

## Komplettlösung für regelbasierte Datenaufbewahrung

# Gesetzeskonform speichern

Fast alle Unternehmen sind gezwungen, Daten nicht nur sicher abzulegen. Gesetzliche und interne Regeln geben zudem vor, dass Informationen unveränderbar, revisionssicher und über lange Zeit vorzuhalten sind. Diese so genannten Compliance-Anforderungen bestimmen vermehrt die Speicherstrukturen.

### .. ULRIKE RIESS

Datenfluten auf Speichermedien zu bannen ist längst kein Problem mehr. Auch große Speicherkapazitäten sind mittlerweile kostengünstig zu erwerben, TBytes lassen sich bereits auf kleinen Flächen verstauen. Dafür baut sich sukzessive ein viel größeres Problem auf: die Verwaltung der stetig wachsenden Informationen. Hinzu kommen Compliance-Anforderungen, gesetzlicher oder betriebsspezifischer Natur, die Firmen zum Umdenken in ihren Speicherumgebungen zwingen.

Michael Schwend, Technical Sales Manager bei **gingcom**, weiß, dass viele Unternehmen sich mit den verlangten Vorgaben heute noch schwer tun: »Vor allem Speicherhersteller treiben das Thema Compliance an. Für zahlreiche Unternehmen ist dies aber ein Begriff, der schwer zu konkretisieren ist. Weiterhin gelten für jede Branche und somit für jede Firma andere Vorschriften. Somit lässt sich auch nicht eine Lösung für alle Bedürfnisse entwickeln und einsetzen. Planungs-, Entwicklungs- und Umsetzungsprozess dauern bei Compliance-Projekten deutlich länger. Hier ist eindeu-

tig Verständnis und Erklärung seitens der Hersteller, aber auch Einsicht und Geduld bei Kunden gefragt.«

### Langzeitarchivierung und regelbasiertes Compliance-Management

Um Compliance-Projekte nutzbringend umzusetzen bedarf es gezielter Planung und strukturierter Sicherungsprozesse. Es gilt nicht nur gesetzliche Vorschriften einzuhalten, sondern Daten auch für den Fall einer Revision oder einer kriminaltechnischen Überprüfung verfügbar und unveränderbar vorzuhalten. Regelbasierte Sicherungsprozesse sowie Langzeitarchivierung sind deswegen für die meisten Unternehmen ein Muss in IT-Planung und -Umgebung. Nicht immer waren solche Voraussetzungen für Speicherprojekte gegeben: »Bis vor kurzem wurde die steigende Datenflut gern mit mehr Speicherplatz und Hardware eingedämmt«, sagt Gingcom-Manager Schwend. »Kontinuierlich sinkende Preise für Speicherplatz machten das relativ einfach. Zudem gibt es keine gesetzliche

Vorgabe, wie und mit welcher Technologie die für das Unternehmen relevanten Daten aufzubewahren sind. Die Spielräume sind hier weit gefasst. Trotzdem erkennen die Anwender die Notwendigkeit und die Vorteile von Speicherstrukturen, regelbasierter Datensicherung und nutzbringendem Management.«

Jede Information hat einen anderen Lebenszyklus und so auch einen anderen Wert für das Unternehmen. Daraus ergibt sich aber auch eine individuelle Handhabung der verschiedenen Datenobjekte. Hersteller Gingcom verfolgt den Ansatz, Dateien und E-Mails in einer so genannten Tiered-Storage-Struktur zu si-

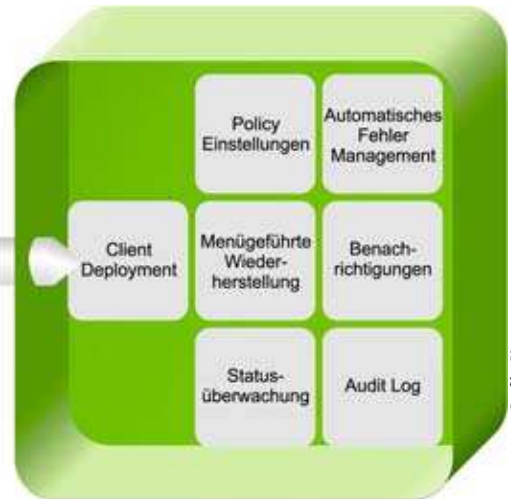


**Gingcom GmbH**  
Saline 29  
D-78628 Rottweil

Tel. 07 41/24 86 68  
Fax 07 41/24 86 69  
[info@gingcom.de](mailto:info@gingcom.de)  
[www.gingcom.de](http://www.gingcom.de)

chern. Dabei erfolgt die Auswahl des Speichermediums je nach Wert der zu sichernden Datei. Daten in ständigem Zugriff, die kritisch für den Geschäftsprozess sind, liegen meist auf FC-Festplatten im Online-Speicher. Weniger sensible Daten, die aber auch über hohe Zugriffszahlen verfügen, liegen oft in SATA-Silos. Informationen, deren Inhalt nur noch für Revisionen und andere Überprüfungen genutzt werden, sind auf Magnetbändern oder optischen Medien sicher verwahrt. Oft ändert sich der Wert eines Dokuments, dann kann es entsprechend auf einen anderen Speicherbereich geschoben werden.

Der Administrator muss die Datenmenge nicht manuell verwalten. In der regelbasierten Verwaltung lassen sich so genannte Policies ansetzen, welche die Dateien über ihren Lebenszyklus hinweg überwachen. Dabei lassen sich nicht nur Regeln für den Speicherort festlegen, sondern auch für Zugriffsberechtigungen. Mit der Gingcom-Appliance kann der IT-Verantwortliche sicherstellen, dass nur Berechtigte auf bestimmte Informationen zugreifen können, selbst in der



Grafik: Gingcom

Ein zentrales Management bringt besten Überblick über alle Sicherungsprozesse und erleichtert Compliance.

unternehmensweiten Suchanfrage. Das ist besonders relevant für Personalakten, Finanzinformationen oder auch Entwicklungsmaterial. Selbst E-Mails, die diesbezüglich Auskunft geben, können so gesichert werden.

## Die Umsetzung der wichtigsten Anforderungen

Einer der wichtigsten Compliance-Faktoren ist die Aufbewahrungszeit. Der Gesetzgeber schreibt sehr genau vor, welches Unternehmen seine Daten über welchen Zeitraum lesbar und zugreifbar vorhalten muss. Das können sechs Monate für Telekommunikationsdaten sein, aber auch 100 Jahre wie beispielsweise für Grundbuchämter. In der Regel müssen Vertragsdaten jeder Firma sieben Jahre vorliegen. Meist richtet sich die Wahl des Archiv-Medium nach der Dauer der Aufbewahrung.

Mit der Gingcom-Lösung lassen sich so genannte »document retention policies« anlegen, die das Dokument entsprechend der Aufbewahrungsfrist schützen. Diese Regeln legen auch fest, wie lange die Datei verwahrt und wann sie kontrolliert gelöscht wird. Der IT-Verantwortliche kann »Archive Retention Time« (ART) und »Backup Retention Time« (BRT) festlegen. BRT beschreibt die Zeit, in der Informationen periodisch gesichert werden und mittels Browsersuche abrufbar sind. ART definiert die Parameter der Langzeit-aufbewahrung. Diese Zeit ist länger als



Grafik: Gingcom

Eine effiziente Compliance-Strategie muss alle Aspekte von Datensicherung und -schutz bis zu Informationsmanagement und IT-Infrastruktur umfassen.

BRT und Daten lassen sich über eine einzigartige Suchfunktion auffinden. Nach Ablauf der ART erfolgt das kontrollierte Löschen der jeweiligen Information.

Diese Retention-Policys lassen sich mittels des Gingcom-Systems auch auf E-Mails anwenden. »Dieses Tool ist enorm wichtig«, betont Schwend. »E-Mail-Verkehr hat heute einen viel höheren Stellenwert als noch vor einigen Jahren. E-Mails können wichtiges Firmenskapital werden, da sie Informationen wie sekundäre Vertragsvereinbarungen und gegenseitige Absprachen enthalten können. Über eine Journaling-Mailbox sammelt die Gingcom-Appliance Nachrichten vom Exchange-Server und sichert diese dann entsprechend den eingestellten Policys. Die gesamte elektronische Korrespondenz kann nach Nutzergruppen unterteilt und nur für die autorisierten Anwender abrufbar sein.«

Eine weitere Anforderung ist die Einhaltung der Zugriffsrechte. Die Suchfunktion innerhalb der Gingcom-Lösung orientiert sich deshalb präzise an den bestehenden Zugriffsbestimmungen in der jeweiligen Domäne.

So werden zum Beispiel bei der Archivierung einer Datei nicht nur die jeweiligen gültigen Zugriffsberechtigungen son-

dern neben der Datei selbst auch alle Metadaten des gesicherten Objekts, beispielsweise Dateiname, Schlüsselwörter innerhalb des Dokuments und Name der Quelle sowie das Erstellungsdatum in einer speziellen Datenbank erfasst. Darüber hinaus unterstützt das System verschiedene Sprachen zur Bedienung und alle herkömmlichen Dateiformate, wie zum Beispiel doc, html oder pdf.

### Unverfälscht und auditfähig

Darüber hinaus ist ein »Auditing« heute in allen Betrieben unerlässlich, um den Weg einzelner Dateien nachzuvollziehen. Damit lässt sich überprüfen, welcher Mitarbeiter eine Datei »angefasst« oder neu angelegt hat. Dies erfolgt bei Gingcom über Log-Files. So ist erkennbar, welche Aktivitäten ein Dokument durchlaufen hat. Unternehmen können sicherstellen, dass ihre gesicherten Daten nicht verändert wurden.

Eine besondere Funktion der Gingcom-Appliance ist die ständige und zufällige Überprüfung der im Archiv befindlichen Dateien. Dies ist wichtig bei der Archivierung über längere Zeiträume. Diese automatische Überprüfung soll die Integrität und damit die Wiederher-

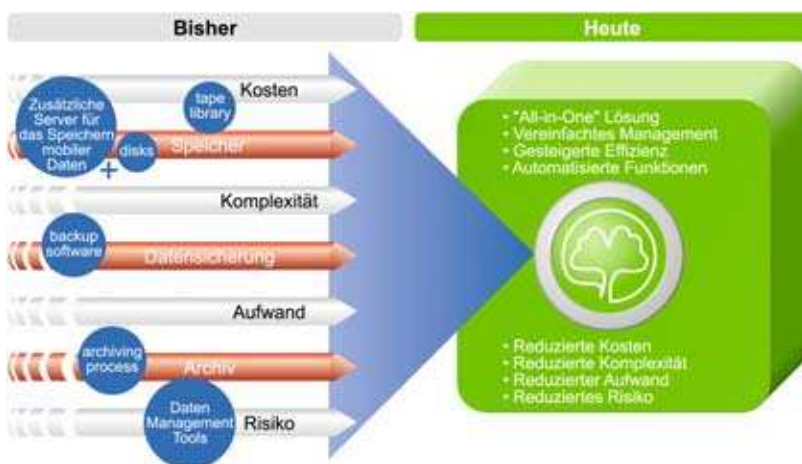
stellbarkeit der gesicherten Informationen garantieren.

Um diese Unveränderbarkeit der archivierten Dateien zu gewährleisten, hat Gingcom ein WORM-ähnliches Verhalten in sein System integriert. Um eine eindeutige Identifizierung zu ermöglichen, arbeitet die Gingcom-Lösung mit so genannten Hash-Keys, die auch als der Fingerabdruck einer Datei bezeichnet werden können. Einen unveränderbaren Hash-Key erhält die Datei direkt bei ihrer Erstellung, beispielsweise an einem Laptop oder Desktop-PC. Diese Aufgabe erfüllt ein spezieller Gingcom-Agent, der das zu schützende System permanent überwacht. Jeder Rechner, der einen solchen Agenten hostet, ist automatisch mit der steuernden Instanz verbunden, der eigentlichen Appliance.

Der berechnete Hash-Key ist einmalig für jede Datei. Wird eine bereits in Gingcom archivierte Datei aufgerufen und verändert, so erhält sie nach der Änderung einen neuen Hash-Key. Damit erfüllt die Gingcom-Appliance eine weitere Compliance-Anforderung, da alle Versionen der Datei einzeln eingesehen werden können und getrennt aufbewahrt werden.

### Rundum konform durch eine Komplettlösung

Die Gingcom-Appliance verbindet Hard- und Software in optimaler Kombination. Zusammen mit anderen Funktionalitäten für Backup, Datenduplizierung und gesetzeskonformer Langzeitarchivierung kann diese Lösung Unternehmen mit 50 bis 500 Mitarbeitern dienen. Für den Online-Speicher stehen bis zu 18 Platteneinschübe zur Verfügung. Diese fassen je nach Bedarf SAS- oder SATA-Festplatten, auch in Mischkonfiguration. Darunter stehen zwei Bandlaufwerke, wahlweise LTO-2 oder LTO-3, für die Archivierung zur Verfügung. Weil die Lösung für Microsoft-Umgebungen optimiert wurde, ist eine Integration in bestehende Netzwerke in nur rund zweieinhalb Stunden bis zur Inbetriebnahme abgeschlossen. Insgesamt stehen dem Anwender entweder 2,2 oder 4,4 TByte an nutzbarem Speicher zur Verfügung. ■



Grafik: Gingcom

Die All-in-One-Funktion reduziert die Komplexität des bisherigen Aufwands.