegebrauch können die Beurteilung eines Medien- oder Sicherungssets beeinträchtigen. Die Befehlszeilenausgabe könnte als „Indizierung der Sicherungsmedien“ verstanden werden. Wie in Abbildung 3 zu sehen ist, werden alle installierten Sicherungsmedien und der Status dieser Medien angezeigt. Die gespeicherten Inhalte werden den Speicheradministratoren oder Projektmanagern des Medienkonsolidierungsprojekts allerdings nicht angezeigt.

Unternehmen, die Dienstleistungen für Datenzugriff anbieten, können Bänder mit Sitzungen nicht nur erkennen, sondern auch den genauen Inhalt der langfristig gespeicherten Sicherungskopien feststellen. Die Indizierung kann durch direktes Lesen des Bandes erfolgen – ohne die ursprünglich verwendete Sicherungssoftware. Da sie unabhängig von der Sicherungssoftware vorgehen und sich nicht auf die Zuverlässigkeit der Metadaten-Datenbank verlassen müssen, sind Datenmanagement-Unternehmen in der Lage, eine vollständige Liste der extrahierten und zusammengefügten Dateien zu liefern. Durch eine detaillierte Analyse auf diesem Niveau können Sie sicherstellen, dass das Budget für Ihr Datenkonsolidierungsprojekt eingehalten wird.

3: Daten verwalten und verbessern
Unternehmen führen regelmäßig inkrementelle (tägliche/wöchentliche) und vollständige Datensicherungen (oft am Monatsende) durch. Dies gilt in der Branche zwar als „Best Practice“, führt aber im Ergebnis dazu, dass dieselben Daten mehrfach gespeichert werden. Wenn die Sicherungsverfahren eines Unternehmens bekannt sind und diese analysiert wurden, lässt sich auf Grundlage dieser Informationen eine Auswahl aus den Daten des relevanten Datensatzes treffen. So können doppelt vorhandene Daten gelöscht werden, vorausgesetzt, dass dem keine rechtlichen Gründe entgegenstehen. Wenn die Daten erhalten bleiben müssen, können Sicherungskopien konsolidiert werden, indem die entsprechenden Daten auf Bändern mit größerem Fassungsvermögen gespeichert werden. Außerdem können auch nicht relevante Systemdateien gelöscht werden. Diese Methode ist als „deNISTing“ bekannt. Hinweis: Die Liste des National Institute of Standards and Technology (NIST) enthält über 28 Millionen Dateisignaturen. Sie dient dazu, Dateien zu erkennen, die keinen nachgewiesenen Wert besitzen. Weitere Informationen hierzu finden Sie in der National Software Reference Library unter **www.nsrl.nist.gov**.

Vier Tipps für einen verbesserten Datenzugriff

4: Bedarf prüfen
Wenn der Projektumfang festgelegt wird, umfasst dieser möglicherweise auch eine notwendige Konvertierung oder sonstige Bearbeitung der Daten. Damit Zeitplan und Budget des Projektes eingehalten werden können, ist es wichtig, das Komplexitätsniveau des Vorhabens zu kennen.

Einfache Konvertierung
Einige Arten der Konvertierung sind unkompliziert – wie das Kopieren von Daten aus einem Betriebssystem, so dass sie von einem anderen Betriebssystem gelesen werden können. Für andere Konvertierungen sind unter Umständen größere Fachkenntnisse erforderlich. Denken Sie beispielsweise daran, wie sich die Spezifikationen für digitale Inhalte bei Mainframe-, Midrange- und Desktopsystemen unterscheiden. Auf IBM- und AS/400-Computern wird der EBCDIC-Code zur Darstellung des Alphabets verwendet, obwohl sonst in den meisten Fällen der ASCII-Code die Norm ist. Diese Art von Projekt erfordert „Übersetzungsarbeit", um die Zugriffsmöglichkeit auf die Daten zu erhalten. So muss beispielsweise eine AS/400-Datenbank im EBCDIC-Format mit festgelegter Länge in eine ASCII-Code-Datei mit flexibler Länge oder eine CSV-Datei konvertiert werden, um auf einem PC lesbar zu sein.

Komplexe Konvertierung und Bearbeitung von Daten
Eine komplexere Konvertierung kann die Bearbeitung von Feldern einer Datenbank umfassen. So erfordern beispielsweise die Richtlinien in der Kreditkartenbranche (PCI-Compliance), dass beim Speichern von Kreditkartennummern die Daten der Karteninhaber maskiert werden. In diesem Fall könnte ein Datenmanagementexperte die Daten entpacken und extrahieren und entsprechende Zeichen – wie z.B. Kreditkartennummern – maskieren.

Das Ergebnis: Eine effiziente, kosteneffektive Lösung
Ein Projekt zur Verwaltung und Bearbeitung gespeicherter Daten kann durch verschiedene gesetzliche, Compliance- oder E-Discovery-Anforderungen angestoßen werden. Durch eine gute Planung der Zugriffsmöglichkeiten auf gesicherte Daten können derartige Anforderungen mit weniger Aufwand und geringeren Risiken erfüllt werden. Unternehmen, die ihre Informations-Management-Strategien klar definieren und die vorgestellten Tipps berücksichtigen, sind gut vorbereitet:

- Klar umrissener Projektplan
- Umfassende Dokumentation der gespeicherten Inhalte
- Verbesserte Nutzung von IT-Ressourcen (personeller und operativer Overhead)
- Pünktliche Bereitstellung der Daten, zugänglich und verfügbar für Geschäftszwecke im angegebenen Format

Datenzugriffsproblem gelöst

Bisher war es zeitaufwendig, technisch schwierig und zu kostspielig, ältere Daten in den ILM-Plan eines Unternehmens zu integrieren. Nach der Wiederherstellung der Daten durch die IT-Abteilung arbeiteten für gewöhnlich Rechts- und IT-Abteilung zusammen an der Analyse der relevanten Daten, die für eine Untersuchung oder einen Rechtsstreit benötigt wurden. Aufgrund von Budget- und Infrastrukturbeschränkungen war die Wiederherstellung von Tausenden oder Zehntausenden von Bändern nicht realisierbar.

Dieses Problem wurde durch eine Optimierung des gesamten Prozesses mit Hilfe von Technologie gelöst. Anstatt sich auf ein falsches Gefühl der Sicherheit zu verlassen, suchen viele Unternehmen jetzt den Rat von Experten mit umfassender Kompetenz hinsichtlich Fragen zu rechtlicher Compliance und IT – mit nachgewiesener Erfahrung in der Anwendung forensisch einwandfreier Methoden.

Kroll Ontrack kann Ihnen bei der Entwicklung einer maßgeschneiderten Lösung helfen:

- **Datenerkennung, Datenzuordnung und Datenerfassung –** geschäftsentscheidende und rechtlich relevante Daten lokalisieren, erhalten und erfassen
- **Migration –** große Datenmengen sicher migrieren
- **Medienkonsolidierung –** inkrementelle oder differenzielle Sicherungen zu einer Sicherungskopie kombinieren
- **Medienkonvertierung –** reibungs- und nahtlose Konvertierung eines Datenformates in ein anderes
- **Bandkatalogisierung –** durch Katalogisieren Zeit, Geld und Ressourcen sparen
- **Bänder duplizieren –** Daten auf unkomplizierte Weise reproduzieren
- **Aufnahme/Archivierung von Bändern –** Bänder für die Aufnahme in ein Archivierungssystem oder System zur Aufbewahrung aus juristischen Gründen vorbereiten

Ein Beispiel aus der Praxis

Für einen Kroll Ontrack-Kunden – ein Fortune 500-Pharmazieunternehmen – wurde Datenmanagement-Kompetenz plötzlich sehr wichtig: In einem Keller, der zum Teil durch eine Sprinkleranlage überflutet worden war, fand man Sicherungsbänder. Niemand kannte den Inhalt der Bänder, und die gespeicherten Daten reichten bis ins Jahr 1996 zurück – bis zu einem Zeitpunkt vor der Übernahme des Unternehmens, dem die Daten ursprünglich gehört hatten. Ungefähr 10% der Bänder waren erst durch das Sprinklersystem beschädigt worden.

Der Kunde schickte Kroll Ontrack über 5100 Medienobjekte (im DLT-, LTO-, Exabyte-, DDS- und CD-Format und anderen Formaten). Gemäß den Anforderungen der Versicherungsgesellschaft musste der Auftrag innerhalb von 6 Monaten erledigt werden. Da die Versicherungsgesellschaft die Wiederherstellung der Daten finanzierte, war sie sehr daran interessiert, dass eine möglichst große Datenmenge von den verschmutzten Bändern wiederhergestellt wird. Schließlich stellte Kroll Ontrack die Daten wieder her und kopierte sie auf mehrere 2-TB-Festplatten.

Über Kroll Ontrack

Kernkompetenzen von Kroll Ontrack sind, neben professioneller Datenrettung, die sichere Datenlöschung, Tape-und Backup-Management, Mailbox Recovery und Computer Forensik. In Deutschland ist die Kroll Ontrack GmbH mit 60 Mitarbeitern seit 1996 in Böblingen vertreten. International beschäftigt das Unternehmen etwa 2.000 Angestellte in mehr als 20 Ländern.

Kroll Ontrack hat sich weltweit als der größte, meist erfahrene und technologisch führende Anbieter von Produkten und Dienstleistungen für die Wiederherstellung von Daten etabliert. Logisch oder physikalisch beschädigte Daten werden in firmeneigenen Laboren und Reinräumen wieder verfügbar gemacht. Mehr als 50.000 zufriedene Kunden pro Jahr nutzen weltweit diesen Service.

Für permanente Datenverfügbarkeit bietet Kroll Ontrack Lösungen zum Tape- und Backupmanagement u.a. durch Konvertierung aus unterschiedlichen Medien- und Dateisystemen.

www.ontrack.de,
www.krollontrack.de

Kroll Ontrack

Mehr Informationen im Internet oder
über unsere kostenlose Hotline:
0800 10 12 13 14
www.krollontrack.de