storage-magazin.de

Ausgabe **1-2018**

Eine Publikation von **speicherguide.de**

Grafik: fotolia.de / istockphoto.com / speicherguide.de

# Backup für den Mittelstand

## Trend: Datensicherung muss sich verändern

# Nur regelmäßige Backup-Tests schützen vor bösen Recovery-Überraschungen

Liebe Leserinnen und Leser,

Karl Fröhlich, Chefredakteur speicherguide.de

letztes Jahr habe ich an dieser Stelle darauf hingewiesen, dass Backup & Recovery heute bei weitem nicht mehr ausreichen. Firmen müssen ihre Datensicherungsstrategien auf den Prüfstand stellen und Data-Protection als umfassenden Datenschutz erkennen und einführen. Damals hatte ich drei Problemherde definiert: Bedrohungen von außen, unterschiedliche Datenquellen und das Erfüllen rechtlicher Bestimmungen und Vorschriften. Die sind nicht nur weiterhin gültig, sondern haben sich fast dramatisch verschärft.

Ransomware gilt nach wie vor als ernstzunehmende Bedrohung. Mit jedem Cloud-Dienst und neuem Mitarbeiter kommen zusätzliche Datenquellen hinzu. Und wenn am 25. Mai die Schonfrist für die Datenschutz-Grundverordnung (DSGVO) endet, werden einige erkennen, dass sie diese Vorschrift und deren Handhabung massiv unterschätzt haben. Das wird sich vor allem auf kleinere Firmen auswirken. Konzerne und große Mittelständler müssen schon aus Compliance-Gründen – und natürlich aus eigenem Interesse – die DSGVO korrekt umsetzen. Je kleiner die Unternehmen der Sparte KMUs werden, desto weniger bis gar nicht haben sich die Verantwortlichen mit dieser Problematik auseinandergesetzt.

Da frage ich mich schon, wie kann das sein? Eine Antwort oder besser eine Bestätigung erhalte ich, während ich diese Zeilen verfasse. Kroll Ontrack schreibt in einer Pressemeldung: Die Anzahl der »Backup-Verweigerer« bleibt hoch. Bitte, was!? Eine Umfrage zum »World Backup Day« ergab, dass ein Drittel der Befragten Unternehmen und Verbraucher kein aktuelles Backup von ihren wichtigen Daten besitzen. Als Grund wird angeführt, es fehle an Zeit, um eine geeignete Backup-Lösung zu finden und diese regelmäßig zu administrieren.

Aber es geht noch weiter: »Warum haben so viele Umfrageteilnehmer einen Datenverlust erlebt, obwohl sie über eine Backup-Lösung verfügen? Eine Antwort darauf ist, dass sie nicht oft genug testen oder prüfen, ob ihr Backup auch ordnungsgemäß funktioniert.«

Ich gehe davon aus, dass alle, die hier mitlesen, ebenso verwundert sind wie ich, oder? Vorschlag: Lesen Sie in diesem Special erstmal über die aktuellen Trends in den Bereichen Backup/Recovery und Data-Protection, Datenschutz und Tape. Dann holen wir uns ein Heiß- oder Kaltgetränk nach Wahl und überprüfen unseren Notfallplan und ob unsere Backups auch wunschgemäß funktionieren.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

## Inhalt

Datenwachstum und unterschiedliche Datenquellen forcieren Komplexität

# Trend: **Datensicherung muss sich verändern**

Das Thema Datensicherung war noch nie als etwas Einfaches verschrien. Im Zuge der Digitalisierung mit vielen Anwendungen und dem zunehmenden Cloud-Einsatz steigt allerdings die Komplexität in ungeahntem Ausmaß. Neben dem Datenwachstum forcieren vor allem unterschiedliche Datenquellen die Komplexität.

Karl Fröhlich

Backup & Recovery, Data-Protection oder Business-Continuity – egal, wie man es nennt, es wird immer komplexer. Das vielbeschworene Datenwachstum ist der eine Aspekt, fast noch problematischer sind die unterschiedlichen Datenquellen. Da sind zunächst physische und virtuelle Entstehungs- und Speicherorte zu nennen. Hinzukommen externe Orte, wie das Internet, mobile Arbeiter mit unterschiedlichen Gerätschaften und mittlerweile diverse Cloud-Dienste und auch aus dem Internet der Dinge (Internet of Things, IoT) sprudeln die Informationen nur so hervor. All diese Quellen gilt es in einer einheitlichen Data-Protection-Strategie zu vereinen. Das Problem: Eine Vereinheitlichung und Zentralisierung der nötigen Datensicherungs-Tools ist mehr oder weniger unmöglich.

Den Marktforschern von **Gartner** zufolge, plant die Mehrheit der der Organisationen ihre momentane Backup-Anwendung bis 2021 mit einer anderen Lösung zu ergänzen oder zu ersetzen. Bis 2020 werden 30 Prozent der großen Unternehmen Snapshots und Backups für mehr als nur operative Recoverys einsetzen (z.B. Disaster-Recovery, Test, Entwicklung, DevOps). Gegenüber dem Jahresanfang 2017 würde dies einer Verdoppelung entsprechen. Gleiches gilt für traditionelle Backup-Anwendungen, die 30 Prozent der Organisationen bis 2020 mit Storage- oder HCIS-Funktionen (Hyperconverged Integrated Systems) für die Mehrheit der Backup-Workloads einsetzen werden.

Bis 2020 soll sich die Anzahl der Unternehmen, welche die Cloud als Backup-Ziel nutzen, auf 20 Prozent verdoppeln. Zudem erwartet Gartner, dass bis 2021 über 50 Prozent der Organisationen die Sicherung mit der Archivierung für die langfristige Datenerhaltung ersetzen. 2017 sind es bisher noch 30 Prozent.

## Backup nicht zu ersetzen

Laut Gartner sollen bis 2022 20 Prozent der Speichersysteme selbstschutzfähig sein. Dies vermeide angeblich generell die Notwendigkeit von Backup-Anwendungen. Dies darf aber bezweifelt werden. Selbst wenn die Speicher 100-prozentig hochverfügbar ausgelegt und resistent gegen äußere Einflüsse wie Feuer und Wasser sein sollten, es ist unwahrscheinlich, dass sie auch gegen Nutzerfehler gefeit sind. Versehentlich gelöschte Daten gehören zu den meisten Recovery-Szenarien.

Auch beim Verlagern von Daten in die Cloud begehen Administratoren durchaus den Denkfehler, die Daten wären beim Provider sicher aufgehoben. In den allermeisten Fällen bezieht sich der Cloud-Vertrag aber nur auf die Verfügbarkeit der aktuellen Daten. »Die Vermeidung von Datenverlust durch Fehler von Benutzern, durch fehlerhafte Software, durch Angriffe von Hackern oder durch Ransomware fällt weiterhin in den Bereich des Kunden«, mahnt **Rainer Kalthoff**, Sales Engineer Central & Eastern Europe bei **Unitrends** (lesen Sie mehr im Interview auf Seite 16). ■

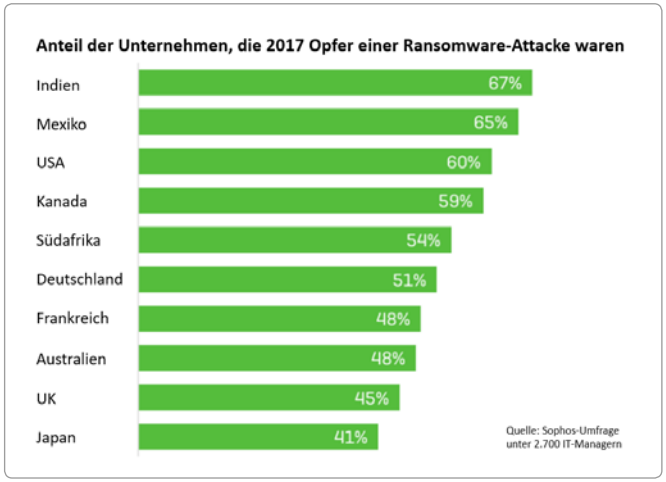
Cyberangriffe: Rund 107.000 Euro Schaden für die Unternehmen

# Ransomware bleibt Schlüsselbedrohung

Schlechte Nachricht für Unternehmen, Ransomware bleibt ein Risikofaktor. Einer Studie von Sophos zufolge war letztes Jahr jede zweite Firma betroffen – im Durchschnitt sogar jeweils zweimal. In Zukunft sollen Deep-Learning-Lösungen für mehr Sicherheit sorgen. Ein aktuelles Backup hilft bei der Wiederherstellung, wenn es getrennt von den Produktivdaten gehalten wird.

Karl Fröhlich

Jedes zweite Unternehmen war 2017 von Ransomware betroffen. Im »Ransomware-Ranking«, belegt Deutschland Platz 6. Zu diesem Ergebnis kommt eine internationale Studie von **Sophos**. 2.700 IT-Entscheider aus Unternehmen mittlerer Größe identifizieren in zehn Ländern Ransomware als eine der Hauptbedrohungen für die IT-Sicherheit. 54 Prozent aller befragten Firmen sahen sich 2017 Attacken durch die Erpressungs-Software ausgesetzt – und dies im Durchschnitt sogar zweifach. Gut 30 Prozent erwarten Ransomware-Angriffe für die Zukunft.




Grafik: Sophos

Opfer von Ransomware-Attacken: **Deutschland ist weltweit auf Platz 6**, trägt aber in Europa das meiste Risiko.

Unternehmen zahlten einen hohen Preis für die Ransomware-Angriffe: Im Schnitt beliefen sich die Schadenskosten auf rund 107.000 Euro. Der genaue Blick auf Deutschland zeigt, dass 63 Prozent einen Schaden zwischen 11.200 und 282.000 Euro erlitten. Die meisten, nämlich 26 Prozent, bezifferten ihre Kosten auf zwischen 56.000 und 112.000 Euro. Bemerkenswert: Im Gegensatz zu Frankreich und dem Vereinigten Königreich, wo auch Beträge im vierstelligen Bereich anfielen, kam in Deutschland kein Unternehmen mit einem Geldwert unter 11.200 Euro davon.

## Ransomware schlägt mehrfach zu

Auffallend ist die Tatsache, dass die Unternehmen in der Regel zweimal attackiert werden. Und dies, obwohl die Mehrheit über ein gängiges IT-Sicherheitskonzept verfügt. Damit die Attacke aber erfolgreich ist, lassen Cyberkriminelle mitunter innerhalb von einer halben Stunde bis zu vier verschiedene Ransomware-Familien frei. Wenn es den IT-Administratoren in Unternehmen nach einem Angriff außerdem nicht vollständig gelingt, die Systeme von der Schadware zu befreien, ist eine Neu-Infektion jederzeit möglich.

Ein Großteil der Befragten war sich zwar bewusst, dass ihre herkömmlichen Sicherheitskonzepte nicht mehr in genügendem Maße greifen, haben aber noch keine weiteren Schritte eingeleitet. Prädiktive Next-Generation-Technologien wie Machine-Learning oder Deep-Learning kommt bisher nur bei einem Viertel zum Einsatz. Immerhin planen in Deutschland 68 Prozent entsprechende Sicherheitsmodule zu implementieren.

Als Gegenmaßnahme empfehlen sich Sicherheitskonzepte auf Basis von Deep-Learning. Damit sollen im Vergleich zum herkömmlichen Machine-Learning genauere Vorhersagen möglich sein, da sich eine viel höhere Anzahl an Stichproben verarbeiten lässt. Damit im Schadensfall betroffene Daten wiederhergestellt werden können, müssen die Backup-Daten getrennt vom Produktivsystem aufbewahrt werden. ■

Muss es wirklich wieder Tape sein?

# **Backup-Storage** in Zeiten von Ransomware und DSGVO

Foto: Fast LTA

**Silent Bricks** sind mit Festplatten oder SSDs bestückt erhältlich, eine Hardware WORM-Versiegelung ist optional.

Eine Backup-Strategie, egal für welche Unternehmensgröße, schließt ein Offline-Medium wie Tape oder Disk mit ein. Nur Medien ohne Verbindung zur IT sind nicht angreifbar. Eine zeitlose Anforderung, vor allem in Zeiten von Ransomware und DSGVO. FAST LTA plädiert für Disk und nennt die Vorteile für KMUs.

Hannes Heckel, FAST LTA

Laut einer aktuellen Studie von **Gartner** *(Discover the Truth About the Use of Disk, Tape and Cloud Backup in 2017)* sind in Europa und den USA nach wie vor über ein Drittel aller Backup-Installationen als Backup-to-Disk-to-Tape (D2D2T) realisiert. Was treibt Unternehmen dazu, weiterhin die in vieler Hinsicht unbeliebten Magnetbänder zur Sicherung einzusetzen?

## Die Argumente für Tape als Tier-3-Storage

Drei Hauptargumente sprechen für Tape:

1. Preis/TByte
2. Skalierbarkeit
3. Sicherheit

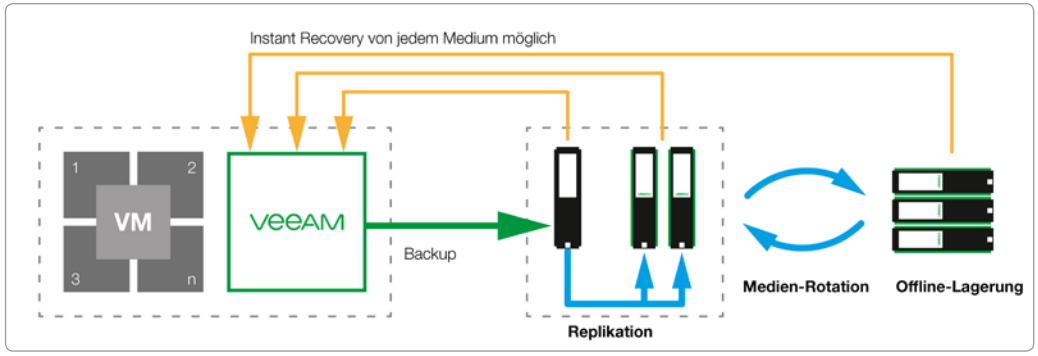
Alle drei basieren auf dem unterschiedlichen Infrastruktur-Prinzip von Bandspeicher und Disk-Speicher: Bei Tape sind Laufwerk und Medium getrennt. Das ermöglicht es, dass Tape den an sich unfairen Vergleich von »Kosten pro TByte« immer gewinnen wird. Investitionskosten in die Erweiterung der Infrastruktur bleiben unberücksichtigt. Auch Kosten für Wartung und Betrieb von mechanisch aufwändigen Tape-Laufwerken dürfen in der TCO-Rechnung nicht vergessen werden.

Da Speicher im Tier 3 nicht ständig online sein muss, werden Wartezeiten und Aufwand akzeptiert, um die angeforderten Daten wieder herzustellen. Die meisten Disk-Systeme müssen dagegen von Anfang an auf eine zu erwartende Kapazität dimensioniert werden, um mit dem Daten-Wachstum mitzuhalten. Und auch das dritte Argument hat mit der Medientrennung zu tun: die Sicherheit. Ein Offline-Medium, ohne Verbindung zur IT, ist nicht angreifbar und kann bei Bedarf leicht dem Eigentümer übergeben werden.

## Die Argumente für Disk-Storage

Vor allem Anfälligkeit durch mechanische Beanspruchung und die Linearität sprechen gegen Tape. Der Zugriff auf einzelne Dateien ist zeitraubend und zur Absicherung gegen Totalausfall müssen Bänder regelmäßig umkopiert werden.

Wir sehen daher einen zunehmenden Willen zum Umstieg auf moderne Technologien. Unsere Kunden sind allerdings aus gutem Grund vorsichtig und zurückhaltend.




Grafik: Fast LTA

Backup-to-Disk-to-Disk (mit Replikation und Offline-Lagerung) mit Veeam und Silent-Bricks.

Ein funktionierendes Tape-Backup zu ersetzen, erfordert Mut und Vertrauen in die ablösende Technologie und deren Anbieter.

## Anforderungen an ein modernes Backup-System

Für einen konkreten, typischen Anwendungsfall gelten beispielsweise folgende Parameter, wie sie so ähnlich bei den meisten unserer Backup-Kunden vorkommen:

- Mehrere TByte an Backup-Daten in verschiedenen Zyklen (daily, weekly, etc.)
- Server sind zunehmend virtualisiert
- Oft steht eine Umstellung der Backup-Software, z.B. zu **Veeam**, an
- Im Zuge dessen soll eine vorhandene Tape-Infrastruktur abgelöst werden, da
  - diese nicht Instant-Recovery-fähig ist
  - diese einen hohen Wartungsaufwand erzeugt
  - der Wunsch nach weniger Komplexität besteht
- Zusätzlich ist oft der Wunsch nach schrittweiser Umstellung mit minimalem Risiko vorhanden

## Die Umsetzung

Systeme und Infrastrukturen in Unternehmen sind über die Jahre gewachsen, Workflows etabliert, und der tägliche Betrieb läuft mehr oder weniger reibungslos. Ein schrittweiser Ersatz vorhandener Systeme ist dabei Grundvoraussetzung. Das folgende Beispiel zeigt anhand einer typischen Veeam-Installation, wie ***FAST LTA*** *Silent Bricks* vorhandene Infrastrukturen schrittweise ersetzen, Workflows optimieren und Kosten sparen können.

## Schritt 1: Ersatz der Tape Library

Kommt Tape zum Einsatz, ist der Ersatz der mechanisch anfälligen Librarys der erste Schritt. Im Falle einer Veeam-Installation wird dabei auch gleich das Tier-2-NAS ersetzt – beide Aufgaben erledigen dann Silent Bricks. Die vorhandene NAS-Installation übernehmen ein oder mehrere Silent Bricks als NAS-Konfiguration. Die Sicherheit wird gegenüber einem RAID-System wesentlich erhöht. Die Anbindung erfolgt weiter über SMB- oder NFS-Shares. Veeam schreibt die erste Backup-Instanz dann ohne sichtbare Änderungen auf das neue Silent-Brick-NAS.

Für die zweite Instanz – bisher Tape – übernimmt eine VTL-Konfiguration mit Silent Bricks. Wie »große Tapes« unterstützen sie auch die Medienrotation von Veeam. Der Umstieg erfolgt zügig und quasi 1:1, ohne veränderte Konfigurationen oder Workflows. Die Offline-Fähigkeit bleibt durch VTL und Medienrotation voll erhalten.

Es gibt aber auch Nachteile dieser Konfiguration. Zum einen werden beide Backup-Instanzen weiterhin über Veeam und den entsprechenden Server erstellt. Zum anderen muss zur Wiederherstellung per Restore auf die VTL-Medien zurückgegriffen werden, ein Instant Recovery ist von diesen Medien – trotz Disk-Basis – nicht möglich.

## Schritt 2: Umstellung auf Replikation

Um die genannten Nachteile zu beseitigen, kann die zweite Instanz vollständig über das Silent-Brick-System erstellt werden. Das »Tape«-Handling fällt dabei weg, die Offline-Fähigkeit bleibt aber erhalten. Dazu erstellt das Silent-Brick-System via Replikation zwei separate Instanzen des Original-Backups. Per Medienrotation bleibt ein Silent Brick jeweils im System, der andere wird offline gelagert. In definierten Abständen erfolgt ein Tausch der Silent Bricks. Die Veeam-Appliance erstellt dabei nur die Instanz, dies reduziert Traffic und Load. Der Hauptvorteil ist jedoch, dass von jedem Medium, online oder offline, jederzeit ein Instant Recovery gestartet werden kann. Die Absicherung gegen Katastrophen oder die Umsetzung einer Stern-Struktur mit zentralen Backup-Servern ist jederzeit möglich – auch nachträglich.

## Schritt 3: Konsolidierung der Speichersysteme

Kunden wünschen sich eine vereinfachte Speicher-Infrastruktur. Durch die individuelle Konfiguration des Silent-Brick-Systems, lassen sich vorhandene Systeme jederzeit konsolidieren. Vor allem bei der Archivierung, zum Teil auch revisionssicher, besteht ein hohes Sicherheitsbedürfnis, das Silent Bricks ideal adressieren. Insbesondere mit dem zertifizierten *Silent Brick WORM* mit Hardware-Versiegelung.

Aber auch das einfache Unternehmens-NAS lässt sich mit Silent Bricks effizient ersetzen. Durch die flexible Skalierbarkeit, ist ein Ausbau jederzeit – auch nach Jahren – problemlos möglich.

Somit entsteht eine konsolidierte und dennoch spezialisierte Speicherstruktur für jede Kapazitäts-Anforderung. Ein System, mit einheitlicher Benutzeroberfläche, deutschen Ansprechpartnern in Vertrieb und Service, und günstige Wartungsverträge mit bis zu zehn Jahren Laufzeit, reduzieren Aufwand, Kosten und Sorgen. ■

**Weitere Informationen**

**FAST LTA AG**
Rüdesheimer Str. 11
80686 München
Tel. 089/89 047-0
E-Mail: info@fast-lta.de
**www.fast-lta.de**

Datenschutz gilt über den Lebenszyklus der Daten und Technologien

# EU-DSGVO – Countdown für die Datensicherheit

Die EU-Datenschutz-Grundverordnung wirkt sich auch auf die Datensicherung aus. Zu erstellen sind Datenschutz- und Datensicherheitskonzepte sowie Folgeabschätzungen. Gegen das Risiko eines Datenverlusts und gegen Verletzungen des Datengeheimnisses gilt es Vorkehrungen zu treffen und zu dokumentieren. »SEP sesam Backup & Recovery« liefert die technische Sicherheit zur Umsetzung der DSGVO.

Andreas Mayer, SEP

Die EU-Datenschutz-Grundverordnung (DSGVO) wird am 25.05.2018 auf Unternehmen und Behörden unmittelbar anwendbar. Das heißt, ab da können hohe Bußgelder fällig werden. Bis zu zehn bzw. 20 Millionen Euro oder bis zu zwei oder vier Prozent des Jahresumsatzes kann die Strafe betragen. Höchste Zeit für Unternehmen und Organisationen sich damit intensiver auseinander zu setzen, denn sehr viele sind dafür noch nicht bereit, wie eine Studie der *Nationalen Initiative für Internetsicherheit* (NIFIS) zeigt. Danach wird von 57 Prozent der befragten IT-Sicherheitskräfte erwartet, dass zum 25. Mai nur 26 bis 50 Prozent der deutschen Unternehmen in der Lage sein werden, die DSGVO-Vorgaben gesetzeskonform umzusetzen. Die DSGVO wirkt sich auf alle Unternehmen aus, die geschäftlich von der EU aus tätig sind bzw. Geschäftsbeziehungen zu Unternehmen/ Organisationen mit Sitz in der EU unterhalten oder Daten in EU-Mitgliedsstaaten sammeln, verarbeiten und speichern. Unternehmen, auch außerhalb der EU, welche Geschäftsbeziehungen zu Unternehmen in der EU und/oder EU-Bürgern mit der Verarbeitung von personenbezogenen Daten unterhalten, unterliegen der DSGVO. Somit sind die Konsequenzen der DSGVO schon fast als weltweit anzusehen. Neu ist auch, dass sogenannte Auftrags-Datenverarbeiter, wie MSP und Cloud-Provider nun auch in der Pflicht sind, die Daten rechtskonform zu behandeln und nicht wie bisher, dass nur der Auftraggeber in der Pflicht war.

## Was sind personenbezogene Daten?

Dies sind Daten, welche sowohl berufliche als auch private Informationen über eine Person beinhalten wie Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge auf Social-Networking-Websites, medizinische Daten sowie auch die IP-Adressen.

## Maßnahmen

Zur DSGVO gehört auch, dass Datenschutz- und Datensicherheitskonzepte sowie Datenschutz-Folgeabschätzungen zu machen sind. Die Datenschutzkonzepte müssen durch technisch-organisatorische Strategien und deren Umsetzung sicherstellen und nachweisen können, dass die DSGVO eingehalten wird. Dies soll auf der Grundlage einer Risikobewertung erfolgen, die auch zu dokumentieren ist ebenso wie auch die hieraus abgeleiteten Maßnahmen in Bezug auf die IT-Sicherheit und die von der IT ausgehenden, unternehmensgefährdenden Risiken durch Datenverlust oder Verletzungen des Datengeheimnisses.

Die Umsetzung muss durch Maßnahmen realisiert werden, die dem aktuellen Stand der Technik entsprechen und dem Datenschutzniveau sowie den Risiken angemessen sind. Dazu sollte eine regelmäßige Soll-/Ist-Analyse mit Risikobewertung und mit einer entsprechenden Datenschutz-/Datensicherheits-Folgeabschätzung kommen, um den Transparenz-, Dokumentations-, ADV- und Sicherheitsmanagementpflichten der DSGVO gerecht zu werden. Datenschutz durch Technik ergänzt die organisatorischen Anforderungen der DSGVO und ist auf den gesamten Lebenszyklus der Daten und Technologien anzuwenden und zu dokumentieren.


Grafik: SEP

## Technische Komponente: Backup Software

Die Backup-Software stellt die technische Lösungskomponente dar und muss daher gewisse technische Anforderungen erfüllen sowie technische Mechanismen bereitstellen, um DSGVO-konform zu sein.

Die *SEP sesam Backup & Recovery*-Software liefert die technische Sicherheit, die Sie zur Umsetzung der DSGVO benötigen. SEP sichert herstellerkonform mit einer einzigen Lösung geschäftskritische Informationen in Applikationen, Datenbanken und Systemen sowohl in physikalischen als auch in virtuellen Umgebungen On-Premise und in der Cloud. Aufgrund der immensen Wichtigkeit der business-relevanten Daten wird eine umfassende Business-Continuity-Strategie benötigt, die auf Recovery-Point-Objectives (RPOs) und Recovery-Time-Objectives (RTOs) fokussiert ist, welche essentiell bei einem Disaster-Recovery-Szenario sind.

Die umfassende *SEP sesam Hybrid Backup-* und *Bare Metal Recovery*-Lösung verhindert Datenverlust und kann die gesamte Umgebung nach einem Disaster-Szenario wiederherstellen, beispielsweise bei höherer Gewalt, Hardware-Fehlern, menschlichen Fehlern, Datenkorruption sowie logischen und Software-Fehlern.

## Backup-Software mit Verschlüsselung

Die Nutzung des Medienbruchs mittels Offline-Medien (Tape) bei den SEP-Backup-Daten ist bei einer Ransomware-Attacke oft die einzige Möglichkeit, nicht infizierte Daten wiederherstellen zu können, falls die Backup-Daten auf den Disksystemen befallen sein sollten.

Zu den zentralen technischen Elementen gehört die Verschlüsselung. Daher ist zum Beispiel auch bei der technologisch führenden *SEP Si3*-Deduplizierung und -Replikation eine Verschlüsselung möglich. Nach Zerlegen des Datenstroms in Blöcke und der Komprimierung jedes Blocks, lässt sich jeder einzelne Block durch einen beliebig definierbaren Key verschlüsseln. Zur Wiederherstellung der Daten kann der Key in der Datenbank des Backup-Servers hinterlegt werden oder der Dateneigentümer muss eine Rücksicherung mit seinem persönlichen Key autorisieren. Diese Verschlüsselung garantiert *BSI*-Konformität.

Zusätzlich beinhaltet die Lösung eine Vielzahl technologischer Ansätze für die gesetzeskonforme Datensicherheit:

- Verschlüsselung der Backups auf Sicherungsmedien (Band, DataStore, Si3 DedupStore), des Datenstromes (On-Premise und in die Cloud) und der Kommunikation
- Externes Passwort für Rücksicherung nach dem 4-Augen-Prinzip
- Effizientes Disaster-Recovery
- Frei von Spyware/Backdoors (Made in Germany)
- Medienbruch: Unterstützung von Offline- und WORM-Medien
- Herstellerkonforme Datensicherung
- Sicherung der Daten auf verschiedenen Ebenen möglich (z.B. auf Hypervisor- und Applikationsebene)
- Standortübergreifende Datensicherung
- Automatische Migration bzw. Kopie von Sicherungsdaten auf unterschiedliche Sicherungsmedien
- Volle Unterstützung von Open-Source-Betriebssystemen auf Backup-Client- und Backup-Server-Seite
- Gesetzeskonforme Sicherung aller Unternehmensdaten
- Gewährt die Netzwerksicherheit in Firewall-Umgebungen durch Einschränken der Kommunikation und des Datentransports auf wenige, dedizierte Ports
- Geplanter und automatischer Restore auf Stand-by-Systeme zum Verifizieren der Backups (für Audits verwendbar)
- Disaster-Recovery-Tests im laufenden Betrieb inklusive Reporting

Mit SEP sesam sind die Daten 24x7 geschützt und immer verfügbar. Die technologische Lösung kann nur einen Teil der gesamten »Compliance-Lösung« darstellen und muss Hand in Hand an die vorher beschriebenen organisatorischen Maßnahmen, Prozesse, Konzepte, Risiko-Analysen, Dokumentationen, etc. gekoppelt werden, um so zu einer ganzheitlichen »rechtskonformen« Lösung zu werden. Mehr Informationen dazu im White-Paper von Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking. ■

**Weitere Informationen**

**SEP AG**
Konrad-Zuse-Straße 5,
83607 Holzkirchen
Tel. +49 (0)8024/463 31-0
E-Mail: info@sep.de
**www.sep.de/de**

Ein Lösungsansatz zur Effizienzsteigerung und Kostensenkung durch optimierte Nutzung von Speicherplattformen

# Warum nicht einfach Nearline-Storage und Backup-Server kombinieren?

Das Backup läuft in aller Regel in den Nachtstunden ab – Zugriff auf den Datei-Server ist tagsüber am allerwichtigsten. Was hindert uns daran, einmal darüber nachzudenken, Nearline-Storage und Backup-Server in einem System zu kombinieren? Erreichen wir da nicht eine deutlich bessere Auslastung vorhandener Hardware und senken Anschaffungs- und Betriebskosten?

Albrecht Hestermann,
actidata Storage Systems

Es versteht sich von selbst, dass jeder Administrator in die Luft geht, wenn die Marketing-Abteilung die 27. Vorversion des neuen Produktkataloges auf dem zentralen Fibre-Channel-Speichersystem ablegt. Letztlich muss jedoch den Mitarbeitern der Marketing-Abteilung zugutegehalten werden, dass diese in aller Regel ja gar nicht wissen, wo sie etwas abspeichern. Was zählt ist vielmehr, dass es morgen noch da ist – ein Dilemma, dem sich auch heute noch viele Administratoren ausgesetzt sehen, obwohl genau das der Ursprung der so genannten unstrukturierten Daten ist. Wurden nicht bereits im Vorfeld Maßnahmen ergriffen, sind die 27 Versionen wohl auch noch in zehn Jahren auf dem zentralen Storage-System vorhanden. Genau hier setzt das Konzept des Nearline-Storage an, denn oftmals reicht für die sichere Speicherung von Benutzerdaten ein einfacher File-Service aus, der über einen Server oder ein NAS-System realisiert wird.

## Nachts Backup und tagsüber aktive NAS-Nutzung

Die Ausnutzung der vollen Leistungsfähigkeit einer IT ist als Ziel zur Erreichung einer optimalen Systemeffizienz unumgänglich. Bekannterweise laufen die Datensicherungsaufträge in aller Regel in den Nachtstunden ab, da hier eben die geringste Belastung der Server und Infrastruktur besteht. Backup-Server, sei es beim Datentransfer auf Disks oder bei der Sicherung auf Tapes, laufen in dieser Zeit mit der höchsten Last. Tagsüber dagegen ist die Auslastung eher gering. Genau hier können durch Änderungen im IT-Konzept freie Ressourcen für andere Services genutzt werden.

Es bietet sich an, die Backup-Server mit Aufgaben eines einfachen File-Servers zu erweitern und vorhandene NAS-Funktionen zu nutzen. Hierdurch erhalten Benutzer günstigen Speicherplatz als Nearline-Storage, denn durch die Planung zusätzlicher Festplatten in einem eigenen RAID-Set lässt sich das einfach und effizient realisieren. Selbstverständlich müssen auch diesen Daten gesichert werden, was dann noch den netten Nebeneffekt hat, dass diese Datensicherung sehr performant direkt im Backup-Server abläuft und somit eine Belastung des LANs entfällt.

## System der Einstiegsklasse vs. skalierbare Lösung

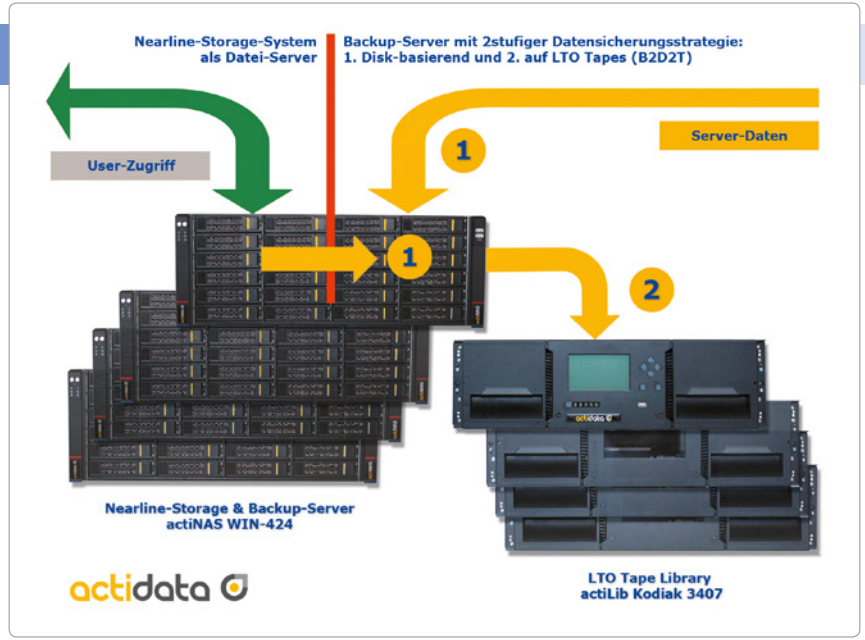
Dies ist vielleicht eine der wichtigsten Fragen bei Anschaffung eines sekundären Speichersystems. Eine allgemeingültige Antwort gibt es nicht, denn jede IT-Struktur ist typisch mit einem Unternehmen gewachsen, hat sich über Jahre hinweg bewährt und ist etabliert. Einzig gemeinsam ist die Tatsache, dass Speicherplatz für die Datei-Ablage als Nearline-Storage sowie die Disk-basierende Datensicherung vorhanden sein muss. Der Bedarf für das Nearline-Storage ist in aller Regel durch das Nutzerverhalten quasi vorgegeben.

Die Abschätzung der nötigen Kapazitätsgrößen für das Disk-basierende Backup kann jedoch von einer Tagessicherung, über eine 5-Tage-Sicherung bis hin zum Großvater-Vater-Sohn-Prinzip variieren. Hier kann der Kapazitätsbedarf also schnell das fünf- bis 20-fache des aktuell belegten Speicherplatzes erreichen – je nachdem, welche Datensicherungsstrategie definiert ist. Gepaart mit der Vorgabe der zusätzlichen Datensicherung auf auswechselbare

Medien (2-stufiges Backup B2D2T mit Tape als Offline-Datensicherung) ergibt sich ein Gesamtbild, so dass die Entscheidung zugunsten eines kompakten, kombinierten NAS- und Backup-System der Einstiegsklasse (z.B. *actiNAS XL 2U-8 RDX*) oder zu einer leistungsstärkeren Storage-Plattform bestehend aus einem 2U- oder 4U-Storage- und Backup-Server (z.B. *actiNAS WIN 212*) mit angeschlossener LTO-Tape-Automation (z.B. *actiLib Kodiak 3407*) ausfällt.

## Datenauslagerung – ist das heute noch wichtig?

Ein klares Ja! Auch wenn die Auslagerung unternehmenskritischer Daten in die Wolke als verlockend zu bezeichnen ist, sprechen doch nach wie vor fehlende Bandbreiten und/oder offene Fragen rund um Datenverschlüsselung und RZ-Standorte dagegen. Oft wird vergessen, dass ein Download-Stream in aller Regel eine deutlich geringere Bitrate liefert – was besonders in der Datenrekonstruktion ein großes Manko darstellt. Deshalb vertrauen viele mittelständische Anwender nach wie vor auf Lösungen, die im direkten und damit schnellen Zugriff liegen. Das hier für ein schnelles Restore die letzte Disk-basierende Datensicherung online zur Verfügung stehen sollte, versteht sich von selbst. Aber was nützt ein Disk-basierendes Backup, wenn ein Verschlüsselungstrojaner die Daten der NAS-Freigaben unwiederbringbar verschlüsselt hat oder gar ein Feuer- oder Wasserschaden die gesamte IT lahmlegte? Die Wichtigkeit unternehmenskritischer Daten sollte Vorständen und Geschäftsführern bekannt sein, die zur Sicherung des Fortbestandes eines Unternehmens die verantwortlichen Administratoren unterstützen müssen und die regelmäßige Auslagerung der Daten an einen sicheren Ort anweisen sollten.




Grafik: actidata

Kombinierte Nearline-Storage und Backup-Struktur mit actiNAS WIN und actiLib LTO Tape Library.

## Erweiterbarkeit von Nearline- & Backup-Storage ist wichtig

Heutige Systeme, beispielsweise der NAS- und Backup-Server *actiNAS WIN*, lassen sich über die externe SAS-Schnittstelle mit professionellen JBODs (Just a Bunch of Disks) erweitern. Besonders wichtig ist hier, dass die Erweiterungseinheiten auch in das so genannte Enclosure-Management das Kopf-Systems eingebunden werden müssen. Hierdurch ist dann die Gehäuse-Überwachung und -Alarmierung sichergestellt.

Gleiches gilt auch für die LTO-Tape-Library, wobei z.B. die *actLib Kodiak 3407* als 3U-Basis-Modul mit weiteren 3U-Erweiterungsmodulen individuell und je nach Bedarf skaliert werden kann. Skalierbarkeit schützt zum einen die Investitionen, denn Erweiterungen sind günstiger in der Anschaffung, als Neu-Systeme. Auch abschreibungstechnisch spricht vieles für die Erweiterungsoptionen, denn Nearline-Storage- und Backup-Systeme werden in aller Regel auf fünf Jahre, im Gegensatz zu drei Jahren bei der zentralen IT, geplant.

## Fazit – Versuch einer Empfehlung

Jede IT-Umgebung hat eigene besondere Merkmale, die sich im Laufe der Jahre bei jedem Unternehmen etabliert haben. Eine Systemempfehlung, die überall einfach einzusetzen ist, wird es nicht geben. Hier ist es wichtig, dass Anbieter eine maßgeschneiderte, auf die jeweiligen Bedürfnisse zugeschnittene Lösung projektieren und zusammen mit den Hard- und Software-Services anbieten. Genau hier setzen die Spezialisten der **actidata** aus Dortmund an, die zusammen mit ausgesuchten Partnern die aktuelle Situation rund um Nearline-Storage und Datensicherung beleuchten und Lösungen passend zu Anforderungen und Budgets ausarbeiten. ■

**Weitere Informationen**

**actidata Storage Systems GmbH**
Wulfshofstr. 16
44149 Dortmund
Tel.: +49 (0) 231/ 96 36 32 – 0
E-Mail: info@actidata.com
**www.actidata.com**

RDX für flexible Einsatzbereiche der Datensicherung

# Regelmäßiges Backup **ist nicht ausreichend**

Eine Datensicherung gewährleistet im Idealfall schnellen Zugriff auf Offline-Daten, bietet ein Backup für schnelle Wiederherstellung sowie Archivierung zur Einhaltung gesetzlicher Vorschriften. Wechseldatenträger sind dabei ein »Muss«. RDX von Tandberg Data stellt dabei eine effiziente Alternative zu Bandlaufwerken dar.


Foto: Tandberg Data

RDX-Wechsel-Medien mit bis zu fünf TByte.

Hugo Bergmann, Tandberg Data

Die gesetzlich von Unternehmen geforderte Konformität zu DSGVO, SEC17a-4(f), SOX, GoBD, StgB, Basel III usw. sowie die Ausbreitung von Schad-Software wie Ransomware verschaffen dem häufig vernachlässigten Thema Datensicherung neue Prominenz. Dabei sind Backup und Archivierung zwar unterschiedliche Aufgaben, sollten aber auf einer gemeinsamen Technologie aufsetzen, um Insellösungen zu vermeiden.

Eine Faustregel für die Datensicherung ist, mindestens eine Kopie des Backups auf einem Wechseldatenträger an einem zweiten Standort vorzuhalten, um ein durchgängiges Disaster-Recovery-Konzept zu implementieren. Wechseldatenträger wie *RDX* (Removable Disk Technology) sind aufgrund geringer Betriebskosten eine Option für beide Anwendungsfälle.

## Medienrotation und Archivierung mit einem System

RDX-Medien kombinieren die Portabilität und Zuverlässigkeit des Bandes mit der Geschwindigkeit einer Festplatte. Sie sind für eine Lebensdauer von mehr als zehn Jahren konzipiert und vollständig rückwärtskompatibel, bieten einen Datendurchsatz von bis zu 1,2 TByte/h und Speicherkapazitäten von bis zu fünf TByte pro Wechselmedium. Sie eignen sich zur Medienrotation ebenso wie für die Archivierung, sowie zum schnellen lokalen Zugriff über das Dateisystem ohne aufwendige Wiederherstellungsprozeduren.

Zur Anwendung kommen sie in Einzellaufwerken wie dem *RDX QuikStor* oder in Appliances wie der *RDX QuikStation* mit vier bzw. acht Laufwerken in einem Chassis. Kompatibel sind die Systeme mit gängiger Backup-Software ebenso wie mit *Windows Backup*, *Apple Time Machine*, auch *VMware*-Bordmittel werden unterstützt. Damit ist RDX für eine effektive Backup-Strategie mit Medienrotation ebenso geeignet wie für die Archivierung.

## Revisionssichere Archivierung mit WORM-Medien

Neben dem reinen Schutz vor Datenverlust muss die Backup-Strategie die Einhaltung gesetzlicher Vorschriften gewährleisten. Beispielsweise müssen in Enterprise-Content-Management- (ECM) und Dokument-Management-Systemen (DMS) Dokumente unveränderbar über mehrere Jahre aufbewahrt werden.

Im medizinischen Bereich unterliegen Patientenakten mit Untersuchungsdaten und Röntgenbilder einer gesetzlichen Aufbewahrungspflicht. Abrechnungsdaten von Praxen und Kliniken müssen bis zu vier Jahre aufbewahrt werden.

Gemäß der DSGVO müssen auch Dokumentationen, Planungsdaten oder Prüfungsunterlagen sein. Im Falle eines Ereignisses müssen Einträge und Informationen gesichtet und nachvollzogen werden, die als Beweismittel vor Gericht Verwendung finden können. Darüber hinaus sind alle Unternehmen gezwungen, steuerrelevante Daten und Buchhaltungsdaten bis zu zehn Jahre revisionssicher für die Betriebsprüfung vorzuhalten.

Dazu ermöglicht der Einsatz eines speziellen *RDX WORM*-Mediums (Write Once Read Many) zusammen mit der *rdxLock WORM*-Software die revisionssichere Archivierung von Geschäftsdaten nach HGB, GDPdU, GoBS, SOX und weiteren gesetzlichen Vorschriften, nach denen Dokumente unveränderbar gespeichert werden müssen. Tandbergs RDX-WORM-Medien lassen sich als revisionssichere Archivmedien für unterschiedlichste Anwendungen einsetzen, sind kompatibel mit allen RDX-QuikStor-Laufwerken und RDX-QuikStation-Disk-Appliances und transparent für Archivanwendungen.

## Schutz vor Ransomware mit rdxLOCK RansomBlock

Ransomware hat sich zu einer großen Gefahr in der Cyberkriminalität für Unternehmen jeder Größe entwickelt. Eine funktionierende Backup-Strategie ist äußerst wichtig und ist primärer Schutz der Geschäftsdaten gegen Viren, Würmer und Ransomware-Angriffe. Allerdings sind Backups ebenso gefährdet. Sobald ein Ransomware-Angriff ein Unternehmen erreicht hat, verbreitet er sich durch das gesamte Netzwerk und befällt Backup-Dateien, die auf anderen Computern und NAS-Systemen abgelegt werden.

Die rdxLOCK-RansomBlock-Funktion setzt zunächst alle Daten auf dem RDX-WORM-Medium in den »Nur Lese«-Modus. Zusätzlich erlaubt sie Schreib-Operationen für auswählbare Anwendungen und Prozesse, ähnlich einer Firewall. Somit können Backup-Anwendungen das RDX-WORM-Medium als ein reguläres Backup-Ziel nutzen.

RansomBlock überprüft ständig alle Schreiboperationen auf das RDX-Medium und vergleicht sie mit der Liste zugelassener und abgelehnter Anwendungen und Prozesse. Im Fall eines Virus oder Ransomware-Angriffs sperrt RansomBlock den Zugriff und schützt somit die Daten auf dem RDX-Medium vor einer Infizierung.

## Backup virtueller Umgebungen

RDX-Lösungen lassen sich in nahezu allen Systemumgebungen einsetzen und sind für die Sicherung von virtualisierten VMware-Maschinen für Veeam zertifiziert. Veeam Backup & Replication bietet eine schnelle, flexible und zuverlässige Wiederherstellung von virtualisierten Anwendungen und Daten. Die Software unterstützt die gesamte virtuelle Infrastruktur mit Features wie Instant Recovery auf Dateiebene, optimierte VM Recovery, Skalierbarkeit, 2-in-1-Backup-&-Replikation, eingebaute De-Duplizierung, zentrales Management und vieles mehr.

Durch das Zusammenspiel von Hard- und Software kann RDX als Wechseldatenträger adressiert werden, um Policys festzulegen, Wiederherstellungspunkte zu setzen und Medienrotationsschemata für die Online-/Offsite-Sicherung zu definieren. Für große Backup-Sets bietet QuikStation logische Volume-Konfigurationen, die mehrere RDX-Laufwerke zu einem Volume zusammenfassen.

## Optimal für KMU

Das RDX-QuikStor-Wechseldatenträger-System von **Tandberg Data** ist ideal für kleine und mittelständische Umgebungen und ermöglicht eine einfache Sicherung und Notfallwiederherstellung mit Medienrotation. In Kombination mit der Backup-Software *Veeam* eignet es sich insbesondere für Datenauslagerung und Datentransport in virtualisierte Umgebungen.

Für Unternehmen, die ihr bestehendes LTO-Bandautomatisierungsgerät ersetzen, aber weiterhin gewohnte Datenmanagement-Verfahren nutzen möchten, kann die RDX QuikStation 8 auch als Virtual-Tape-Library integriert werden oder im Hybrid-Modus mit einer Kombination als Einzellaufwerk und Tape-Emulation in einem Gerät genutzt werden. ■

**Weitere Informationen**

**Tandberg Data GmbH**
Feldstrasse 81, 44141 Dortmund
Tel. 00 49 (0)231/54 36-110
**www.tandbergdata.com/de/**

Bänder als Offline-Medium und gegen Ransomware

# Tape lebt, wächst und gedeiht

Der Tape-Markt erlebt eine regelrechte Renaissance. Unternehmen und IT-Abteilungen sehen Ransomware und Hackerangriffe als ernsthafte Bedrohung und vertrauen nun wieder verstärkt auf das Band. Auch wenn die Disk-Fraktion es immer gerne anders darstellt, Tape lebt, wächst und gedeiht. Als Offline-Medium und zu Archivierungszwecken sind Bänder auch weiterhin unverzichtbar.

Karl Fröhlich

Zugegeben Tape erinnert immer ein wenig an die frühen Tage des IT-Zeitalters. Nicht zuletzt durch Film und Fernsehen, haben wir Bilder mit Räumen im Kopf, voller großer Schränke mit überdimensionalen Spulen. Moderne Bandspeicher sind aber kein übriggebliebenes Relikt aus dem IT-Steinzeitalter. Die neue LTO-8-Generation bringt unkomprimiert zwölf TByte auf einer handtellergroßen, kompakten Cartridge unter.

In den letzten Jahren sah es so aus, als ob Disk als Sicherungs- und Archivierungsmedium komplett übernimmt. Festplatten bieten schnellere Datenraten und ein, auf den ersten Blick, gutes Preis-Leistungs-Verhältnis. Eine für Archiv-Zwecke ausgelegte Festplatte, wie beispielsweise die **Seagate** *Archive HDD v2 8TB,* kommt auf rund 25 Euro/TByte. Ein einzelnes LTO-7-Medium mit sechs TByte liegt bei zirka 11,66 Euro/TByte. Die entsprechenden Hersteller rechnen gerne Disk und Tape gegeneinander auf. Dies ist aber ein stückweit wie Äpfel mit Birnen zu vergleichen und je nachdem, welche Technologie der jeweilige Anbieter vertritt, gewichten sich die Vor- und Nachteile.

Fakt ist, die Disk ist aufgrund seiner besseren Performance das Backup-Medium Nummer eins. Anders lässt sich das Datenwachstum kaum bändigen und in das zur Verfügung stehende Backup-Zeitfenster pressen. Eine sinnvolle Datensicherungsstrategie sieht aber eine Kopie auf einem weiteren Medium vor – dies kann eine Festplatte oder Band sein – sowie eine extern aufbewahrte Kopie. Spätestens bei der Auslagerung der Sicherungen punktet Tape gegenüber den HDDs mit einer wesentlich besseren Energiebilanz und einem günstigeren Preis-Leistungs-Verhältnis.

## Offline-Medien schützen vor Ransomware & Co

Früher sollte ein sogenanntes Offline-Medium vor Datenverlust durch Feuer, Wasserschäden und Naturgewalten schützen. Vor allem kleine Unternehmen sahen hier oftmals keine Notwendigkeit für eine Investition. Seitdem Hackerangriffe und Ransomware zu einer ernsthaften und greifbaren Bedrohung geworden sind, erlebt Tape eine regelrechte Renaissance.

»Ransomware ist als größte Bedrohung für den Datenbestand seitens der Admins definiert worden«, erklärt **Albrecht Hestermann**, Leiter Vertrieb & Marketing bei **actidata Storage Systems**. »Datensicherung ist hier natürlich das A und O, wobei die Datenmengen und die damit verbundenen Kosten im Rahmen bleiben müssen. Es gibt bzw. gab eine Tendenz, sich bei der Datensicherung auf Disk-basierende Backups zu konzentrieren. Durch Ransomware und die Einführung von LTO-7 wurden wieder verstärkt Tape-Autoloader und -Librarys im Rahmen eines zweistufigen Backups eingesetzt.«

Hier setze laut Hestermann auch das neue LTO-7 Type M-Format mit neun TByte native an. Für eine regelmäßige Datensicherung, die beispielsweise über 14 Tage oder einen Monat gehe, sei das preisgünstige LTO-7-Medium (ca. 70 Euro/Cartridge) speziell für kleine und mittlere Unternehmen eine echte Alternative.

Dies sieht auch **Stefan Roth**, Head of Storage Business Central Europe bei **Fujitsu**, so. Er hatte auf einer Roadshow-Tour An-


Foto: Fujitsu

Mit Tape-Librarys lassen sich Backups mit Medienrotation, auch als Ransomware-Abwehr, sowie Archivlösungen umsetzen.

fang des Jahres dem vielbeschworenen Ableben von Tape eine Absage erteilt. Tape werde nicht vor der Disk sterben.

»LTO-8 bietet wieder komplett neue Möglichkeiten«, meint Roth. »Die Speicherkapazität hat sich erhöht, die Zugriffszeiten verkürzt und die Performance deutlich beschleunigt. Im Zuge der Datenmengen, die man auslagern und archivieren muss, gewinnt Tape wieder wesentlich an Aufmerksamkeit.«

## LTO-Roadmap bis Gen12

Im Q4/2017 hat das **LTO Consortium** eine neue Roadmap veröffentlicht, die nun bis zur 12. Generation (Gen12) reicht. Vermutlich um das Jahr 2030 herum sollen pro Cartridge 192 TByte (native) möglich sein. Mit einer Kompression von 2,5:1 sogar bis zu 480 TByte. Umgerechnet passen dann 16 LTO-8-Tapes auf ein Band. Zugegeben, dies klingt momentan schon noch nach Zukunftsvision. Allerdings, wenn wir heute zwölf Jahre zurückschauen: Ende 2006 wurden die Lizenzen für LTO-4 mit 800 GByte vergeben. Die unkomprimierte TByte-Grenze fiel 2009/2010 mit LTO-5 (1,5 TByte). Seitdem kommt alle zwei bis drei Jahre eine neue Generation auf den Markt.

Auch wenn Kritiker nimmermüde das Magnetband als aussterbendes Speichermedium sehen, Tape lebt. Als Offline-Medium und zu Archivierungszwecken sind Bänder unverzichtbar. ■

### Tandberg Quikstation

**Tandberg** *RDX QuikStation* ist eine automatisierte und skalierbare Library mit vier bzw. acht Laufwerksslots. Allerdings verwendet das System keine Tapes, sondern setzt auf Disk-basierte RDX-Wechselmedien. Diese sollen die Portabilität und Zuverlässigkeit des Bandes mit der Geschwindigkeit einer Festplatte kombinieren. RDX bietet einen Datendurchsatz von bis zu 1,2 TByte/h und Kapazitäten von bis zu fünf TByte pro Wechselmedium. Das 1U flache 4-Slot-Modell ist bereits ab zirka 1.650 Euro erhältlich, die 8-Slot-Variante ab rund 3.300 Euro. Die Medienpreise bewegen sich zwischen rund 90 (500 GByte) und 600 Euro (5 TByte).
Mehr Infos über die Quikstation-Serie »

### Fujitsu Eternus LT

**Fujitsu**s *ETERNUS LT*-Serie bietet eine Backup-Lösung für nahezu jede Unternehmensgröße. Die Bandbibliotheken beginnen bei 1U flachen 8-Slot-Autoloadern (*LT20 S2*) für automatische Backup- und Archivoperationen. Flexibel skalieren können IT-Abteilungen mit den 2U- bzw. 4U-Librarys (LT40 S2/LT60 S2), die mit 24 bzw. 48 Slots eine Kapazität von bis 360 bzw. 720 TByte erreichen. Mit dem »Pay as you grow«-Konzept bezahlen Kunden nur, was tatsächlich im Moment für das geplante Wachstum benötigt wird. Je nach Modell und Ausstattung beginnen die Preise bei rund 5.000 Euro.
Mehr Infos über die Eternus-Serie »

### Actidata Kodiak 3407

Der skalierbare Bandroboter *actiLib Kodiak 3407* von **Actidata** richtet sich an kleine und mittlere Unternehmen und eignet sich sowohl für Backup-Strategien, als auch zur Archivierung. Im Basis-Modul 3407-BTL ist Platz für drei LTO-Laufwerke, die sich auch im Mix-Betrieb einsetzen lassen. Mit 32 LTO-Slots in zwei herausnehmbaren Magazinen sind mit LTO-6-Medien unkomprimiert 80 TByte möglich, mit LTO-7 eine Kapazität von 192 TByte und mit LTO-8 bis zu 384 TByte. Mit zusätzlichen Erweiterungsmodulen 3407-ETL lassen sich je nach Format 100, 240 bzw. 480 TByte (native) hinzufügen. Der Preis beginnt bei 6.804 Euro (LTO-6).
Mehr Infos über den Kodiak 3407 »

### Qualstar Q8

Als Einstiegsgerät für Büros und kleine Firmen lässt sich der 1U-Autoloader *Q8* von **Qualstar** mit acht Bandkassetten bestücken. Dafür stehen zwei vierer Magazine zur Verfügung. Die Library unterstützt LTO-8 und verarbeitet LTO-7-Medien nach dem »LTO-7 Type M«-Format. Insgesamt deckt das Backup- und Archiv-System damit 72 bis 96 TByte ab.
Die Datenrate soll bei 300 MByte/s bzw. 10,8 GByte/h liegen. Die Tape-Librarys der Q-Serie lassen sich mit SAS- oder Fibre-Channel-Schnittstellen bestücken. Der Q8 wird vom in Kirchheim/Teck ansässigen Storage Distributor Starline ab 3.720 Euro netto angeboten.
Mehr Infos über den Q8 »

Nur eine Generation abwärtskompatibel

# LTO-8: Doppelte Kapazität und etwas mehr Speed

Das Tape-Segment hat ein neues Flaggschiff: Seit Oktober 2017 ist mit LTO-8 der neueste Bandstandard auf dem Markt. Gegenüber der Vorgängergeneration hat sich die unkomprimierte Speicherkapazität auf zwölf TByte verdoppelt. Die Performance hat sich von LTO-7 mit 300 MByte/s auf 360 MByte/s nur wenig verbessert.


Foto: IBM

LTO-8 bietet unkomprimiert einen Speicherplatz von zwölf TByte und schafft eine Backup-Rate von bis zu 1,296 TByte/h.

Karl Fröhlich

Nicht zuletzt durch *LTO-8* kommt wieder Leben in den Tape-Markt. Das Bandformat bietet eine native Kapazität von zwölf TByte und bis zu 30 TByte mit 2,5:1-Kompression. Auf einer Kassette ist das schon eine brauchbare Menge. Die Datenrate beträgt unkomprimiert bis zu 360 MByte/s bzw. 750 MByte/s mit 2,5:1-Kompression. Dies ist allerdings weniger als in der 2015 veröffentlichten Roadmap vorhergesagt. Hier wurde komprimiert noch von 32 TByte und maximal 1.180 MByte/s gesprochen. LTO-8 kommt nun auf eine Backup-Rate von bis zu 1,296 TByte/h. Die Verbesserung gegenüber LTO-7 (1,08 TByte/h) ist eher minimal.

LTO-8 unterstützt weiterhin eine Hardware-Verschlüsselung (AES-256-Bit), Datenpartitionierung sowie WORM-Funktionen (Write-Once Read-Many). Auch LTFS (Linear Tape Filesystem) ist möglich, damit lassen sich die Tapes wie ein Block-Device ansprechen.

Für Unmut sorgt, dass LTO-8-Bandlaufwerke nur zu bisherigen LTO-Cartridges der Generation 7 abwärtskompatibel sind. In vielen IT-Abteilungen ist es gängige Praxis, eine Tape-Generation zu überspringen. LTO-9 soll wieder die letzte und vorletzte Generation verarbeiten. Nachdem LTO-8 gerade erst auf den Markt gekommen ist, ist es müßig darüber zu diskutieren, wann LTO-9 kommen könnte. Unkomprimiert wird die nächste Generation 24 TByte auf einem Band unterbringen, vermutlich ab 2021.

## LTO-8 schafft mit LTO-7 Type M neun TByte

Ein interessanter Aspekt, der für LTO-8 spricht: LTO-8-Bandlaufwerke können neun TByte auf einer neuen, unbenutzten LTO-7-Kassette speichern, anstelle der eigentlichen sechs TByte gemäß dem LTO-7-Format. Dieses Format wird seit Mitte Februar 2018 als LTO-7 Type M bezeichnet. Ursprünglich wurde hier von LTO-M8 gesprochen. Auf den Barcode-Etiketten sollen die letzten zwei Zeichen auf M8 enden.

Eine normale LTO-7-Kassette wird als LTO-7 Typ A bezeichnet, hat eine Kapazität von sechs TByte und ist mit einem Barcode-Etikett mit der Endung »L7« gekennzeichnet. Eine LTO-8-Kassette mit zwölf TByte Kapazität hört auf dem Barcode auf die Endung »L8«.

Zu beachten ist, LTO-7-Medien müssen unbenutzt sein, um sie als Type M zu initialisieren. Einmal als Type M initialisiert, lässt sie sich nicht mehr als 6-TByte-LTO-7-Kassette verwenden. Außerdem kann eine LTO-7-Type-M-Kassette nur in einem LTO-8-Laufwerk verarbeitet werden. LTO-7-Laufwerke verarbeiten keine LTO-7-Medien vom Typ M. ■

3-2-1-Backup-Regel darf kein Bremsklotz und möglicher Kostentreiber sein

# **Backup als Mehrwert sehen** und nicht nur als Kostentreiber

Stetiges Wachstum an Daten und Systemen, unter anderem durch die digitale Transformation, fordert nicht nur die Erweiterung der IT-Infrastruktur in Bezug auf Datenspeicherung, sondern auch neue Ansätze bei der Datensicherung und -wiederherstellung. Es gilt nicht nur die Zeitfenster für Backup-Prozesse weiter zu verkürzen, sondern vor allem festgelegte Recovery-Ziele bestmöglich einzuhalten und dabei innerhalb des vorgegebenen Budgets zu bleiben. Wir sprachen hierzu mit Rainer Kalthoff, Sales Engineer Central & Eastern Europe bei Unitrends.

**Rainer Kalthoff,** Unitrends:

»Backup wird oft nur als kostentreibender Faktor angesehen und nicht als der Mehrwert, den er bei vernünftiger Planung und Umsetzung bringen kann.«

**Nicht zuletzt durch die Cloud scheint das Backup immer komplexer zu werden. Trügt dieser Eindruck?**

**Kalthoff:** Das kommt stark darauf an, wie Unternehmen die Cloud verwenden. Dem Administrator bietet die Cloud zwei grundlegend verschiedene Ansätze in Bezug auf das Backup, bei denen das Thema Backup sowohl komplexer als auch einfacher sein kann.

Im ersten Fall gibt es Workloads innerhalb der Cloud, die gesichert werden müssen. Verschiebung von lokalen Workloads oder Arbeitsprozessen in die Cloud kann dem Nutzer die Arbeit einfacher machen, kann Material und Kosten sparen und auch für den Administrator Zeit für die Betreuung der Applikation einsparen.

Auf der anderen Seite ergeben sich für den Administrator neue Probleme, auch gerade in Bezug auf die DSGVO. Was viele gerne verdrängen ist, dass durch die Verlagerung in die Cloud nicht der Zwang zur ordentlichen Sicherung der dort vorhandenen Daten entfällt. Natürlich werden die Cloud-Daten durch die jeweiligen Anbieter so gut wie möglich gegen Systemausfälle abgesichert. In den allermeisten Fällen bezieht sich der Cloud-Vertrag aber nur auf die Verfügbarkeit der aktuellen Daten. Die Vermeidung von Datenverlust durch Fehler von Benutzern, durch fehlerhafte Software, durch Angriffe von Hackern oder durch Ransomware fällt weiterhin in den Bereich des Kunden.

Erschwerend kommt hinzu, dass für die meisten Cloud-Dienste klassische Sicherungskonzepte gar nicht vorgesehen sind. Beim Betrieb virtueller Maschinen in der Cloud ist es zum Beispiel in den meisten Fällen nicht oder nur sehr schwer möglich zur Verwaltung direkt auf den Cloud-Hypervisor zuzugreifen. Die meisten VMs in der Cloud verhalten sich bezüglich Wartung als ob lokal ein physischer Server zu betreuen wäre. Dazu sind sie dann meist nicht einmal so flexibel wie ein physischer Server, weil der Nutzer keine vollständige Kontrolle über den Boot-Prozess erhält.

Wir bietet hier für viele Cloud-Dienste Abhilfe, auch schon für den Umstieg von On-Premises zu Cloud. Mit unserem Tool Boomerang kann der Administrator lokale *Vmware*-Workloads schnell und einfach zu *AWS* oder *Microsoft Azure* kopieren oder migrieren. Auch Cloud-Bursting ist möglich.

Dabei wird die VM lokal für ein Projekt vorbereitet und danach in die Cloud transferiert. Dort wird sie auf die benötigten und lokal nicht vorhandenen Ressourcen vergrößert und erledigt ihre Arbeit. Nach Abschluss des Projekts kümmert sich Boomerang automatisch um die Verkleinerung und den Rücktransfer.

*Unitrends Backup* ermöglicht Ihnen ein ordentliches Backup Ihrer Workloads in Azure sowie Amazon Web Services. Die Sicherung erfolgt über Agenten im Betriebssystem. Die gesicherten Daten können Sie bei Bedarf in eine andere Cloud oder in die lokale Infrastruktur replizieren.

Für SaaS-Anwendungen decken wir mit Spanning-Backup nicht nur die Sicherung von *Office 365* mit E-Mail, *SharePoint* und *OneDrive* ab, sondern in Kürze auch Ihre Daten in *Google GSuite* sowie *SalesForce*.

Beim zweiten Ansatz für den Administrator wird die Cloud als Ziel für die Ablage von Off-Site-Backups verwendet. Wir bieten genau dies mit der Hardware-Appliance *Recovery Series* sowie der Software-Appliance *Unitrends Backup*. Sie haben die Möglichkeit lokaler Datensicherung nahezu aller Computing-Ressourcen in Verbindung mit einer speziell entwickelten Cloud-Lösung für die Langzeit-Ablage von Sicherungsdaten außer Haus, inklusive verschiedener DRaaS-Optionen.

**Was sind aus Ihrer Sicht die Problemherde bei der Datensicherung in kleinen und mittleren Unternehmen? Und wie sollten KMUs diesen begegnen?**

**Kalthoff:** Aus der Sicht des Herstellers von Backup- und Recovery-Lösungen gibt es einige, immer wieder auftretende Probleme, gerade in kleinen und mittleren Unternehmensgrößen. Es fängt schon damit an, dass jahrzehntelang in Verwendung befindliche Lösungen trotz mittlerweile umfassender Änderungen der eigenen Infrastruktur nicht auf den Prüfstand kommen. Backup wird häufig, trotz der durch die DSGVO bevorstehenden Notwendigkeiten, oft nur als kostentreibender Faktor angesehen und nicht als der Mehrwert, den es bei vernünftiger Planung und Umsetzung bringen kann.

In Bezug auf die Nutzung der Cloud treffen wir nicht nur auf unflexible Ansichten (»Ich will meine Daten nicht aus der Hand geben«), allgemeines Desinteresse oder Verdrängung (»Hatte noch kein(e) Zeit/Gelegenheit/Interesse mir Gedanken dazu zu machen«), sondern immer wieder auch auf Bedenken bezüglich der verfügbaren Bandbreite, die bei realistischer Betrachtung in vielen Fällen gar kein so großes Problem ist.

Gerade im KMU-Bereich wäre deshalb eine planvollere Herangehensweise an das Thema Backup und Recovery dringend angebracht. Verantwortliche sollten einen Schritt zurück treten und sich von den Zwängen des bekannten Instrumentariums lösen. Sie sollten ihre Anwendungen, Abläufe und dadurch entstehenden Daten betrachten und diese nach Wichtigkeit kategorisieren. Dann sollten sie sich überlegen, was bei einem Verlust dieser Daten passieren würde und daraus Zeitspannen für Toleranzen bei Datenverlust und Ausfallzeit (RPO/RTO) ableiten.

Erst jetzt sollten sie objektiv die technischen und finanziellen Möglichkeiten betrachten, mit welchen die gewünschten RPO/RTO umgesetzt werden könnten. In vielen Fällen erweist sich dann nämlich die seit langem blind eingesetzte Lösung (Soft- und Hardware) als dafür untauglich oder zu teuer.

Aktuell verhalten sich viele Verantwortliche wie ein Holzarbeiter im Wald, der sich darüber beklagt dass er mit seiner stumpfen Axt nicht genug Bäume pro Tag schafft und wegen des dadurch entstandenen Drucks und Überstunden nicht dazu kommt seine Axt zu schärfen.

**Hat die 3-2-1-Backup-Regel in Zeiten stetig wachsender Datenvolumen heute noch Gültigkeit? Wie sollte eine moderne Datensicherungsstrategie aussehen?**

**Kalthoff:** Wie bereits oben angemerkt ist auch die 3-2-1-Backup-Regel bei stumpfem Befolgen dieser Regel mit aufgesetzten Scheuklappen ein Bremsklotz und möglicher Kostentreiber. Für eine moderne Strategie benötigt der Verantwortliche eine andere Perspektive.

Beim ersten Schritt in dieser neuen Perspektive sollte es sich um die Business-Continuity handeln. Provokativ ausgedrückt brauchen Unternehmen kein Backup, sondern eine funktionierende Wiederherstellung, innerhalb von definierten Parametern. Bevor diese Parameter nicht ausgearbeitet wurden, kann die Datensicherungsstrategie nicht vollständig erfolgreich sein.

Stellt man als Verantwortlicher dann fest, dass die ideale Strategie nicht vorhandene Ressourcen (zweiter Standort, neuere Hard- und Software) fordert, sollte man immer die Cloud mit in die Rechnung aufnehmen. Hier machen viele Verantwortliche den Fehler von »der Cloud« zu sprechen. Die eine Cloud, passend für jeden, gibt es aber nicht. Es genügt nicht die üblichen Verdächtigen einzubeziehen (Hyperscale Cloud von Azure, AWS...). Sie sollten auch über Cloud-Angebote von MSPs, CSPs oder SSPs nachdenken oder herstellerbasierte Continuity-Clouds, wie die Unitrends-Cloud, auf Kosten und Nutzen prüfen. Stellt sich am Ende heraus, dass 3-2-1 die für Sie genau richtige Lösung ist, dann setzen Sie sie um. In den meisten Fällen wird es jedoch sinnvoller sein, die »1« über einen Service zu erfüllen.

**Wie sehen Sie die Cloud als ausgelagertes Backup-Medium? Ist die Cloud wirklich eine Alternative zu Tape?**

**Kalthoff:** Fast alle Firmen benötigen für die Datensicherung eine Langzeit-Aufbewahrung, die früher fast ausschließlich mit Bändern umgesetzt wurde. Bänder haben im On-Premises-Bereich starke Konkurrenz von Festplattensystemen erhalten, sind bei der physischen Off-Site-Lagerung jedoch immer noch meist das Mittel der Wahl.

Nutzt eine Firma die Cloud für die Langzeit-Aufbewahrung, geht es oft in erster Linie um die Vermeidung von fehleranfälligen manuellen Prozessen bei der Verwaltung von physischen Datenträgern zur Off-Site-Lagerung. Gegenüber diesen klassischen Methoden hat die Cloud heute eine Vielzahl an zusätzlichen Vorteilen zu bieten:

- Eine einfachere und vollständig automatisierte Bedienung.
- Bessere Wiederherstellungsbedingungen gegenüber Bändern, die plötzlich ausfallen können.
- Einfache Möglichkeit zu skalieren, wenn der Speicherbedarf zunimmt.
- Die Möglichkeit Backups auch in der Cloud zu testen.
- Die Möglichkeit der Einbindung von Disaster-Recovery-as-a-Service (DRaaS), um bei einem Ausfall des lokalen Standorts über die Cloud weiter arbeiten zu können.

Wir bieten genau dies mit unserer Hardware-Appliance Recovery-Series sowie der Software-Appliance Unitrends-Backup. Sie haben die Möglichkeit lokaler Datensicherung nahezu aller Computing-Ressourcen in Verbindung mit einer speziell entwickelten Cloud-Lösung für die Langzeit-Ablage von Sicherungsdaten außer Haus. Dazu kommen verschiedenen DRaaS-Optionen für manuelle und automatisierte DR-Tests bis auf Anwendungsebene sowie mögliches Failover und Failback mit Hilfe der Cloud.

**Bisher scheint die Skepsis zu überwiegen. Wie sehen Sie hier die Entwicklung?**

**Kalthoff:** In den meisten Fällen ist die Skepsis gegenüber der Cloud unbegründet und entsteht in überraschend vielen Fällen durch Unwissen, Halbwissen oder gar Ignoranz. Der Einstieg in die Cloud geschieht immer öfter durch Office 365. Viele aufstrebende Firmen haben auch geografisch sehr verteilt arbeitende Angestellte, die über die Cloud einfacher im Team zusammen arbeiten können als über eine lokale Infrastruktur im Hauptquartier. Ist der Nutzer erst einmal erfolgreich mit einem Teil seiner Daten in der Cloud, fallen auch leichter die Wiederstände gegen die Cloud als Ablage von Backup-Daten.

Wir bieten hier mit der hybriden Cloud (lokale Sicherung und Aufbewahrung der Daten mit der Cloud als Absicherung dieser Daten außer Haus) genau das, was viele Verantwortliche benötigen. Es spricht wenig dagegen SaaS, PaaS, IaaS oder DRaaS von verschiedenen Anbietern zu beziehen. Die parallele Verwendung von verschiedenen Cloud-Providern, je nach Anwendungsgebiet wie Hyperscale-Clouds für Business-Anwendungen und Continuity-Clouds für das Datensicherungskonzept, wird in Zukunft häufiger vorkommen. Auch wenn eine Multi-Cloud-Lösung möglicherweise etwas höhere Kosten verursacht, zieht der Verantwortliche den höheren Nutzen aus der Spezialisierung der jeweiligen Cloud-Anbieter. Er kann für jedes Szenario den für ihn besten Service bekommen, was für einen einzelnen Anbieter gar nicht zu leisten ist. ■

Newsletter-Abonnenten erhalten die neue Ausgabe jeweils »linkfrisch« an ihren Mail-Account. Registrieren Sie sich bitte hier.
Beachten Sie auch unser Archiv im Download-Bereich.

**storage-magazin.de**
eine Publikation von speicherguide.de GbR
Karl Fröhlich, Ulrike Rieß
Ginsterweg 12, 81377 München
Tel. +49 (0) 89-740 03 99
E-Mail: redaktion@speicherguide.de

**Chefredaktion, Konzept:**
Karl Fröhlich (verantwortlich für den redaktionellen Inhalt)
Tel. 089-740 03 99
E-Mail: redaktion@speicherguide.de

**Redaktion:**
Karl Fröhlich

**Schlussredaktion:**
Brigitte Scholz

**Layout/Grafik:**
Uwe Klenner, Layout und Gestaltung,
Rittsteiger Str. 104, 94036 Passau,
Tel. 08 51-9 86 24 15
www.layout-und-gestaltung.de

**Titelbild:**
speicherguide.de

**Mediaberatung:**
Claudia Hesse,
Tel. +41 (0) 41 - 780 04 86
E-Mail: media@speicherguide.de

**Webkonzeption und Technik:**
Günther Schmidlehner
E-Mail: webmaster@speicherguide.de



## Unser Team

**Karl Fröhlich**,
Chefredakteur
speicherguide.de

**Claudia Hesse**,
Mediaberatung
speicherguide.de

speicherguide.de
Das Storage-Magazin

Wir empfehlen zur vollständigen Funktionalität des eBooks »Acrobat Reader«, ab Version 9