

storage-magazin.de

powered by **it-daily.net**

Eine Publikation von ***speicherguide.de***

Einkaufsführer Backup

Bild: Dall-E (KI)

2024

02

Marktübersicht Backup-Software & Tape-Librarys

Editorial

DATENSICHERHEIT VS. WACHSTUM, KOSTEN UND KOMPLEXITÄT



Karl Fröhlich
Chefredakteur
speicherguide.de

Liebe Leserinnen und Leser,

im Vorfeld zu dieser Ausgabe befragte mich (zufällig) eine Unternehmensberatung zum Markt für Archivierung und Backup. Ich habe natürlich gleich interveniert, das wären zwei komplett getrennte Märkte. Sagen wir es so, man hat mir geduldig zugehört, andere Experten hätten den Rat erteilt, Archivierung und Backup zusammen zu betrachten. Nun mag es für diese spezielle Marktanalyse möglicherweise sinnvoll sein, in der Praxis sehe ich das nicht.

Eine gute Datenmanagement-Strategie berücksichtigt beides, unter Beachtung der unterschiedlichen Zwecke. Das Backup soll einen Datenverlust vermeiden und dient der Wiederherstellung von Daten. Möglichst sicher und zügig, ungeachtet der Ursache des Katastrophenfalls. Während das Backup vor allem für aktive Daten zuständig ist, kümmert sich das Archiv um Daten, die nicht mehr regelmäßig oder gar nicht mehr benötigt werden.

Die Grundanforderung des Marktes ist die Sicherheit der Daten zu gewährleisten. Ransomware und Cyberattacken sind das offensichtliche Hauptproblem, dem sich alle Unternehmen, ungeachtet ihrer Größe stellen müssen. Die generellen Grundprobleme lauten aber Datenwachstum, steigende Komplexität und Kosten. Das Wachstum ist kaum aufzuhalten, muss aber verwaltet werden. In Kombination mit der Cybersicherheit wird die Infrastruktur zwangsläufig

komplexer. In den seltensten Fällen steigen die finanziellen Mittel im gleichen Maße, dementsprechend müssen sich alle Faktoren den Kosten unterordnen.

Ein Punkt, warum auch Tape wieder ins Rampenlicht gerückt ist. Magnetbänder gelten als günstig, in der Anschaffung (Preis/TByte) und weil sie im Ruhezustand keine Energie verbrauchen. Freilich gibt's hier auch andere Lösungen und Bandroboter gibt es nicht umsonst. Trotzdem ist Tape wieder en vogue, mehr denn je. Wie wir hören, wurden letzten Jahr so viele Tape-Librarys verkauft wie nie zuvor. Als Schutz vor Cyberkriminellen müssen Backup-Sets physikalisch vom Netz getrennt und ausgelagert an einem sicheren Standort aufbewahrt werden. Dazu benötigen wir mobile Speichermedien, die sich aus den Backup-Systemen herausnehmen lassen. Auch ein Punkt, warum Backup und Archiv zwar ähnlich aber eben nicht das Gleiche sind.

In diesem Storage-Magazin haben wir die Trends, Produkte und Lösungen im Backup-Markt für Sie zusammengefasst.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Bild: shutterstock / chayanuphol



SEITE
5

Datensicherung mit maximaler Cyber-Resilienz

SCHNELLES RECOVERY FÜR UNTERNEHMEN LEBENSNOTWENDIG

Backup und Recovery ist nicht mehr das profane Sichern von Dateikopien und dem Rücksichern einzelner Files. Heute geht es um eine schnelle Betriebswiederherstellung. Zu groß ist die Bedrohung, dass eine Cyberattacke das ganze Unternehmen lahmlegt. Die Datensicherung muss dem gerecht werden.

Marktübersicht Tape-Librarys

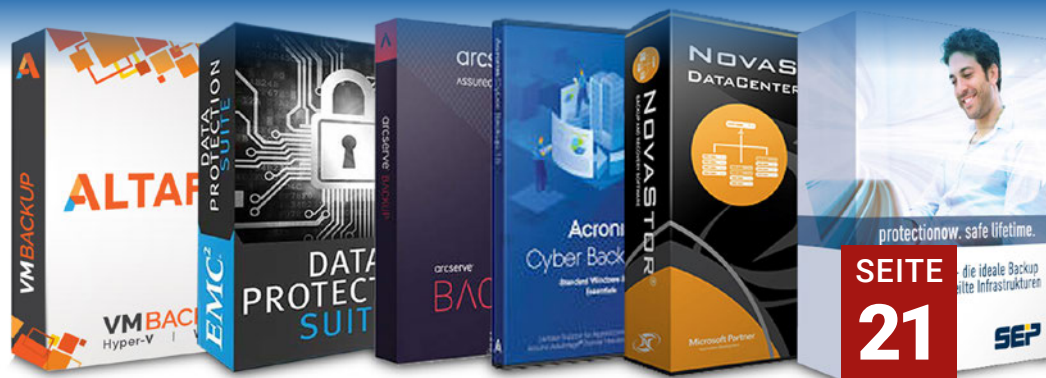
AUTOMATISCHE UND SKALIERBARE BACKUPS



SEITE
16

Bild: Overland Tandberg

MARKTÜBERBLICK BACKUP-SOFTWARE



SEITE
21

Collage: speicherguide.de und die jeweiligen Hersteller

Das Angebot an Backup-Software für Mittelstands- und Enterprise-Umgebungen ist über die Jahre beachtlich gewachsen. IT-Manager haben die Wahl zwischen Spezialisten und umfangreichen Plattform-Produkten, die zunehmend als Abomodell zu erwerben sind.

Übersicht Storage-Anbieter



SEITE
15

Editorial	2
Datensicherung	
Schnelles Recovery für Unternehmen lebensnotwendig	5
Advertorial	
Die 5 wichtigsten Kriterien für Backup-Storage	8
Datensicherung	
Ransom-Abwehr: Offsite-Backup & Air-Gap	10
Immutable-Storage: Unveränderliche Datenintegrität	13
Service	
Anbieterübersicht	15
Datensicherung	
Marktübersicht Tape-Librarys	16
Marktübersicht Backup-Software	21
Unersetzlich: Die 3-2-2-1-Backup-Regel	28
Service	
Impressum	29

Sicheres Backup als Schutz vor den Folgen von Ransomware Attacken

Ein Angriff durch Ransomware ist für ein Unternehmen immer eine Katastrophe. Allein das Schützen des Netzwerk vor weiteren Angriffen erfordert oft viele Tage. Ist dann auch noch das Backup der Unternehmensdaten von der Attacke betroffen, kann das den Ruin bedeuten.

Den besten Schutz des Backups bieten natürlich nach wie vor **ausgelagerte LTO-Kassetten**, da hier jede Art von Remote-Zugriff zu 100% ausgeschlossen werden kann. Auch bei Libraries sollten die Kanister mit dem Backup am besten entnommen werden.

Doch auch die Hersteller von **diskbasiertem Backup** haben einiges getan, den Zugriff auf die Datensicherungen zu verhindern. Minimum der Anforderungen ist, dass die Daten nur für die Backupsoftware selbst sichtbar sind. Das ist z.B. bei **Open-E JovianDSS** der Fall, wenn die Daten snapshotbasiert auf einen weiteren Rechner gesichert werden.



EonStor GS 1000 Gen2

Ebenso macht es mittlerweile auch **Infotrend** mit ihren **EonStor GS** Systemen. Hier kommt eine **Data-Lock** Funktion dazu, die Backup-Volumes unveränderlich macht.

Außerdem bietet Infotrend die






Möglichkeit, selbständig Backups zu ziehen, sowie **S3 Immutable Backupvolumes für Veeam** zur Verfügung zu stellen.

Sehr elegant hat das **ExaGrid** gelöst: Hier werden die Backups nach Auslagerung in eine **zweite Repository-Ebene** (mit Deduplikation

auch über viele Knoten) gesichert. Dort können sie mit einer einstellbaren **Retention Time** vor jeder Veränderung geschützt werden. Bei **Veeam**, der idealen Software für die Sicherung virtueller Maschinen, lässt sich ein Linux Server zum **Hardened Linux Immutable Repository** machen, das nur von der Software direkt erreicht werden kann und ebenso durch Retention Zeiten geschützt wird.

Backuplösungen mit Schutz vor Ransomware bei EUROstor:

(mehr Info unter www.EUROstor.com/backup.)

- **LTO Tape Libraries von Actidata**
Schutz der Daten durch räumliche Auslagerung 
- **Veeam Backup Server**
Zweit-Sicherung der Virtuellen Maschinen in ein Immutable Repository (s. rechts) 
- **ExaGrid Tiered Backup Storage**
Backups mit Retention in einer zweiten Backupenebene 
- **Infotrend EonStor GS**
Volumecopy mit Schreibschutz durch Data-Lock Funktion und als S3 Speicher für Veeam Repository 
- **Open-E JovianDSS Storage**
snapshot basierte On-/Off-site Data Protection (ODP) auf zweiten Standort 



Alle Storage-Systeme aus einer Hand:

EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, Scale-Out Clustern und Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die

Virtualisierung. Dazu kommen RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches.

Rufen Sie uns einfach an, wir beraten Sie gerne! Registrieren Sie sich auch für unseren Storage Newsletter (Print oder E-Mail, 3 x pro Jahr) unter www.EUROstor.com/Newsletter.



VEEAM AMD EPYC



ES-3036 als Hardened Linux Immutable Repository mit 36 Slots (12 davon auf der Rückseite)

ES-3036, 36 3.5" Slots, z.B. teilbestückt mit **€ 12.483,10** (inkl. MwSt.) **€ 10.490,-** (exkl. MwSt.)
12 x 20 TB SATA Enterprise HDDs,
2 x 512 GB M.2 Boot-SSD für das Betriebssystem

Hardened Linux Backup Repository Server:

- Storage-Server mit 36 3.5" Slots, bis 864 TB bei Verwendung von 24 TB Disks
- alternativ: 12/16/24 3.5" Slots, 24/72 2.5" Slots
- AMD EPYC Rome 7232P Prozessor, 8 Core, 3,1 GHz auf Supermicro H12SSL-NT Board, 7 PCIe 4.0 Slots
- 64 GB RAM, optional bis zu 1 TB
- 2 x 10 GbE (RJ45) onboard, opt. mehr und bis 100 GbE
- OS auf 512 GB NVMe M.2 SSDs im RAID 1, Ubuntu auf Wunsch vorinstalliert
- Areca RAID Controller mit 12 Gbit SAS, RAID Management über dedizierten Netzwerkport
- optional Erweiterungports für bis zu 512 Laufwerke
- Monitoring, remote Management und iKVM Console über Netzwerk (IPMI)
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt • Tel: +49 (0)711 70 70 91 70 • Fax: +49 (0)711 70 70 91 60

Preisänderung, Druckfehler und Irrtum vorbehalten.

Informieren und registrieren Sie sich auf unserer Website: www.EUROstor.com/Newsletter

E-Mail: Info@EUROstor.com - Tel.: +49 (0)711 70 70 91 70



Karl Fröhlich
speicherguide.de

Datensicherung mit maximaler Cyber-Resilienz

SCHNELLES RECOVERY FÜR UNTERNEHMEN LEBENSNOTWENDIG

Backup und Recovery ist nicht mehr das profane Sichern von Dateikopien und dem Rücksichern einzelner Files. Heute geht es um eine schnelle Betriebswiederherstellung. Zu groß ist die Bedrohung, dass eine Cyberattacke das ganze Unternehmen lahmlegt. Die Datensicherung muss dem gerecht werden.

Ransomware und Cyberkriminalität bleiben die Herausforderungen Nummer eins. Die Bedrohung durch Erpresser-Software und Malware steigt seit Jahren. Laut **Cybereason**-Report (Ransomware: Die wahren Kosten für deutsche Unternehmen 2024) waren 63 Prozent der befragten Unternehmen in Deutschland in den letzten 24 Monaten von mehr als einem Ransomware-Angriff betroffen. In diesem Zeitraum zahlten deutsche Firmen im Schnitt 762.000 US-Dollar Lösegeld. In den USA sind es 1,4 Millionen US-Dollar. Der Gesamtschaden liegt dagegen weit höher: 46 Prozent aller Befragten schätzen diesen auf ein bis zehn Millionen US-Dollar und 16 Prozent auf über zehn Millionen US-Dollar.

Mit dem Ransomware-Angriff einher kamen zudem Kosten für Rücktritte aus den Reihen des C-Level (33 %), Umsatzeinbußen durch vorübergehende Schließung des Unternehmens (32 %) und entgangene Gewinne (31 %). Hinzukommen Imageschäden und daraus resultierende Entlassungen.

Die Attacken zielen dabei vor allem auf Daten und Identitäten ab. Laut **Sophos** Threat-Report (Cybercrime on Main Street) sind kleine und mittlere Unternehmen weit öfter betroffen, als man es anhand der medialen Berichterstattung vermuten möchte. Ein Mangel an erfahrenem Sicherheitspersonal, unzureichende Investitionen in die Cybersicherheit und insgesamt

geringere Budgets für Informationstechnologie tragen zu dieser Verwundbarkeit bei. Wobei KMUs keine Kleinigkeit sind: Nach Angaben der **Weltbank** repräsentieren kleine und mittlere Organisationen mehr als 90 Prozent der weltweiten Unternehmen und stellen mehr als 50 Prozent der weltweiten Beschäftigung. Für Cyberkriminelle ist dies ein äußerst lukratives Segment.

Investments in Data-Protection unumgänglich

Wir weisen seit Jahren darauf hin, zu viele KMUs haben in manchen Bereichen noch Nachholbedarf. Wer nach dem Motto `uns passiert schon nix,

wir sind ja nicht interessant für Angreifer` agiert, riskiert viel. Noch immer haben rund die Hälfte aller deutscher Unternehmen keine echten Notfallpläne und bis zu 80 Prozent sagen von sich selber, dass sie sicherheitstechnisch nicht mit der Bedrohungslage mithalten können. »Das ist alarmierend«, bringt es **Hannes Heckel**, Leiter Marketing bei **FAST LTA**, auf den Punkt.

Kleine und mittlere Unternehmen (KMU) stehen vor der Aufgabe, eine Datensicherung so aufzusetzen, dass sie die maximale Cyber-Resilienz gewährleistet. »Die Datensicherung soll nach einem Desaster eine schnelle

Betriebswiederherstellung gewährleisten«, erklärt **NovaStor**-Geschäftsführer **Stefan Utzinger**. »Leicht gesagt, aber Fachkräftemangel, zu geringe Budgets, Überlastung und die fortschreitende Digitalisierung machen es den Verantwortlichen schwer.«


Bezüglich des aktuellen Geschäfts hören wir unterschiedliche Aussagen aus der Branche. Während die einen von guten Umsätzen sprechen, bezeichnen andere den Markt als zurückhaltend. Die Wahrheit liegt vermutlich in der Mitte. Generell sehen wir den Mittelstand eher in einer schwierigen Phase, viele haben Schwierigkeiten mit einer verlässlichen Planung, nicht nur bei Investitionen in die IT. Speziell bei Familienunternehmen steht jede Investition mehr als nur einmal auf dem Prüfstand. Der Trend: Sich auf das Notwendige beschränken, mit einer Tendenz zu kostengünstigeren Produkten. Systemhäuser, die mittelständische Kunden betreuen, sprechen durchaus über eine reale »Insolvenz- und Liquidationswelle«. In absehbarer Zeit dürfte der Markt nicht einfacher werden.

Datensicherung aus Recovery-Sicht betrachten





Für Fast-LTA-Manager Heckel ist das Zeitalter der Backups vorbei: »Der Fokus muss auf Recovery liegen, dabei erfordern unterschiedliche Datenklassen verschiedene Strategien und



Nach Statista-Schätzungen steigen die weltweiten Kosten der Cyberkriminalität in den nächsten vier Jahren sprunghaft an, von 9,22 Billionen US-Dollar im Jahr 2024 auf 13,82 Billionen Dollar im Jahr 2028.





Enterprise-Grade Storage Appliances

-  Hochverfügbar
-  Sicherheit
-  App Store
-  File, Block, Object
-  24/7 Support

„TrueNAS ist auf jeder Ebene ein Volltreffer - im Vertrieb, in der Technik und im Support.“

„Eine großartige Erfahrung mit einem neuen Backup-Server“

„Erstklassige Leistung und Wert für jeden Euro“

www.truenas.de



Albrecht Hestermann
Actidata

»Die Angst vor Ransomware ist nach wie vor der treibende Faktor für Data-Protection-Projekte.«

Technologien. Daten in irgendeinem Safe auf Tape nutzen nichts, wenn man schnell und wahlfrei darauf zugreifen muss, um den laufenden Betrieb zu sichern. Technologien, die nichts zur Recovery-Strategie beitragen, haben in Backups nichts mehr zu suchen.«

Wobei Magnetbänder und Tape-Automation nach wie vor fester Bestandteil einer Datensicherungsstrategie bleiben. Die Nachfrage steigt seit rund zwei Jahre kontinuierlich. »Ver-

stärkt wird nach Lösungen mit Einzel-Streamern gefragt«, sagt **Albrecht Hestermann**, Vertriebsleiter bei **actidata**. »Hier will man dem Anspruch gerecht werden, unternehmenswichtige Tage regelmäßig extern an einem sicheren Ort auszulagern.«

Hinzukommt, laut Hestermann, die Frage, wie geht der Admin mit den so genannten unstrukturierten Daten um. »Die Einteilung nach `cold` und `hot data` erscheint vielen zu einfach. Immer noch wird meist alles gesichert – was natürlich den Speicherbedarf wachsen lässt. Lösungen hierzu mö-



Hannes Heckel
Fast LTA

»Immutability soll die Folgen eines Cyberangriffs abschwächen, ist aber kein Allheilmittel.«

gen in einer Daten-Management-Software liegen, wobei das Thema von KMUs nicht wirklich angefasst wird. Budgets hierfür liegen in der Regel nicht bereit.«

Backup-Software: mehr Sicherheit & Unveränderlichkeit

In Folge wirkt sich der neue Fokus auf die Datensicherung auch auf das Geschäft mit Backup-Software aus. Die Jahre der Konsolidierung sind erst einmal vorbei. Gleichzeitig steigen die Anforderungen an die Backup-Lösung.

»Neben ausgeklügelten Backup Konzepten, die die Compliance-Anforderungen unterstützen und die Schutz gegen Ransomware bieten, sind auch die Immutable-Technologien wie SIS und Blocky4sesam zum Ransomware-Schutz der Backups sehr wichtig«, erklärt **Andreas Mayer**, Director Marketing bei **SEP**. »Hinzu kommt auch der *S3 Object Lock*, das heißt, die Immutability von S3 mit der Unveränderbarkeit der Daten mittels Lock-Retention (Vorgabe der Aufbewahrungsfrist).« Außerdem sei ein Restore-Virus-Check der Backup-Daten eine gute Möglichkeit mehr Sicherheit zu erreichen. Hier werden beim Restore die Daten noch einmal auf Viren überprüft. Sollte das Backup kompromittiert sein, werden infizierte Dateien gemeldet und lassen sich vom Restore ausschließen. Dies sei, laut Mayer, ein weiterer Sicherheitsvorteil,



Stefan Utzinger
Novastor

»Für einen optimalen Schutz, muss die Datensicherung die geschäftlichen und technischen Anforderungen abdecken.«

denn zum Zeitpunkt der Datenwiederherstellung sind meist mehr Virenpattern bekannt als zum Backup-Zeitpunkt.

Datensicherung ganzheitlich betrachtet

»Bei der Datensicherung geht es nicht mehr um die Sicherung einzelner Files«, mahnt Novastor-Chef Utzinger. »Im Vordergrund steht die schnelle Betriebswiederherstellung nach einem Disaster, wie einem Cyberangriff. IT-Verantwortliche stehen nicht vor der

Aufgabe, sämtliche Daten im Unternehmen einfach zu sichern. Vielmehr stehen sie vor der Herausforderung des Disaster-Recovery-Managements. Das heißt, sie müssen sicherstellen, dass die Organisation im Ernstfall schnellstmöglich wieder arbeitsfähig ist und die Daten wieder verfügbar sind.«

Gerade der Ansatz, ganzheitliche Lösungen aus der Applikationssicht zu denken, soll KMUs helfen, ihre IT schlank und effizient zu gestalten. Experten zufolge bedeuten Silo-Strukturen mehr Aufwand in der Organisation, im Management und in der Administration, und seien somit ein Kostentreiber. Ziel solle sein, dass Lösungen ganzheitlich alle Aspekte und bestimmte Anwendungen abdecken, um damit starre Strukturen aufzubrechen und IT-Managern letztendlich die Arbeit zu erleichtern. ■

Weiterführende Links:

- ➔ **Ransomware: Millionenschaden für deutsche Unternehmen**
- ➔ **Cybercrime: Daten von KMUs primäres Ziel**
- ➔ **Archivierung vs. Backup: Ähnlich und doch komplett anders**

Datensicherung ohne Kompromisse

DIE 5 WICHTIGSTEN KRITERIEN FÜR BACKUP-STORAGE

Datensicherung hat sich grundlegend gewandelt: Der Fokus hat sich deutlich vom Backup zum Recovery verschoben. Grund dafür ist natürlich die ständig steigende Bedrohung durch Cyber-Attacken, insbesondere Ransomware.

Fragt man eine beliebige KI, was die wichtigsten Kriterien für die Auswahl eines geeigneten Speichersystems für Backup & Recovery sind, erscheinen wenig überraschend folgende Punkte:

1. Kapazität und Skalierbarkeit
2. Performance
3. Zuverlässigkeit und Ausfallsicherheit
4. Datensicherheit & Immutability
5. Kosten

Dabei befindet man sich immer im Spannungsfeld, das eine oder andere Kriterium zu optimieren, ohne zu viele Kompromisse in anderen Punkten eingehen zu müssen. Und natürlich schwanken die Anforderungen stark und müssen für ihren

speziellen Einsatz ausbalanciert werden.

Mit dem *Silent Brick*-System bietet **FAST LTA** eine Speicherlösung an, die speziell auf diese Anforderungen hin entwickelt und optimiert wurde. Dem System liegt das Prinzip zugrunde, die Speicherkapazität unabhängig vom Hauptsystem gestalten zu können. So stehen Speichermodule – Silent Bricks – in Versionen mit Flash und Festplatten, in verschiedenen Größen und sogar als Air-Gap-fähige Medien zur Verfügung.

Kapazität und Skalierbarkeit

Natürlich müssen moderne Speichersysteme mit den steigenden Kapazitätsanforderungen mitwachsen. Dabei muss beachtet werden, dass der Kapazitätsausbau unterschiedlich stark

zu Buche schlägt. Schnelle Flash-Speicher als Primary-Target kosten deutlich mehr als Air-Gap-Medien oder Archivkapazität. Neben der eigentlichen Skalierbarkeit hat also auch die Granularität Einfluss auf die Kosten. Die mögliche Ausbaugröße muss zum Budget passen.

Silent Bricks skalieren modular. Als Primary-Storage kommen Flash-basierte Silent Bricks zum Einsatz, für große Kapazitäten eignen sich eher solche mit Festplatten. Der Ausbau der Kapazität erfolgt einfach durch Hinzufügen weiterer Silent Bricks, unabhängig für jeden einzelnen Bereich.

Performance

Die Performance-Anforderungen haben sich mit dem verschobenen Fokus auf den Recovery-Teil der Datensiche-

rung deutlich erhöht. Zeitkritische Daten müssen so schnell wie irgend möglich wiederherstellbar sein, um die Ausfalllücke so kurz wie möglich zu halten. Aber auch Daten, bei denen ein Restore theoretisch länger dauern darf, bremst den Prozess des Recovery erheblich ab, vor allem, wenn Daten nicht im wahlfreien Zugriff sind und zunächst von Offline-Medien komplett umkopiert werden müssen.

Anders als Tape basieren Silent Bricks immer auf nicht-linearen Medien wie Flash oder Festplatten und bieten deshalb aus Prinzip jederzeit wahlfreien Zugriff. Selbst im Fall eines Air-Gaps verhält sich der Silent Brick nach dem erneuten Mount wie ein schnelles, nicht-lineares Medium. Aufwändiges Umkopieren entfällt deshalb.



Hannes Heckel
FAST LTA

Zuverlässigkeit und Ausfallsicherheit

Alle Maßnahmen nutzen aber natürlich nichts, wenn die Speicherlösungen nicht über Jahre hinweg zuverlässig ihren Dienst tun und geeignete Technologien zum Schutz gegen Ausfall vorweisen. Zur Zuverlässigkeit gehört auch, inwiefern man sich auf den oder die Hersteller verlassen kann, wie hoch der Wartungsaufwand ist, und ob über einen langen Zeitraum gesichert Ersatzteile zur Verfügung stehen.

Für Silent Bricks bietet FAST LTA mit CARE Wartungsverträge mit bis zu zehn Jahren Laufzeit an. Die Zuverlässigkeit der FAST LTA Langzeit-speicher ist legendär und durch die Kombination der Technologien zum Schutz vor Datenverlust durch Komponentenausfall begründet.

Datensicherheit und Immutability

Backups dienen ja genau dazu, Daten vor Verlust zu schützen. Da Angriffe inzwischen fast immer zunächst die Datensicherung im Visier haben, ist ein besonderer Schutz der gesicherten Daten essenziell. Hier hat sich in jüngster Vergangenheit das Prinzip der Immutability etabliert, bei dem Daten für bestimmte Zeiträume mit unterschiedlichen Technologien gegen Veränderung oder Löschen geschützt werden.

Im Silent Brick System vereinen wir gleich mehrere solcher Technologien,

inklusive der physischen Trennung der Speichermedien vom eigentlichen System: dem Air-Gap. Ebenso verfügbar: Software-unabhängige Immutability durch Continuous-Snapshots sowie die Unterstützung von Object-Locking im S3-Speicherbereich.

Kosten

Schließlich müssen sich alle Kriterien am Ende dem zur Verfügung stehenden Budget unterordnen. Auch deshalb ist die genaue Betrachtung der vorhandenen Daten, die Klassifizierung und die Bewertung nach RTO (Recovery Time Objective) und RPO (Reco-

very Point Objective) besonders wichtig. Nicht alle Datensätze erfordern schnelle, teure Flash-Medien. Es darf aber nicht nur der reine Preis pro TByte herangezogen werden. Kosten, die über die Zeit durch Wartung, Migration und auch Systemausfälle auftreten, können weit schwerer wiegen. Zu zurückhaltende Investitionen in die Datensicherung können sich insbesondere nach einem erfolgten Angriff rächen – und teuer zu stehen kommen.

Eine Möglichkeit, die Kosten für die Datensicherung von Anfang an zu reduzieren, ist die systematische Herausnahme geeigneter Daten. Unstruk-

turierte Daten, die sich kaum mehr verändern oder sogar automatisch erzeugt wurden, können durch eine Absicherung mittels eines sicheren WORM-Archivs aus dem Backup genommen werden, was Aufwand, Komplexität und Kosten erheblich reduziert.

Mit den *Silent Cubes* bietet FAST LTA seit über 15 Jahren einen WORM-Archivspeicher an, der speziell zum langfristigen Schutz unstrukturierter Daten entwickelt wurde. Silent Cubes und Silent Brick ergänzen sich ideal und sorgen für eine vereinfachte, hochsichere und auf Dauer kostengünstige Datensicherung. ■



Das Silent Brick System bietet Speichermedien für alle Anforderungen der modernen Datensicherung von Flash bis Air-Gap.

Weitere Informationen:

FAST LTA GmbH

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



Karl Fröhlich
speicherguide.de

Datensicherung bestmöglich vor Angriffen schützen

RANSOM-ABWEHR: **OFFSITE-BACKUP & AIR-GAP**

Backups sorgen dafür, dass ein IT-Katastrophenfall wie Hard- und Software-Defekte, menschliche Fehler oder ein Ransomware-Angriff keinen Datenverlust zur Folge haben. Dies gelingt aber nur, wenn auch die Sicherungen selbst bestmöglich geschützt sind. Ein Offsite-Backup mit Air-Gap ist daher Pflicht.

Bild via Quelle: Dall-E (KI)

Bedeutung und Wert einer umfassenden Backup-Strategie sind unbestritten. Immer wieder neu zu prüfen ist angesichts sich verändernder Rahmenbedingungen jedoch, wie diese Strategie aussehen sollte. Ransomware-Attacken haben die Notwendigkeit eines Medienbruchs bzw. Offsite-Backups wieder in den Vordergrund gerückt.

Ein gutes, aktuelles und vollständiges Backup an einem anderen Ort (*Offsite*), der nicht über das Netzwerk erreichbar und damit auch nicht darüber angreifbar ist (*Air-Gap*) und sinnvollerweise auf anderen Medien vorliegt, ist keine Option mehr, sondern Pflicht. Kritiker, die vor zwei, drei Jahren eine entsprechende Strategie noch als zu aufwändig und teuer abtaten, sind mehr oder weniger verstummt. Unangreifbare Backups sind für Unternehmen alternativlos.

Ransomware hat auch den Tape-Markt wiederbelebt. Jahrzehntlang wurde das Magnetband von den Festplattenherstellern und Branche-Größen wie EMC für tot erklärt. Ende der 2010er Jahre ging der Trend für Tape in Richtung Archivmedium. »Tape ist prädestiniert dafür um Offsite-Backups zu erstellen – also eine Kopie an einem anderen Standort«, erklärt **Ines Wolf**, Presales CE bei **Quantum**. »Dabei bleiben durch die Backup-Applikation alle Metadaten erhalten, es ist aber kein direkter Zugriff auf die Daten



Foto: Quantum

Ines Wolf
Quantum

»Tape ist prädestiniert dafür um Offsite-Backups zu erstellen.«

mehr möglich. Zusätzlich schätzten Kunden den Medienbruch, der Angreifern den Zugriff verwehrt.«

Wobei ein Air-Gap mit physikalischer und elektrischer Trennung nicht nur mit Tape möglich ist. Das Silent Brick-System von Fast LTA ist beispielsweise ein Wechselspeicher, bei dem sich Module mit zwölf Festplatten oder SSDs, die sich einfach per Hand austauschen lassen. **actidata-** hat mit dem Q-DX6 Ende letzten Jahres ein 5-Bay-NAS mit integrierter Wechselspeichereinheit herausgebracht, mit dem sich ebenfalls ein Air-Gap realisieren lässt.

Für und wider die 3-2-1-1-Backup-Regel

Die 3-2-1-Regel gilt als Standardstrategie. Experten plädieren dafür, mit 3-2-1-1-Backups noch einen Schritt weiterzugehen: Drei Sicherungskopien, zwei unterschiedliche Medientypen nutzen und idealerweise noch je eine Offsite- und eine Offline-Kopie bereitstellen. Damit haben IT-Manager die Möglichkeit, die Hardware-Funktionalitäten mit zu nutzen – also etwa eine Backup-Kopie zu erstellen, die für den Backup-Administrator nicht sichtbar ist und damit auf diesem Wege auch nicht angegriffen werden kann.

»Der Drei-Zwei-Eins-Eins-Ansatz ist sehr gut«, stimmt **Hannes Heckel**, Director Marketing bei **FAST LTA**, grundsätzlich zu. »Wir sehen aber, dass die Grenzen zwischen Backup und Archivierung sehr stark aufgelöst werden. Etwa durch NAS-Backup, wo sich angesichts der Datenmengen nicht mehr mit dem Drei-Zwei-Eins-Eins-Ansatz arbeiten lässt. Oder auch durch Backup-Archive auf Object-Stores, was schon in den Bereich der Archivierung hineingeht.« Für manche Abteilungen könne es daher sinnvoll sein, ein WORM-Medium (Write Once, Read Many) für bestimmte Aufgaben bereitzuhalten.

»Das klassische Backup – ein Server, der gesichert werden muss und von dessen Sicherung dann Kopien angelegt werden – gibt es so immer



Foto: Fast LTA

Hannes Heckel
FAST LTA

»Air-Gap ist auch über schnellere Medien realisierbar, und benötigt nicht unbedingt Tape.«

seltener«, skizziert Heckel die Entwicklung aus Sicht von Fast LTA. »Auch die Evolution der Backup-Software geht davon weg und dahin, dass immer weitere Bereiche umfasst und abgedeckt werden. Daher braucht man Systeme, die möglichst flexibel alle diese Aspekte abdecken. Air-Gap ist heute auch über schnellere Medien realisierbar, und benötigt nicht unbedingt Tape«. Genauso sei es beim Einsatz des Software-basierten Objektspeichers etwa mit Object-Lock.

Dieser bringt das Backup zusammen mit der Archivierung. Diese verlangt aber nicht nur Sicherung über Unbeschreibbarkeit, sondern eben auch eine beabsichtigte Löschung.

Datenverlust vermeiden

»Kleinere Unternehmen benötigen eine greifbare Lösung, die zu ihrem Kostenrahmen passen«, sagt Quantum-Managerin Wolf. »Um diese zu finden, sollten sie sich nicht direkt mit der Technik beschäftigen, sondern vielmehr folgende Fragen stellen: Wie schaffe ich es, eine zweite Kopie meiner Backup-Daten zu schreiben. Wo kann ich diese hinlegen und wie verwalte ich sie? Was mache ich lokal, was bei einem Dienstleister? Und wie komme ich wieder an die Daten ran, wenn etwas passiert? Wieviel Datenverlust kann ich mir leisten?«

Ein Backup-Konzept zu erstellen, das dann für 80 Prozent der Nutzer funktioniert, sei heute tatsächlich der falsche Ansatz, pflichtet Heckel bei. Vielmehr sei die individuelle Betrachtung wichtig, weil letztendlich die Nutzung darüber entscheide, was gebraucht werde. »Ich kann mir natürlich beliebig viele Offline-Kopien anlegen, aber die meisten Leute haben ja auch eine Beschränkung hinsichtlich der Kosten, des Aufwands und der Zeit«, sagt Heckel. Sein Fazit: »In den allermeisten Fällen gibt es mehr als einen Weg, der für den Kunden passend ist.«



Foto: Vitos Haina

Jörg Riether
Vitos Haina

»Erst eine Definition der Prozesse ermöglicht eine Backup-Strategie.«

Kaum jemand starte zudem bei null. Daher hänge die Antwort auf neue Herausforderungen wie sich ändernde Cyberattacken auch immer davon ab, was als Basis schon vorhanden ist.

»Was will ich eigentlich?« ist auch aus Sicht von **Volker Wester**, Geschäftsführer von **Cristie Data**, die entscheidende Frage, die sich Unternehmen stellen sollten. Um die zu beantworten, müssten sie die Anfor-

derungen ermitteln – vielleicht auch mit externer Hilfe. »Aus den Anforderungen heraus gilt es dann, ein Gesamtkonzept zu erstellen.« Pauschale Empfehlungen könne man eigentlich nicht mehr geben.

Dem schließt sich Wolf an: »Am besten kommt man voran, wenn man unterschiedliche Szenarien skizziert und deren Vor- und Nachteile abwägt.« Dazu empfiehlt die Quantum Managerin, dass sich Firmen unter anderem fragen: Wie es jetzt aussieht, wo sie hinmöchten, wo sie Schmerzen haben und was nicht läuft, ob Know-how fehlt und inwieweit sich Anforderungen geändert haben, seit das aktuelle Konzept entworfen wurde.

»Die Hersteller liegen eigentlich gar nicht so weit auseinander – wenn man es mit etwas Abstand betrachtet«, bilanziert **Jörg Riether**, Leiter IT-Verband bei **Vitos Haina**, auf einem von speicherguide.de organisierten Roundtable. Das Storage-Medium sei gar nicht entscheidend. »Wichtig ist vielmehr, für sich Prozesse zu definieren, die die Backup-Strategie erst möglich machen.« Gedanken über Skalierung, Datendurchsatz und Performance seien dann erst der zweite Schritt – und ohnehin in jedem Fall erforderlich. ■

Cyberkriminelle überall da tut Hilfe not

Who're you gonna call?

Securitybusters!

Mehr Infos dazu im Printmagazin

itsecurity

und online auf www.it-daily.net



Karl Fröhlich
speicherguide.de

Datenmanipulation unmöglich

IMMUTABLE-STORAGE: **UNVERÄNDERLICHE DATENINTEGRITÄT**

Bedrohungen wie Ransomware, Datenmanipulation und unbeabsichtigte Löschungen sind allgegenwärtig. Daher ist es notwendig, Daten in einem unveränderlichen Format zu speichern. Möglich ist dies mit Immutable-Storage-Systemen auf Basis von WORM-Medien oder S3 Object-Lock.

Bild via ChatGPT/DALL-E

Für Unternehmen und ihre digital gespeicherten Daten ist Cyberkriminalität eine ernste Bedrohung: Schätzungen von **Statista Market Insights** zufolge steigen die globalen Kosten durch Cyberkriminalität in den nächsten vier Jahren stark an, von 9,22 Billionen US-Dollar im Jahr 2024 auf 13,82 Billionen US-Dollar bis 2028. Selbst Skeptiker, die alles für übertrieben halten, können sich diesen Zahlen nicht verschließen. Lagen 2018 die Kosten noch unter einer Billion, waren es 2023 schon über acht Billionen US-Dollar.

Daher ist es unerlässlich für die Sicherheit und Unveränderlichkeit der digitalen Unternehmensdaten zu sorgen. Immutable-Storage ist hier ein wichtiger Baustein in der Datenspeicherungs- und Datensicherungsstrategie. Immutable-Storage bezeichnet eine Art von Datenspeicherung, bei der einmal geschriebene Daten nicht mehr geändert oder gelöscht werden können, zumindest für einen vorher festgelegten Zeitraum. Diese Eigenschaft gewährleistet die Unveränderlichkeit und Permanenz der Daten, was für die Einhaltung von Compliance-Richtlinien, die Verbesserung der Datensicherheit und die Gewährleistung einer genauen Datenspeicherung von entscheidender Bedeutung ist.

Die Funktionsweise von unveränderlichen Speichern lässt sich auf

unterschiedliche Arten erreichen.

- **WORM (Write Once, Read Many)**
- **Blockchain**
- **Object-Lock und Retention-Policy**

Die Vorteile von Immutable-Storage sind eindeutig: Durch die Unveränderlichkeit der Daten wird der Schutz vor Ransomware und Malware verbessert, da diese Bedrohungen die Daten nicht verschlüsseln oder verändern können. IT-Abteilungen erfüllen damit Compliance-Anforderungen und vereinfachen Audits, da die Datenhistorie klar und unveränderlich ist. Gleichzeitig garantiert es auch über längere Zeit die Integrität der Daten, was für Branchen, die auf genaue und unveränderte Daten angewiesen sind, unerlässlich ist.

Jedoch gibt es auch Nachteile und Limitationen:

- **Erhöhte Kosten:** Die Notwendigkeit zusätzlicher Speicherkapazität, um Duplikate und unveränderliche Daten zu speichern, sollte genau kalkuliert werden.
- **Verwaltungskomplexität:** Die Implementierung und Verwaltung von Immutable-Storage können durchaus komplex sein, vor allem in Umgebungen mit großen Datenmengen.
- **Performance-Einbußen:** In einigen Fällen beeinträchtigen die Unveränderlichkeitsanforderungen die Schreibgeschwindigkeit.

Unveränderbare Speicher mit S3 Object-Lock

So richtig populär wurden Immutability mit **Amazons S3 Object Lock**. Mittlerweile gilt Object-Lock als Industriestandard für die Unveränderbarkeit von Objektspeichern und kommt längst nicht mehr nur zusammen mit AWS zum Einsatz. Es blockiert die permanente Löschung von Objekten während eines vom IT-Manager definierten Aufbewahrungszeitraums.

Obwohl Object Locks als Funktion spezifisch für Objektspeichersysteme entwickelt wurden, ist das Konzept der Datenunveränderlichkeit nicht auf Objektspeicher beschränkt. Die Implementierung in anderen Speichersystemen hängt von den spezifischen Technologien, dem Systemdesign und den verfügbaren Tools ab. Jedes Speichersystem hat seine eigenen Methoden, um Unveränderlichkeit auf verschiedene Weise zu unterstützen, wobei Objektspeicher aufgrund ihrer architektonischen Vorteile und der Einfachheit der Anwendung von Richtlinien auf Objektebene oft die flexibelsten und leistungsfähigsten Lösungen bieten.

Immutability: Ein Risiko bleibt

Bei allen Vorteilen sind IT-Anwender trotzdem gut beraten, Immutable-Systeme skeptisch zu betrachten: »Auch ihnen liegt immer irgendein Betriebs-

system zugrunde«, mahnt **Jörg Riether**, Leiter IT-Verband bei **Vitos Haina**, auf einem von speicherguide.de organisierten Roundtable. »Damit haben sie genauso Bugs und Schwachstellen wie andere IT-Systeme. Selbst wenn sie die nicht haben, gibt es eventuell noch Low-Level-Interfaces auf die Systeme – insofern würde ich mich nie hundertprozentig darauf verlassen.« Seine Empfehlung lautet daher: »Immutable Storage – aber immer in Kombination mit komplett ausgelagerten Medien.« Bei denen spiele die Technologie – Tape, Disk NVME-SSDs oder optische Speichermedien – dann eine untergeordnete Rolle. »Hauptsache, sie sind elektronisch getrennt (Stichwort Air-Gap)«, betont Riether.

Seine Ansicht begründet Riether damit, dass die Anwendungsfälle heute anders als früher sind, als man auf ein Backup nur im Notfall zurückgegriffen hat. Heute könnten zum Beispiel Tausende von virtuellen Servern in einer Testumgebung laufen, um etwas zu simulieren und es würden viele Backup-Systeme auch im operativen Betrieb genutzt – und dafür seien eben Online-Datenspeicher ideal. ■

Weitere Informationen:

Lesen Sie den Artikel in einer detaillierteren Langfassung auf speicherguide.de

TrueNAS
ENTERPRISE

Enterprise-Grade Storage Appliances

- Hochverfügbar
- Sicherheit
- App Store
- File, Block, Object
- 24/7 Support

„TrueNAS ist auf jeder Ebene ein Volltreffer - im Vertrieb, in der Technik und im Support.“

„Eine großartige Erfahrung mit einem neuen Backup-Server“

„Erstklassige Leistung und Wert für jeden Euro“

Holstein IT-SOLUTIONS

www.truenas.de



EUROSTOR

www.eurostor.com



EUROstor ist ein europaweit tätiger Hersteller von Speichersystemen, insbesondere RAID Systemen und Storage Appliances mit Sitz in Filderstadt (bei Stuttgart). Geschäftsführer von EUROstor ist Franz Bochtler. Für die technische Leitung verantwortlich ist Wolfgang Bauer.

Wir entwickeln, fertigen und vertreiben europaweit hochwertige Datenspeichersysteme für den professionellen Einsatz und die spezifischen Anforderungen bei Unternehmen in der Großindustrie, dem Mittelstand sowie bei Forschung und Lehre. EUROstor vertreibt Produkte ausschließlich an gewerbliche Endkunden und Wiederverkäufer.

Sitz der Gesellschaft:
Filderstadt

Jahr der Gründung:
2004

Zielgruppe:
gewerbliche Endkunden und Wiederverkäufer



N-TEC GmbH

n-tec.eu

Sitz der Gesellschaft:
Ismaning

Jahr der Gründung:
2001

Zielgruppe:
Vor allem KMU + öffentliche Auftraggeber

N-TEC konzentriert sich auf universell einsetzbare und skalierbare Speicherlösungen für Unternehmen und setzt dabei auf sorgfältig ausgewählte, namhafte Hersteller. Im Fokus stehen Object Storage Lösungen für Private Clouds und Storage Systeme mit hoher Verfügbarkeit. Klassische Server, SAN und Unified Storage Systeme, sowie revisions sichere WORM Archive und Backup Lösungen runden die Produktpalette ab. Kunden erhalten bei N-TEC alles aus einer Hand – vom Pre Sales bis zum After Sales und langjährigen Support. N-TEC ist immer der zentrale Ansprechpartner für alle Belange.



Holstein IT-Solutions

truenas.de/



Holstein IT-Solutions aus Norddeutschland vereint kompetente IT-Experten unter seinem Dach. Das junge und motivierte Team unterstützt Behörden, Bildungseinrichtungen sowie mittelständische und große Unternehmen bei Infrastrukturprojekten von der Planung über die Umsetzung bis hin zum Betrieb. Die Stärken sind Enterprise-grade Storage-, Security-, Netzwerk- und Virtualisierungslösungen. Der IT-Systemspezialist setzt bevorzugt auf Open Source sowie offene Standards für mehr Kompatibilität und Investitionsschutz.

Sitz der Gesellschaft:
Hagen

Jahr der Gründung:
2015

Zielgruppe:
mittelständische Industrieunternehmen, Behörden, Bildungseinrichtungen, Gesundheitswesen, Energiesektor, Mediendienstleister



FAST LTA

www.fast-lta.de



Sitz der Gesellschaft:
München

Jahr der Gründung:
1999

Zielgruppe:
KMUs, VARs und Industriekunden

Wir sind die Spezialisten für Sekundärspeicher, für Archivierung und Backup.

Unsere Produkte und Services helfen mittelständischen Anwendern, Datensicherung und Datenmigration zu vereinfachen, rechtliche und regulatorische Risiken zu minimieren, und das langfristige Risiko, Daten zu verlieren, nachhaltig zu verringern.

Marktübersicht Tape-Librarys

AUTOMATISCHE UND SKALIERBARE BACKUPS

Mit der steigenden Zahl an Cyberangriffen kehrte auch das Leben in den Tape-Markt zurück. Ein gutes Preis-Leistungs-Verhältnis, ein geringer Energieverbrauch und der notwendige Medienbruch in der Backup-Strategie, inklusive Air-Gap, sprechen nach wie vor für den Einsatz von Magnetbändern. Richtig ausgewählt, ermöglichen sie ein bedarfsgerechtes Wachstum und schützen somit die getätigten Investitionen.



Karl Fröhlich
speicherguide.de

Bei Tape-Librarys hat sich in den letzten Jahren technologisch wenig getan, trotzdem sind Bandbibliotheken sehr angesagt. »Auch wenn es nicht viel Neues gab, haben wir wohl noch nie so viele Tape-Librarys verkauft wie im letzten Jahr«, bestätigt **Wolfgang Bauer**, Technischer Leiter bei **EUROstor**. »Wegen der hohen Kapazität von LTO-9 Kassetten sind es im Schnitt eher kleinere Librarys. Die Bänder werden dann meist zugriffssicher gelagert.« Daher gehe es in diesem Bereich auch nicht um irgendwelche tollen Zusatzfunktionen. Die Technik müsse »einfach nur« zuverlässig funktionieren.

»Tape-Speicher hat traditionell als Ressource für die langfristige Datenspeicherung und Archivierung gedient«, ergänzt **Natalie Kremer**, Global Product & Channel Marketing Mana-

ger bei **Overland Tandberg**. »Weitere Gründe, warum Tape heute attraktiver denn je ist, sind geringere Kosten pro GByte, geringerer Stromverbrauch und eine umweltfreundliche Speicherlösung. Diese Faktoren gewinnen mehr und mehr an Bedeutung, insbesondere in Ländern mit hohen Energiekosten (Strom).«

In Zeiten von Cyberangriffen und Ransomware-Attacken bieten Tape-Lösungen das so wichtige Feature Air-Gap: »Air-Gap erhöht die Datensicherheit massiv und macht Backups bzw. andere Datenbestände tatsächlich immun gegen Ransomware-Angriffe«, sagt Kremer. »Kaufentscheidungen für Tape-Librarys werden aktuell hauptsächlich im Hinblick auf Skalierbarkeit, Langlebigkeit mit entsprechenden Service-Leveln sowie Nachhaltigkeit getroffen.«



Bild: Overland Tandberg

Tape-Librarys in Modulbauweise erlauben ein flexibles Skalieren, zum Teil über komplette Rack-Schränke hinweg.

Dass die Tape-Technologie nicht innovativ ist, mag **Albrecht Hestermann**, Vertriebsleiter bei **actidata**, so nicht gelten lassen: »Nicht zuletzt steht hierfür die Datenaufzeichnung von 50 TByte, native auf IBM TS1160-Laufwerke. Diese nutzen hier Strontium-Ferit-Bänder, also eine neue Magnetbandtechnologie, die auch die Basis

für zukünftige LTO-Laufwerke in Tape-Librarys sein wird. Diese werden sich auch zukünftig in einer mehrstufigen Datensicherungsstrategie und auch in der Langzeitspeicherung großer Datenmengen (Archivierung) behaupten. Zumal eine Alternative zur kostengünstigen Speicherung großer Datenmengen bis dato nicht abzusehen ist.«

Die Einstiegsgröße für einen Bandroboter beginnt bei knapp 4.200 Euro (netto). Hierfür erhält man beispielsweise einen **actidata actiLib 1U LTO-Autoloader** mit einem LTO-7-Laufwerk und acht Slots im U1-Rackmount-Format. Mit LTO-8 kosten die Autoloader etwas mehr und mit LTO-9 ab zirka 4.520 Euro. Diese Kategorie gilt als Einstieg für kleine Unternehmen. Mit acht Bändern lässt sich eine unkomprimierte Speicherkapazität von 48 bis 144 TByte realisieren.

Ein größeres Datenwachstum erfordert dagegen skalierbare und flexibel ausbaubare Tape-Libraries. Hier bilden 2U-Geräte den Einstieg, die mit bis zu 24 Tape-Slots unkomprimiert eine Gesamtkapazität zwischen 144 TByte (LTO-7) und 432 TByte (LTO-9) bereitstellen. Die *NEOs T24*-Serie von **Overland-Tandberg** beginnt in der Anschaffung bei nicht ganz 5.000 bis 6.500 Euro.

Vorteile einer Tape-Library

Um Fehlerquellen möglichst auszuschließen, empfiehlt es sich den täglichen Sicherungsjob zu automatisieren. Bandroboter unterstützen hier und entlasten den IT-Beauftragten in KMUs und Abteilungen bei der täglichen Datensicherung.

Ein Roboter entnimmt die einzelnen Tapes automatisch, legt sie in den Streamer und befördert sie nach vollendetem Backup oder Restore wieder in den dafür vorgesehenen Aufbewahrungsort. Eine Backup-Software steuert den selbstständigen Wechsel der Datenträger. Entweder wird jeweils ein neues Band zur täglichen Sicherung eingelegt oder, falls die Kapazität nicht ausreicht, ein weiteres Tape. Zudem lässt sich so das Vergessen oder die falsche Auswahl eines Mediums vermeiden. Auch die ab und an notwendige Reinigung des Bandlaufwerks übernimmt das System automatisch. Neben der Automatisierung



Bild: Acldata

Bandroboter automatisieren nicht nur den Sicherungsjob, sondern bringen auch einen Medienbruch in die Backup-Strategie, inklusive Air-Gap.

des Backups finden Tape-Libraries auch für die dauerhafte Speicherung von Daten Verwendung.

Midrange- und Highend-Libraries mit hoher Skalierbarkeit

Vor rund zwei Jahren lagen LTO-7 und LTO-8 noch gleichauf, mittlerweile geht der Trend zu LTO-8 und LTO-9. Gekauft werden vor allem SAS-Tape-Library in 2U-Bauhöhe, oft mit zusätzlichen Magazinen. Die Admins entnehmen nicht nur Bänder, sondern verstärkt komplette Backup-Sets aus der IT und lagern diese extern.

Typischerweise fragen Käufer nach Tape-Libraries (3U) mit 40 Slots und LTO-8-Laufwerken an. Diese lassen sich bei allen Herstellern mit zusätzlichen Modulen weiter ausbauen und skalieren beispielsweise auf bis zu 280 Einschübe und 21 Streamer. Mit 80 Slots lassen sich mit LTO-8 in sechs Höheneinheiten fast 1 PByte darstellen. An der Ausstattung hat sich seit

Jahren wenig geändert: Im Midrange gehören eine SAS- oder Fibre-Channel-Schnittstelle zum Standard sowie ein Barcode-Leser und ein bis drei Mailslots, für die schnelle Ein- und Ausgabe von mehreren Cartridges. Die Ausbaufähigkeit, sprich zusätzlicher Slots in einem Modul, regeln die Hersteller über eine Software-Lizenz. Zudem erlauben die meisten Anbieter eine Verschlüsselung über das LTO-Laufwerk. Als Bandformat ist LTO-8 in der Regel die erste Wahl, 2016 war es noch LTO-6. Pro Cartridge lassen sich unkomprimiert 12 TByte unterbringen. Die native Datentransferrate wird mit 360 MByte/s angegeben. Langsam im Kommen sind auch Systeme mit LTO-9. Unkomprimiert passen 18 TByte auf ein Band. Die Datentransferraten liegen native bei bis zu 400 MByte/s.

Topklasse mit Hunderten von Tape-Slots

Wer mehr benötigt, kann beispielsweise mit der **Fujitsu LT270 S2** von 138 bis 713 Slots pro Rack skalieren. Mit LTO-8 sind native über 8,5 PByte möglich. Insgesamt lassen sich acht Racks zusammenschalten. Dies ergibt 67,73 PByte mit 5.644 Cartridges sowie bis zu 128 Laufwerke.

Die **Scalar i6000** von **Quantum** bietet im Vollausbau mit 20 Racks bis zu 12.006 Stellplätze mit maximal 216,1 PByte native und 192 Tape-Drives. ■

Air-Gap auch mit Disk-Speichern möglich

Tape gilt als das Offline-Medium schlechthin. Dass es auch anders geht, belegt **FAST LTA** mit seinen *Silent Brick*-Systemen. Diese bestehen aus Modulen, den sogenannten Bricks, die sich per Hand austauschen lassen. Die Sekundärspeicher unterstützen Air-Gap, WORM und Immutability.

Das Herz der Geräte bildet der Controller. Er nimmt im Rack drei Höheneinheiten ein und bietet fünf Slots für mobile Silent Bricks oder die stationären Silent Brick DS. Alternativ dazu kann der IT-Manager fünf Extension Shelves mit jeweils 14 Slots



Bild: Fast LTA

Das besondere an den Silent Brick-Systemen sind die mobilen Medien, mit denen sich auch Offline-Backups mit Air-Gap realisieren lassen.

anschließen. Der mit 3,5-Zoll-Festplatten bestückte *Silent Brick DS* bietet beispielsweise 48, 96 oder 240 TByte Bruttokapazität, die sich auch zu größeren Volumes kombinieren lassen. Für die Verbindung zum Netzwerk dienen zwei 10-GbE-Schnittstellen, als Variante für den Anschluss einer virtuellen Tape-Library (VTL) ist auch eine Ausführung mit zwei Fibre-Channel-Schnittstellen erhältlich.

In die Slots passen die Silent Bricks von Fast LTA. Es handelt sich dabei um Container, die jeweils zwölf Datenträger aufnehmen. Sie stecken in stabilen Aluminium-Gehäusen, die dank Griff und optionalem Transport-Case gut für mobile Anwendungen vorbereitet ist. Bei den Datenträgern hat der Kunde die Wahl zwischen Festplatten und SSDs. Die Laufwerke in einem Brick stammen immer aus verschiedenen Chargen, um die Wahrscheinlichkeit von Ausfällen aufgrund von Produktionsfehlern zu minimieren. Dank einer Konfiguration mit dualer oder Tripel-Parity (SecureNAS 2p/3p) oder, für einen Archivspeicher, mit vierfacher Redundanz mit Erasure-Coding und linearem Dateisystem (SecureNAS ERC oder VTL) entsteht auch beim Ausfall mehrerer Laufwerke kein Datenverlust.

Mit den Silent Bricks adressiert Fast LTA die Bereiche Sekundärspeicher und File-server-Storage, Backup und Archiv sowie Langzeitarchive (Cold-Storage). Die Wartungsverträge sind auf bis zu einer Dauer von bis zu zehn Jahren ausgelegt, inklusive Vor-Ort-Austausch und optionaler 24/7/365-Erreichbarkeit.

Der S3-kompatible Objektspeicher unterstützt zudem Object-Locking und -Retention. Damit lässt sich auch ein sogenannter Immutability-Schutz der Sekundärspeichersysteme umsetzen. Das kleinste Silent Brick mit einem Slot für Langzeitarchive beginnt bei unter 6.000 Euro netto.

MARKTÜBERSICHT TAPE LIBRARYS

Hersteller	Produktname	Bandformat	Max. Tape-Slots/ Basiseinheit	Tape-Drives	Max. Kapazität in TByte	Transferrate in TByte/h	Schnittstellen	Formfaktor (Rackmount)	Nettopreis (Euro)
Actidata www.actidata.com	actiLib 1U LTO-Autoloader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.170
	actiLib 1U LTO-Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.220
	actiLib 1U LTO-Autoloader	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.520
	actiLib 2U LTO Tape Library	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 4.790
	actiLib 2U LTO Tape Library	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.140
	actiLib 2U LTO Tape Library	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.800
	actiLib Kodiak 3407	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	EOL
	actiLib Kodiak 3407	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 7.560
	actiLib Kodiak 3407	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 8.455
	actiLib Kodiak 6807	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	EOL
	actiLib Kodiak 6807	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 11.195
	actiLib Kodiak 6807	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 11.965
Fujitsu www.fujitsu.com/de/	Eternus LT20 S2	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 4.300
	Eternus LT20 S2	LTO-8	8	1	96	1,1	SAS 6G, FC 8Gb	1U	ab 4.400
	Eternus LT140	LTO-7	20	1-3	120	22,7	SAS 6G, FC 8Gb	3U	ab 6.500
	Eternus LT140	LTO-8	20	1-3	240	22,7	SAS 6G, FC 8Gb	3U	ab 6.900
	Eternus LT260	LTO-7	80	1-6	480	45,4	SAS 6G, FC 8Gb	6U	ab 7.990
	Eternus LT260	LTO-8	80	1-6	960	45,4	SAS 6G, FC 8Gb	6U	ab 8.590
HPE www.hpe.com	StoreEver MSL 1/8 Tape Autoloader	LTO-6	8	1	20	0,6	SAS 6G/12G, FC 8Gb	1U	ab 3.000
	StoreEver MSL 1/8 Tape Autoloader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.469
	StoreEver MSL 1/8 Tape Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 5.500
	StoreEver MSL 1/8 Tape Autoloader	LTO-9	8	1	144	2,2	SAS 6G/12G, FC 8Gb	1U	ab 6.500
	StoreEver MSL2024	LTO-6	24	1-2	60	2,2	SAS 6G/12G, FC 8Gb	2U	ab 4.130
	StoreEver MSL2024	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 4.826
	StoreEver MSL2024	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.724
	StoreEver MSL2024	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 9.500
	StoreEver MSL3040	LTO-6	40	1-3	100	22,5	SAS 6G/12G, FC 8Gb	3U	ab 4.560
	StoreEver MSL3040	LTO-7	40	1-3	240	22,5	SAS 6G/12G, FC 8Gb	3U	ab 7.900
	StoreEver MSL3040	LTO-8	40	1-3	480	22,5	SAS 6G/12G, FC 8Gb	3U	ab 5.840
	StoreEver MSL3040	LTO-9	40	1-21	720	22,5	SAS 6G/12G, FC 8Gb	3U	ab 6.890
	StoreEver MSL6480	LTO-6	80	1-6	200	3,46	SAS 6G/12G, FC 8Gb	6U	ab 17.400
	StoreEver MSL6480	LTO-7	80	1-6	480	6,48	SAS 6G/12G, FC 8Gb	6U	ab 19.200
StoreEver MSL6480	LTO-8	80	1-6	960	6,48	SAS 6G/12G, FC 8Gb	6U	ab 25.600	
StoreEver MSL6480	LTO-9	80	1-6	1.440	6,48	SAS 6G/12G, FC 8Gb	6U	ab 28.270	
IBM www.ibm.com	TS2900	LTO-5	9	1	13,5	0,3	SAS 6G	1U	ab 6.800
	TS2900	LTO-6	9	1	22,5	0,6	SAS 6G	1U	ab 7.300
	TS2900	LTO-7	9	1	54	1,1	SAS 6G	1U	ab 7.400
	TS2900	LTO-8	9	1	108	1,1	SAS 6G	1U	ab 7.735
	TS2900	LTO-9	9	1	144	1,1	SAS 6G	1U	ab 8.300
	TS4300	LTO-6	40	1-3	100	0,6	SAS 6G, FC 8Gb	3U	ab 6.300
	TS4300	LTO-7	40	1-3	240	3	SAS 6G, FC 8Gb	3U	ab 6.990
	TS4300	LTO-8	40	1-3	480	3	SAS 6G, FC 8Gb	3U	ab 7.290
	TS4300	LTO-9	40	1-3	720	3	SAS 6G, FC 8Gb	3U	ab 16.800

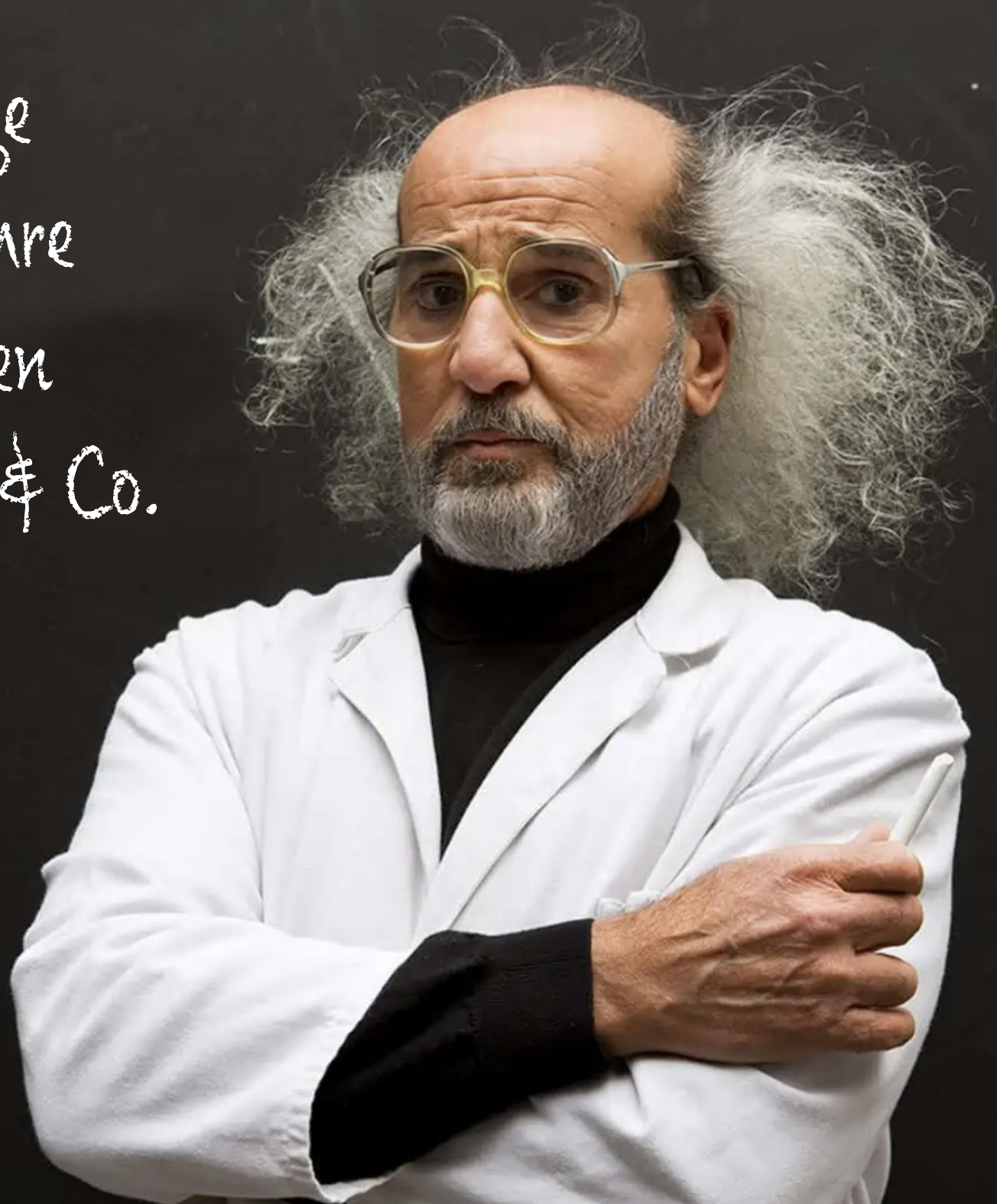
Hersteller	Produktname	Bandformat	Max. Tape-Slots/ Basiseinheit	Tape-Drives	Max. Kapazität in TByte	Transferrate in TByte/h	Schnittstellen	Formfaktor (Rackmount)	Nettopreis (Euro)
Oracle www.oracle.com/de/	StorageTek SL4000	LTO-7	339	1-24	2.000	24,7	FC, Ficon	42U	ab 129.000
	StorageTek SL4000	LTO-8	339	1-24	4.000	29,7	FC, Ficon	42U	k.A.
	StorageTek SL8500	LTO-7	2.000	64	12.000	65,9	FC, FCoE, Ficon	42U	ab 246.000
	StorageTek SL8500	LTO-8	2.000	64	24.000	82,9	FC, FCoE, Ficon	42U	k.A.
Overland-Tandberg www.overlandtandberg.com	NEOs StorageLoader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.910
	NEOs StorageLoader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.510
	NEOs StorageLoader	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 5.430
	NEOs T24	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.465
	NEOs T24	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.150
	NEOs T24	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 6.740
	NEOxl 40	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	ab 10.657
	NEOxl 40	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 10.876
	NEOxl 40	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 12.374
	NEOxl 80	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 19.695
	NEOxl 80	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 21.960
	NEOxl 80	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 24.595
Qualstar www.qualstar.com	Q8	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 5.100
	Q8	LTO-8	8	1	96	1,1	SAS 6G, FC 8Gb	1U	ab 5.970
	Q8	LTO-9	8	1	144	1,1	SAS 6G, FC 8Gb	1U	ab 7.400
	Q24	LTO-7	24	1-2	144	2,2	SAS 6G, FC 8Gb	2U	ab 4.430
	Q24	LTO-8	24	1-2	288	2,2	SAS 6G, FC 8Gb	2U	ab 7.720
	Q24	LTO-9	24	1-2	432	2,2	SAS 6G, FC 8Gb	2U	ab 7.810
	Q40	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	ab 5.830
	Q40	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 7.720
	Q40	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 10.200
	Q80	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 11.690
Q80	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 12.930	
Q80	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 14.520	
Quantum www.quantum.com	Scalar i3	LTO-7	25-400	1-24	150	0,54	SAS 6G/12G, FC 8Gb	3U-24U	ab 10.370
	Scalar i3	LTO-8	25-400	1-24	300	1,08	SAS 6G/12G, FC 8Gb	3U-24U	ab 11.600
	Scalar i3	LTO-9	25-400	1-24	450	1,62	SAS 6G/12G, FC 8Gb	3U-24U	ab 13.450
	Scalar i6	LTO-7	50-800	1-24	300	1,08	SAS 6G/12G, FC 8Gb	6U-48U	ab 16.600
	Scalar i6	LTO-8	50-800	1-24	600	2,16	SAS 6G/12G, FC 8Gb	6U-48U	ab 17.800
	Scalar i6	LTO-9	50-800	1-24	900	3,24	SAS 6G/12G, FC 8Gb	6U-48U	ab 23.200
	Scalar i6000	LTO-7	100-12k	1-192	600	2,16	SAS 6G/12G, FC 8Gb	Full Rack	ab 70.000
	Scalar i6000	LTO-8	100-12k	1-192	1.200	4,32	SAS 6G/12G, FC 8Gb	Full Rack	k.A.
Scalar i6000	LTO-9	100-12k	1-192	1.800	6,48	SAS 6G/12G, FC 8Gb	Full Rack	k.A.	
Spectra Logic spectralogic.com	Spectra T380	LTO-6	380	12	950	6.900	SAS 6G, FC 8Gb	24U	k.A.
	Spectra T380	LTO-7	380	12	3.400	13	SAS 6G, FC 8Gb	24U	k.A.
	Spectra T380	LTO-8	380	12	4.500	15,55	SAS 6G, FC 8Gb	24U	k.A.
	Spectra T380	LTO-9	380	12	6.800	17,28	SAS 6G, FC 8Gb	24U	k.A.
	Spectra T950	LTO-6	920	24	2.300	13,8	FC 8Gb	Full Rack	ab 8.100
	Spectra T950	LTO-7	920	24	8.280	25,92	FC 8Gb	Full Rack	ab 9.000
	Spectra T950	LTO-8	920	24	11.000	31,1	FC 8Gb	Full Rack	k.A.
	Spectra T950	LTO-9	920	24	16.500	34,56	FC 8Gb	Full Rack	k.A.

Quelle: speicherguide.de

Angaben: Kapazitäten und Performance-Werte unkomprimiert; k.A. = keine Angabe

Doc. tec. Storage
beantwortet alle Ihre
technischen Fragen
zu Storage, Backup & Co.

Stellen Sie Ihre Frage an:
DocStorage@speicherguide.de



Backup & Recovery für Mittelstand und Enterprise

MARKTÜBERBLICK **BACKUP-SOFTWARE**

Das Angebot an Backup-Software für Mittelstands- und Enterprise-Umgebungen ist über die Jahre beachtlich gewachsen. IT-Manager haben die Wahl zwischen Spezialisten und umfangreichen Plattform-Produkten, die zunehmend als Abomodell zu erwerben sind.



Michael Baumann
speicherguide.de

Das Backup gilt als »Last Line of Defense« für etwaige Katastrophen, die den digitalen Datenbestand bedrohen und die Backup-Software ist dabei die Schaltzentrale. Ziel ist es bei Bedarf, Daten zügig wiederherzustellen. Dabei steht heute die Sicherung gegen Ransomware-Attacken und andere Schad-Software im Mittelpunkt. Dazu müssen »Immutability« oder WORM-Funktionen (Write Once Read Many) an einem lokalen Standort und/oder in der Cloud verfügbar sein. Das leistet Backup-Software heute quasi durchgängig. Ebenso muss ein Medienbruch (Air-Gap) gewährleistet werden. Auch dies ist mittlerweile Standard, um 3-2-1-Strategien beim Backup umzusetzen.

Im Mittelstands- und Enterprise-Segment überzeugen manche Datensicherungs-Produkte durch universelle Leistungsvielfalt, andere sind eher

»Spezialisten«. Dennoch: Für uns sollte Backup-Software idealerweise eine breite Palette an Hosts, Anwendungen, Speichertechnologien und Datensicherungs-Strategien unterstützen. Die Software sollte modular aufgebaut, skalierbar und mit einer Vielzahl von Plattformen, Betriebssystemen, Tape-Libraries, Laufwerken und Topologien kompatibel sein. Auch Mobilität bzw. die Sicherung am Front-End rücken für RZ-Administratoren zunehmend in den Fokus.

Die Kosten sind schwer zu ermitteln. Lizenzen für ein Endgerät starten ab 50 Euro und erreichen schnell vierstellige Euro-Bereiche pro Server oder Host. Ebenso verbreitet wie Lizenzen sind Abo- und SaaS-Modelle (Software-as-a-Service), die je nach Service-Level stark divergieren. Viele Anbieter scheuen davor zurück, Preisangabe zu veröffentlichen. Die offizielle Be-

gründung lautet freilich, dass die Anforderungen der Unternehmen zu unterschiedlich sind. Das ist in der Regel Quatsch, die Anbieter scheuen schlicht die Vergleichbarkeit.

Security-Funktionen auch im Backup immer wichtiger

Als Anhaltspunkt wird gerne der *Magic Quadrant* »Enterprise Backup and Recovery Software« von **Gartner** herangezogen. Daran ist grundsätzlich nichts auszusetzen. Der MQ bildet allgemeine Markttrends ab und gilt als Referenz für die Verfolgung und Bewertung von Anbietern von Datensicherungs-lösungen für Unternehmen. Nur ist die Entstehung bzw. die Interpretation nicht immer transparent. Zudem stützen sie sich ausschließlich auf den globalen Markt und berücksichtigen keine loka-

Anbieter	Produkt
Acronis	Cyber Protect →
Altaro	VM Backup →
Arcserve	UDP (Unified Data Protection) →
Cohesity	Data Protect →
CommVault	Complete Backup und Recovery →
Dell EMC	Networker Data Protection Suite →
IBM	Spectrum Protect →
Novastor	DataCenter →
Quest	NetVault →
Rubrik	Cloud Data Management →
SEP	Sesam Apollon →
Veeam	Backup & Replication →
Veritas	NetBackup →

len Tendenzen. Deswegen verweisen wir auch auf das *Professional User Rating* von **techconsult**, den *PUR-S Security Solutions 2024*. Anstelle eines Quadranten, visualisiert Techconsult seine Resultate in Form eines Diamanten. Die Ergebnisse setzen sich aus einer Umfrage unter mehr als 3.500 Security-Experten zusammen, die ihre eingesetzten Lösungen und deren Hersteller bewerten. Allerdings vermi-



Karl Fröhlich
speicherguide.de

schen die Marktforscher hier die Bereiche Backup/Recovery und Security.

Wobei natürlich eine Backup-Software heute wesentlich mehr Security-Funktionen mitbringt als früher. »Im Zuge des KI-bedingten Fortschritts auch aufseiten der Cyberkriminellen, ist es von äußerster Wichtigkeit, moderne und innovative IT-Security-Lösungen einzusetzen um sich dem entgegenzustellen«, sagt Techconsult-Analyst **Raphael Napieralski**. »Die befragten Security-Experten sind sich dessen ebenfalls bewusst und bewerten die Innovationsfähigkeit der Security-Hersteller als wichtiges Merkmal. Sämtliche IT-Security-Hersteller, die als Champion ausgezeichnet wurden, erhielten durch die Security-Experten stark überdurchschnittliche Bewertungen ihrer Innovationsfähigkeiten.« Diese betreffen nicht nur komplett neue Lösungen, sondern auch die stetigen Verbesserungen bereits bestehender Lösungen. Aus heutiger Sicht den stets bestmöglichen Cyberschutz zu erhalten, ist das, was sich alle Hersteller für ihre Kunden ins Pflichtenheft schreiben. Grundsätzlich werde dies auch von allen platzierten Herstellern erfüllt, wobei einige aus Sicht der Kunden besonders positiv auffallen.

Backup-Markt zunehmend komplex

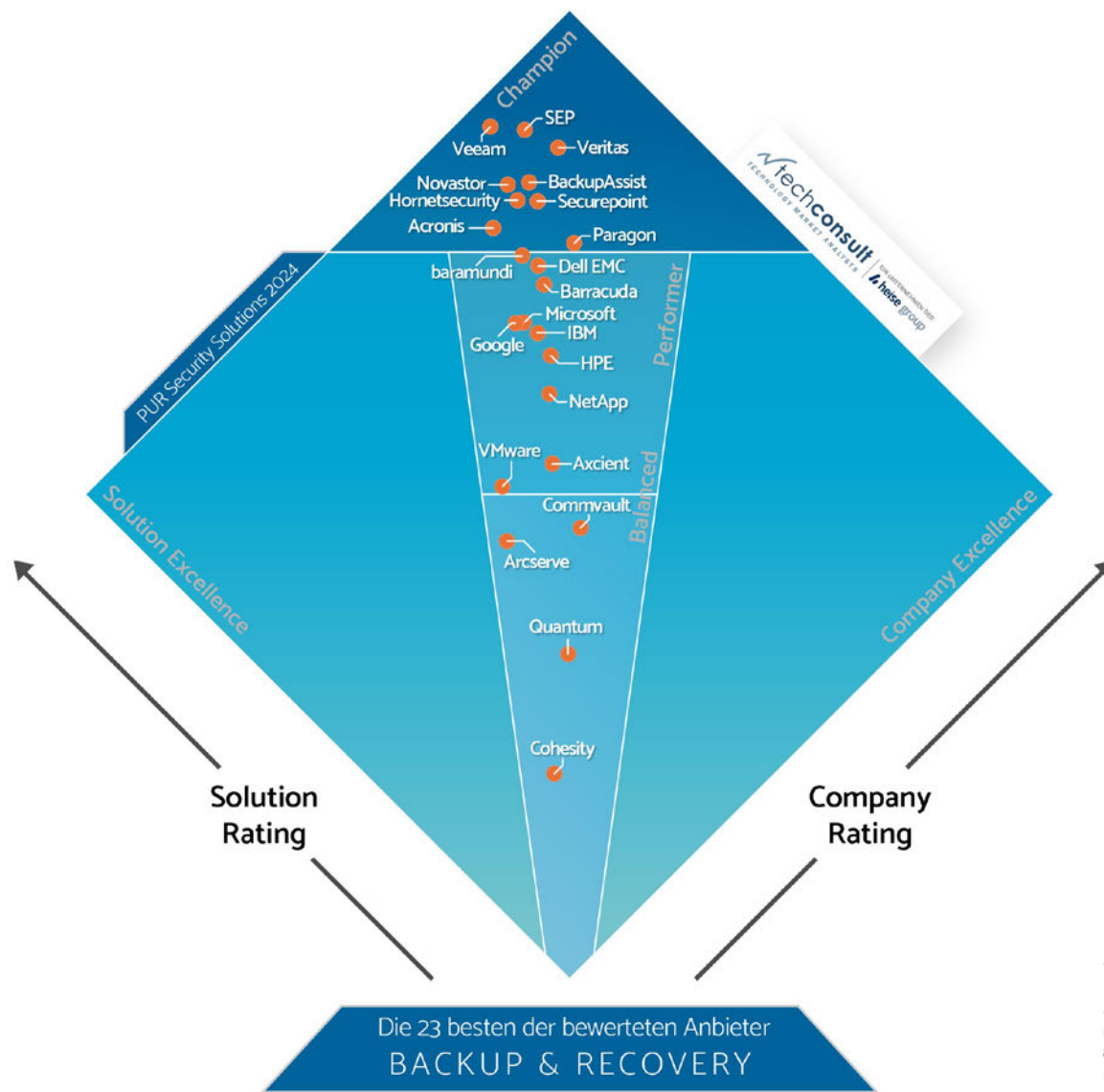
Beschreibung des Backup/Recovery-Marktes wird zunehmend komplexer: Das klassische Modell mit Backup-

Server und Backup-Software ist kaum mehr existent. Zu unterscheiden gilt es zwischen verschiedenen Ansätzen, die dazu unter Umständen ineinanderfließen.

Block-Level-Backup: Das Block-basierte Backup analysiert Daten identifiziert nur die geänderten Blöcke. Dies ermöglicht eine schnellere Sicherung und Wiederherstellung von Daten. Dies reduziert die benötigte Zeit und die Auswirkungen auf die Systemleistung während der Sicherung. Da nur die geänderten Blöcke gesichert werden, wird weniger Speicherplatz benötigt. Das Block-basierte Backup soll eine granulare Wiederherstellung von Dateien und Ordnern erlauben, was besonders nützlich ist, wenn nur bestimmte Teile der Daten wiederhergestellt werden müssen.

File-Backup sichert Dateien und Ordner auf Basis von Datei-Systemen, meist komprimiert, meist auf einem NAS-System. Die Wiederherstellung ist relativ einfach, aber letztlich Ressourcen-intensiv. Bei KMU wird aber die selektive Sicherung und die einfache Versionisierung geschätzt. Der Zeit- und Ressourcen-Aufwand ist relativ hoch, zusätzliche Ressourcen wie Bandbreite und Rechenleistung werden belastet.

Object-Storage-Backup: Beim Object-Storage-Backup werden die Daten in Form von Objekten in einem Objektspeicher gesichert. Diese Sys-



»Professional User Rating: Security Solutions 2024« (PUR-S) haben zum achten Mal mehr als 3.500 Anwenderunternehmen IT-Sicherheitshersteller und ihre Lösungen bewertet.

Grafik: Techconsult

teme sind in der Regel hoch skalierbar und können große Mengen an Daten verarbeiten. Dies erlaubt die Sicherung und Speicherung großer Datenmengen. Object-Storage bietet Mechanismen zur Datenreplikation und -verteilung, um Redundanz und Zuverlässigkeit sicherzustellen. Dadurch werden die Daten vor Verlust geschützt und die Verfügbarkeit erhöht. Sie unterstützen verschiedene Arten von Daten, einschließlich unstrukturierter Daten wie zum Beispiel Dateien, Bilder oder Videos. Dies ermöglicht die Sicherung und Wiederherstellung einer Vielzahl von Datenarten. Sie sind relativ einfach skalierbar, wenn die Datenmenge wächst.

Allerdings kann dies auch Nachteile haben: Da Objektspeicher über das Netzwerk zugänglich sind, sind Latenzproblemen möglich, insbesondere bei großen Datenmengen oder bei der Wiederherstellung von Daten. Auch können sich Komplexität, Kosten und die Abhängigkeiten von der Infrastruktur summieren, und zusätzliche Investitionen in Hardware, Netzwerk und andere Ressourcen erfordern.

Container-Backup: Auch Container lassen sich für Backup-Zwecke verwenden. Der Fokus liegt hier auf der letzt-gesunden Konfiguration einer Anwendung, weniger der verarbeiteten Daten selbst. Container sind eine Art von Virtualisierungs-Technologie, die es ermöglicht, Anwendungen und

ihre Abhängigkeiten in einer isolierten Umgebung auszuführen. Dadurch können sie leicht von einem System auf ein anderes verschoben oder repliziert werden, was die Portabilität und Flexibilität des Backups erhöht.

Container können schnell und einfach skaliert werden, dislokal gleichzeitig ausgeführt werden, um die Backup-Geschwindigkeit zu erhöhen oder die Last auf mehrere Systeme zu verteilen. Container sind ressourcenschonend und benötigen weniger Speicherplatz und Rechenleistung im Vergleich zu herkömmlichen virtuellen Maschinen.

Allerdings gibt es auch potenzielle Nachteile bei der Verwendung von Containern für Backup oder das Backup von Containern: Die Verwendung erfordert zusätzliche Kenntnisse und Fähigkeiten in der Container-Technologie und vor allem ist das Backup eng mit der verwendeten Container-Plattform verbunden. Wenn sich die Plattform ändert oder nicht mehr unterstützt wird, kann dies die Wiederherstellung des Backups erschweren.

Blockchain vs. Backup-Software

Schreiben die Analysten solche Marktübersichten letztmals? Vielleicht – Cloud, Object, Container – lokale, out-gesourcete, as-a-Service-Angebote überschreiten das Maß der Lesbarkeit, – über die Sinnhaftigkeit mag man streiten. Zumal der deutsche Mittel-

stand aus unserer Erfahrung progressiver ist, als man international so denkt.

In dem Sinne mal einen Blick voraus: Blockchain als Backup-Ansatz? Kurz gesagt, heute keinesfalls. Doch wer weiß...

Blockchain nutzt das Internet als dezentrale, transparente Datenbank im Netz, die es ermöglicht, Datenblöcke unveränderbar zu speichern. Eine Art Peer-to-Peer-Netzwerk auf Block-Level. Warum sollte man dies (einmal ungeachtet von Compliance-Vorgaben gedacht) mit Unternehmensdaten tun?

Die Änderung eines Daten-Sets wird erfasst, hat aber keine Wirkung. Es handelt sich um Datenblöcke, keine Datenbank. Potenziell sind auf Grund der Multiplikation und Dezentralisierung fokussierte Angriffe kaum möglich. Auslesen ist nur dem Dateneigentümer möglich, wegen kryptographischer Algorithmen, die nur dem Daten-Eigentümer zugänglich sind.

Bezahlt wird dies über Tokens, Kryptowährungen. Tokens erwirbt man über Einstellen von Blocks, oder über bares Geld, ohne zu wissen an wen. Das ist ein Finanzmarkt, der sich offenbar inzwischen durchaus etab-

liert hat und wenig mit den Anfängen im Darknet zu tun haben. Zumindest wird *Elon Musk* deswegen nicht gerichtlich verfolgt. Für eine gewisse Klientel ist das wohl normal.

Die Blockchain-Technologie ermöglicht die Verteilung der Daten auf mehreren Knoten oder Teilnehmern im Netzwerk. Dadurch wird das Risiko eines einzelnen Ausfalls oder einer zentralen Schwachstelle minimiert. Selbst wenn einige Knoten ausfallen, bleiben die Daten auf anderen Knoten verfügbar.

Jeder Block enthält eine Liste von Transaktionen oder Daten und einen eindeutigen Hash-Wert, der den vorherigen Block identifiziert. Durch Kryptographie kann nur der Einsteller den Wert des Blocks entschlüsseln. Blocks und Daten sind nicht unveränderlich, jedoch nur mit Erlaubnis des Einstellers legitimiert.

Nur, Backup-Anbieter spielen in dieser Welt keine Rolle mehr. Heute taugt die Technologie, wenn überhaupt, zur Sicherung ausgewählter Bytes oder Scripts, die mit Daten arbeiten. Wiederherstellungs-Pragmatismen greifen nicht. Aber eventuell zukünftig.

Arcserve UDP

Das Backup-Portfolio von **Arcserve** umfasst *Arcserve UDP*, *Arcserve Backup*, *Arcserve UDP Appliances*, *UDP Cloud Hybrid*, *OneXafe Storage-App-*

liances und *SaaS-Backup*. Die meisten Kunden gehören dem Mittelstandssegment an. Anfang 2021 fusionierte Arcserve mit **StorageCraft**, insbesondere um Appliances mit *Nutanix* zu vertreiben.

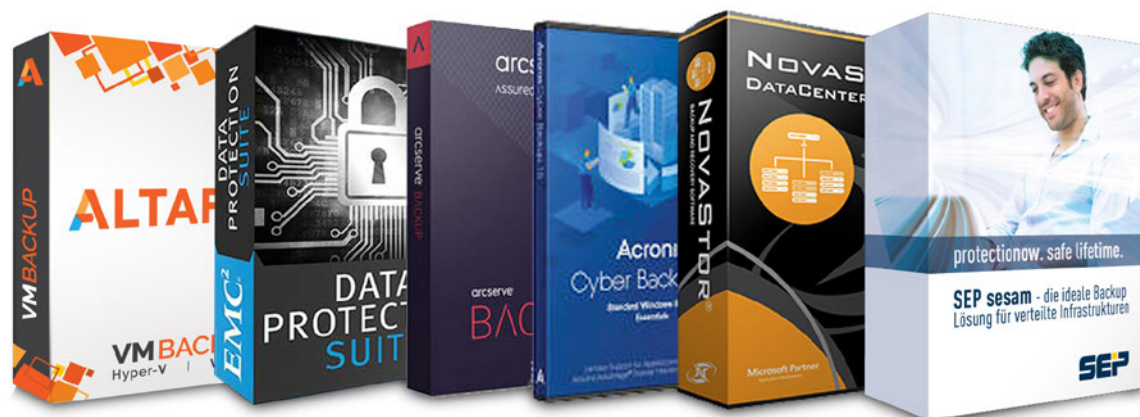
Mit *Arcserve UDP 9.0* (Unified Data Protection) kündigt der Hersteller die nächste Generation seiner zentral verwalteten Backup- und Disaster-Recovery-Lösung an. Die Software eignet sich eigenen Angaben zufolge für jede Art von Dateninfrastruktur und Workloads. Sie soll Data-Protection, *Sophos Intercept X Advanced Cybersecurity*, unveränderlichen Speicher und Tape-Backup mit skalierbarer Geschäftskontinuität (Business Continuity) kombinieren – sowohl Onsite als auch Offsite.

Auch Arcserve offeriert verschiedene Lizenzmöglichkeiten, unter anderem wird über Sockel oder Server lizenziert, in den Editionen Standard, Advanced und Premium. Online wird Arcserve UDP 9.1 für einen Sockel ab 809 Euro angeboten (Standard Edition, 1 Jahr Enterprise-Maintenance).

Acronis Cyber Protect

Vor ein paar Jahren ordnete der magischen Quadranten **Acronis** noch als Visionär ein. Mittlerweile ist das Software-Haus bei den Herausforderern und Nischenanbietern angekommen. Grundsätzlich ist dies erstmal ein Abstieg. Gleichzeitig konzentriert sich

Weitere Informationen:
Lesen Sie eine **ausführliche Fassung des Marktüberblicks** auf [speicherguide.de](https://www.spiecherguide.de)



Collage: speicherguide.de und die jeweiligen Hersteller

Acronis weniger auf Enterprise-Kunden, sondern auf Managed-Service-Provider (MSP) und den Mittelstand.

Durch die Übernahme mehrerer Cybersicherheitsfirmen in den letzten 24 Monaten verfügt Acronis über ein ansehnliches Sicherheits- und Präventionsportfolio, und die Produkte selbst (*Cyber Protect* und *Cyber Protect Cloud*) bieten eine angemessene Abdeckung für Endpunkte, VMs, SaaS und verschiedene Workloads.

Gartner weist jedoch auf Bedenken hinsichtlich der Skalierbarkeit und der Unterstützung für mehrere Funktionen hin, die für Unternehmenskunden wichtig sind.

Die Preise von Acronis Cyber Protect beginnen in der Standard-Edition für einen Server/VM bei zirka 480 Euro

pro Jahr. Die Advanced-Version beginnt bei 770 Euro.

Cohesity Data Protect

Cohesity Data Protect ist eine Datenmanagement-Lösung zum Schutz von cloud-nativen, SaaS- und On-Premise-Daten ab, aber auch auf Backup, Wiederherstellung, Replikation und Notfallwiederherstellung von Daten, aber auch auf die weiterführende Verarbeitung von Metadaten, etwa für Tests, Entwicklung und Analytics.

Von einer einheitlichen Benutzeroberfläche können laut Hersteller Hypervisoren (Vmware, Nutanix AHV, Microsoft Hyper-V, RHeV), traditionelle und moderne Datenbanken (Oracle, SQL, MongoDB, Cassandra, CouchbaseDB, Hbase) und Anwendungen

(SAP HANA, EPIC, Office 365, Kubernetes), Big-Data-Hadoop-Workloads, Speicher (Pure, Netapp, Cisco, Dell EMC) und physische Workloads (Microsoft, Solaris, Linux, AIX) verwaltet, gesichert und wiederhergestellt werden.

Cohesity Data Protect ist ein Abonnement-Dienst, der je nach Funktionalität und Kapazität bis in den fünfstelligen Bereich jährlich kosten kann. Zudem ist der Dienst als Add-on zur Cohesity Data-Plattform verfügbar, die in der Premium-Edition für etwa 1.200 Euro jährlich buchbar ist, wiederum mit unzähligen Variablen.

Interessant wird es, wie es künftig weitergeht, denn Cohesity wird mit **Veritas** fusionieren und übernimmt dessen Data-Protection-Business.

Commvault

Commvault gehört im Gartner- und Forrester-Ranking zu den Marktführern im Enterprise-Bereich. Die breite Unterstützung von Public-Cloud-Angeboten, Hypervisoren, Big-Data-Fähigkeit und die Eignung für viele Storage-Arrays sind die von den Analysten angeführten Gründe.

Commvault Complete Backup und Recovery bietet eine umfassende Plattform für die Sicherung und Wiederherstellung von Daten in physischen, virtuellen und Cloud-Umgebungen. Die Software ermöglicht die regelmäßige Sicherung von Daten auf verschiedenen Speichermedien wie Festplatten, Bandlaufwerken oder Cloud-Speichern. Es können inkrementelle, differentielle oder vollständige Backups durchgeführt werden.

Multi- und Hybrid-Cloud-Support, Remote-Duplikation, Deduplikation und Encryption sind inkludiert, ebenso Engines für intelligente Archivierung von Nutzerdaten in lokalen und in der Cloud gespeicherten Mailboxen sowie in anderen nutzerbasierten Datenspeichern. Künstliche Intelligenz und Algorithmen für maschinelles Lernen sollen laut Hersteller die Leistung optimieren, Muster analysieren und Anomalien melden. Die Software ermöglicht die Wiederherstellung von Daten auf verschiedenen Ebenen, von einzelnen Dateien bis hin zu kompletten Systemen. Commvault bietet di-

verse Reporting- und Monitoring-Funktionen, um den Status der Backups zu überwachen und Berichte über den Backup- und Wiederherstellungsstatus zu erstellen.

Commvault adressiert vor allem große Unternehmen und gilt eher als komplex, insbesondere für KMU und wegen des universellen Ansatzes. Analysten loben allerdings die enorme Skalierbarkeit. In punkto Preisbeispielen gehört Commvault zu den zugeknöpften Unternehmen. Die Jahreslizenzen beginnen für beispielsweise eine Instanz zwischen rund 1.500 und 1.900 Euro netto.

IBM Storage Protect

IBM Storage Protect, vorher *Spectrum Protect* und ehemals *Tivoli Storage Manager* (TSM), ist eine Backup-Recovery-Software mit Funktionen für Deduplizierung, Snapshot, Management und Disaster-Recovery.

IBM bietet unter anderem eine Zwei-Schlüssel-Autorisierung für Administratorbefehle, Verschlüsselung, proaktiven Sicherheitsbenachrichtigungen sowie eine native Unterstützung für Band- und unveränderlichen Objektspeicher. Pro Server skaliert die Lösung auf bis zu 4 PByte an Client-Daten und soll eine Aufnahme von bis zu 100 TByte an neuen und geänderten Client-Daten pro Tag ermöglichen.

Bei den Preisoptionen ist eine monatliche Lizenzierung möglich, es sind

aber auch zeitlich unbegrenzte Lizenz erhältlich. Hier nennt der Hersteller beispielsweise 2.160 US-Dollar pro zehn verwalteter VMs oder pro TByte.

Novastor Datacenter

Das in Hamburg ansässige Unternehmen **Novastor** bietet mit *NovaStor DataCenter* eine ganzheitliche Datensicherung für physische und virtuelle Server auf derselben Oberfläche, zentralisiert die Sicherung verteilter Daten und das Medien-Management von Cloud, Disk und Tape inklusive Datenauslagerung.

Der Hersteller verspricht freie Wahl bei Speichermedien und -herstellern, hohen Automationsgrad, Fehlertoleranz und effiziente Speichernutzung. Adressiert werden primär mittelständischen Unternehmen, Behörden und öffentliche Verwaltungen, die Lösung skaliert aber auch auf mehrere tausend Server.

Zuletzt integrierten die Hamburger eine *Microsoft 365*-Sicherungen in die Backup-Software. Ein weiteres extra Tool ist künftig nicht mehr nötig. Die aktuelle Version kommt zudem mit einem Cloud-Backup, welches zusammen mit Partner *Ionos* möglich ist. Damit soll sich auch eine automatisierte 3-2-1-Strategie aus der Software heraus aufsetzen lassen. Ein separater Vertrag mit dem Internet-Anbieter ist nicht notwendig, die Verwaltung ist komplett über die Datensicherungs-Oberfläche möglich.

Die Software ist in diversen Lizenzmodellen erhältlich. Eine Mietlizenz für die *Novastor Datacenter Suite* (1 Universal, 15 Workstation, 5 TByte) beginnt im Online-Handel beispielsweise bei 1.923 Euro netto.

Rubrik

Gartner führt **Rubrik** im Magic Quadrant 2023 auf Rang 1 im Bereich Vision und auf Rang 3 bei den Leaders. Mit mehreren Erweiterungen der Cloud-basierten Datensicherungsfunktionen, einschließlich eines neuen *Security Command Centers*, konzentriert sich der Hersteller weiter auf den Ausbau seiner Ransomware-Erkennungs-/Schutzfunktionen sowie der Automatisierung.

Die Analysten bemängeln allerdings, dass die Fokussierung auf die Sicherheit, zu Lasten der Gesamtentwicklung des Backup-Angebots gehe. Andere Anbieter führen laut *Gartner* in den Bereichen SaaS/BaaS mehr Lösungen und hätten diese schneller in den Markt gebracht.

Dafür garantiert **Rubrik** seinen Kunden eine schnelle Wiederherstellung ihrer Daten für den Geschäftsbetrieb nach einem Cyber- oder Ransomware-Angriff. Andernfalls deckt der Hersteller bis zu fünf Millionen US-Dollar für die Kosten im Zusammenhang mit der Datenwiederherstellung. Dieses Angebot gilt für **Rubrik-Kunden**, die die *Rubrik Enterprise Edition* einsetzen

und mit einem *Rubrik Customer Experience Manager (CEM)* zusammenarbeiten, um sicherzustellen, dass die Best-Practices der Branche für die Datensicherheit eingehalten werden.

In puncto Preisgestaltung lässt sich **Rubrik** nicht in die Karten schauen. Soweit wir es recherchieren konnten, beginnen entsprechende Installationen im höheren fünfstelligen Bereich.

SEP Sesam

Der deutsche Datensicherungs-Spezialist **SEP** hat sich mit seiner Backup-Software, derzeit im Release *SEP sesam Apollon v2*, auf die Unterstützung von allem und jedem spezialisiert. Soll heißen, es arbeitet mit nahezu jedem Betriebssystem und Hypervisoren sowie allen gängigen Anwendungen zusammen. Zuletzt wurde beispielsweise die Sicherung von *SAP IQ (OLVM)* hinzugefügt sowie eine schnellere Sicherung von *VMware*-Instanzen mittels Snapshots.

Zudem setzt **SEP Sesam** auf Immutability: Die Funktionen *Blocky4sesam*, *S3 Object Lock* und *SEP immutable Storage (SiS)* sollen als weitere Sicherheitsstufe die Backups selbst vor Ransomware schützen. Der Restore-Virus-Check *Ikarus* soll zudem die Sicherheit erhöhen und überprüft Daten beim Restore nochmal auf Viren. Der Einsatz von *SEP Si3 NG* Inline-Deduplizierung soll eine Speicherplatz-

KEEP UPDATED

Auf dem Laufenden bleiben

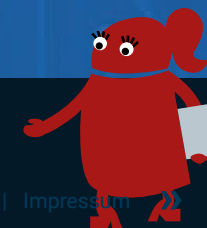
Jetzt unseren Storage-Newsletter abonnieren



Mittwoch & Freitag lesenswertes über Backup, Storage & Datacenter

speicherguide.de
Das Storage-Magazin

TRENDS | STRATEGIEN | LÖSUNGEN



sparende Ablage oder Replikation der Daten ermöglichen.

SEP bietet verschiedene Lizenzmodelle an. Diese reichen von der einfachen Volumenlizenzierung nach TByte-Datenvolumen, bis hin zur speziellen Lösung und Lizenzierung für Managed-Service-Provider (MSPs). Mit der kostenlosen Community-Edition können Anwender SEP Sesam in limitiertem Umfang und nach kostenloser Registrierung ebenfalls nutzen. SEP sesam Professional beginnt beispielsweise bei 1.284 Euro netto (1 TByte, 1 Jahr). Die 1-TByte-Erweiterung beläuft sich auf 1.029 Euro. Die Kauflizenz inklusive Maintenance beginnt bei rund 3.990 Euro.

Veeam Backup & Replication

Veeam Backup & Replication (VBR) verspricht eine schnelle und zuverlässige Wiederherstellung von Daten, Anwendungen und virtuellen Maschinen. Es ermöglicht granulare Wiederherstellungen auf Datei- oder Objektebene sowie vollständige Systemwiederherstellungen. Mit der *Instant VM Recovery*-Funktion können virtuelle Maschinen in wenigen Minuten wiederhergestellt werden. *Veeam ONE* ist ein zusätzlicher Analyse-Dienst.

VBR unterstützt eine breite Palette von Plattformen und Umgebungen, einschließlich virtueller Architekturen wie *VMware vSphere* und *Microsoft*

Hyper-V, physische Server, Cloud-Umgebungen wie *Microsoft Azure* und *Amazon Web Services (AWS)* sowie *Microsoft 365*. Seine Wurzeln hat VBR

in der Sicherung von virtuellen Vmware-Instanzen. Mittlerweile werden aber auch physische Umgebungen unterstützt. Die Zukunft liegt in der Cloud.

Veeam baut sein Angebot entsprechend aus.

VBR ist momentan in der Version 12.1 erhältlich. Zu den Funktionen ge-

hören unter anderem neue Cloud-Funktionalitäten, darunter auch direkter Schreibzugriff auf Objektspeicher, sowie Cloud-basierte Agenten. Die native Verfügbarkeit unveränderlicher Backups soll Anwender mehr Kontrolle und eine schnellere Wiederherstellung nach Ransomware-Angriffen ermöglichen. Ein Plug-in für Backup & Replication für *Kasten by Veeam K10 V5.0* erlaubt die zentrale Verwaltung der Kubernetes-Datensicherung. Seit April 2023 fasst Veeam seine Produktpalette im Bereich der Sicherung & Wiederherstellung, Überwachung und Orchestrierung unter dem Namen *Veeam Data Platform (VDP)* zusammen. Derzeit sind vier Modelle (*Veeam Universal License, VUL*) erhältlich, die auf Basis der Workloads lizenziert werden. Im Internet sind aber auch noch Lizenzen pro CPU/Socket erhältlich bzw. nach Instanzen. Eine Subscription-Lizenz für VBR v12.1 Enterprise Plus Edition (5 VMs, 1 Jahr) beginnt beispielsweise bei rund 860 Euro netto. Eine Foundation-Universal-Lizenz für zehn Instanzen und einem Jahr Laufzeit wird unter anderem für etwas über 1.170 Euro angeboten. ■



Weitere Informationen:

Lesen Sie eine **ausführliche Fassung des Marktüberblicks** auf speicherguide.de

Sicheres Backup als Schutz vor den Folgen von Ransomware Attacken

Ein Angriff durch Ransomware ist für ein Unternehmen immer eine Katastrophe. Allein das Schützen des Netzwerk vor weiteren Angriffen erfordert oft viele Tage. Ist dann auch noch das Backup der Unternehmensdaten von der Attacke betroffen, kann das den Ruin bedeuten.

Den besten Schutz des Backups bieten natürlich nach wie vor **ausgelagerte LTO-Kassetten**, da hier jede Art von Remote-Zugriff zu 100% ausgeschlossen werden kann. Auch bei Libraries sollten die Kanister mit dem Backup am besten entnommen werden.

Doch auch die Hersteller von **diskbasiertem Backup** haben einiges getan, den Zugriff auf die Datensicherungen zu verhindern. Minimum der Anforderungen ist, dass die Daten nur für die Backupsoftware selbst sichtbar sind. Das ist z.B. bei **Open-E JovianDSS** der Fall, wenn die Daten snapshotbasiert auf einen weiteren Rechner gesichert werden.



EonStor GS 1000 Gen2

Ebenso macht es mittlerweile auch **Infotrend** mit ihren **EonStor GS** Systemen. Hier kommt eine **Data-Lock** Funktion dazu, die Backup-Volumes unveränderlich macht.

Außerdem bietet Infotrend die






Möglichkeit, selbständig Backups zu ziehen, sowie **S3 Immutable Backupvolumes für Veeam** zur Verfügung zu stellen.

Sehr elegant hat das **ExaGrid** gelöst: Hier werden die Backups nach Auslagerung in eine **zweite Repository-Ebene** (mit Deduplikation

auch über viele Knoten) gesichert. Dort können sie mit einer einstellbaren **Retention Time** vor jeder Veränderung geschützt werden. Bei **Veeam**, der idealen Software für die Sicherung virtueller Maschinen, lässt sich ein Linux Server zum **Hardened Linux Immutable Repository** machen, das nur von der Software direkt erreicht werden kann und ebenso durch Retention Zeiten geschützt wird.

Backuplösungen mit Schutz vor Ransomware bei EUROstor:

(mehr Info unter www.EUROstor.com/backup.)

- **LTO Tape Libraries von Actidata**
Schutz der Daten durch räumliche Auslagerung 
- **Veeam Backup Server**
Zweit-Sicherung der Virtuellen Maschinen in ein Immutable Repository (s. rechts) 
- **ExaGrid Tiered Backup Storage**
Backups mit Retention in einer zweiten Backupenebene 
- **Infotrend EonStor GS**
Volumecopy mit Schreibschutz durch Data-Lock Funktion und als S3 Speicher für Veeam Repository 
- **Open-E JovianDSS Storage**
snapshot basierte On-/Off-site Data Protection (ODP) auf zweiten Standort 



Alle Storage-Systeme aus einer Hand:

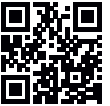
EUROstor ist seit 2004 Hersteller von Storage-Systemen. Unsere software-defined Server Lösungen reichen von kleinen File-Servern bis hin zu hochverfügbaren Storage-Clustern, Scale-Out Clustern und Ceph- und Cloud-Servern, aber auch allgemein einsetzbaren Servern, beispielsweise für die

Virtualisierung. Dazu kommen RAID Systeme, LTO-Libraries, Connectivity Produkte wie Brocade FC-Switches.

Rufen Sie uns einfach an, wir beraten Sie gerne! Registrieren Sie sich auch für unseren Storage Newsletter (Print oder E-Mail, 3 x pro Jahr) unter www.EUROstor.com/Newsletter.



VEEAM AMD EPYC



ES-3036 als Hardened Linux Immutable Repository mit 36 Slots (12 davon auf der Rückseite)

ES-3036, 36 3.5" Slots, z.B. teilbestückt mit **€ 12.483,10** (inkl. MwSt.) **€ 10.490,-** (exkl. MwSt.)
12 x 20 TB SATA Enterprise HDDs,
2 x 512 GB M.2 Boot-SSD für das Betriebssystem

Hardened Linux Backup Repository Server:

- Storage-Server mit 36 3.5" Slots, bis 864 TB bei Verwendung von 24 TB Disks
- alternativ: 12/16/24 3.5" Slots, 24/72 2.5" Slots
- AMD EPYC Rome 7232P Prozessor, 8 Core, 3,1 GHz auf Supermicro H12SSL-NT Board, 7 PCIe 4.0 Slots
- 64 GB RAM, optional bis zu 1 TB
- 2 x 10 GbE (RJ45) onboard, opt. mehr und bis 100 GbE
- OS auf 512 GB NVMe M.2 SSDs im RAID 1, Ubuntu auf Wunsch vorinstalliert
- Areca RAID Controller mit 12 Gbit SAS, RAID Management über dedizierten Netzwerkport
- optional Erweiterungports für bis zu 512 Laufwerke
- Monitoring, remote Management und iKVM Console über Netzwerk (IPMI)
- inklusive 3 Jahre Standard Wartung mit kostenlosem Telefon- und E-Mail-Support, optional: Erweiterung auf 5 Jahre, Express-Austausch oder Vor-Ort-Service

EUROstor GmbH • Hornbergstr. 39 • D-70794 Filderstadt • Tel: +49 (0)711 70 70 91 70 • Fax: +49 (0)711 70 70 91 60

Preisänderung, Druckfehler und Irrtum vorbehalten.

Informieren und registrieren Sie sich auf unserer Website: www.EUROstor.com/Newsletter

E-Mail: Info@EUROstor.com - Tel.: +49 (0)711 70 70 91 70

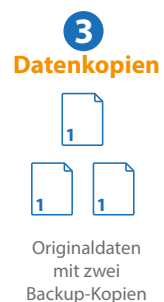
Einfache aber effektive Backup-Strategie plus Unveränderlichkeit

UNERSETZLICH: DIE 3-2-1-(1-)BACKUP-REGEL

Der Daten-Gau lauert immer und überall und betrifft geschäftliche wie auch private Daten gleichermaßen. Vor Hardware-Defekten, amoklaufenden Programmen und Benutzerfehlern ist keiner gefeit. Außerdem dürfen Feuer- und Wasserschäden sowie neuzeitliche Bedrohungen wie Cyber- und Ransomware-Attacken nicht außer Acht gelassen werden. Um sich vor Datenverlust zu schützen, ist die 3-2-1-(1-)Backup-Regel daher unersetzlich.

Egal für welche Backup-Strategie man sich entscheidet, die 3-2-1-Backup-Regel gilt als kleinster gemeinsamer Nenner, den es zu erfüllen gilt. Das heißt, drei Kopien der Daten, gespeichert auf zwei unterschiedlichen Speichermedien (Medienbruch) und mindestens einer Offsite-Kopie. Im Detail kommt es natürlich auf die Art und Menge der Daten an und welche Technologien vorwiegend zum Einsatz kommen. Hat dies früher ausgereicht, empfiehlt sich in Zeiten von Cyberattacken eine zusätzliche unveränderliche Kopie (Offline/Immutable).

Unabhängig von der IT-Umgebung, gehören unternehmenskritische Daten so gut es geht geschützt. Wobei dies natürlich auch für die Daten von Einzelpersonen gilt. Je mehr Kopien von einem Datensatz vorhanden sind, desto größer ist der Schutz vor Datenverlust. Risikofaktor Nummer eins ist ein möglicher Hardware-Defekt. Spei-



chermedien jeglicher Art wie Festplatten, Disk-Arrays, SSDs, Speicherkarten, aber auch der interne Speicher von Smartphones und Tablets, sind als mechanische und/oder elektronische Bauteile nicht vor einem Ausfall gefeit. Ohne Kopie sind die Daten unweigerlich verloren. Datenrettungsdienste erreichen heutzutage durchaus kleine Wunder, verlassen kann man sich darauf aber nicht. Zudem ist Datenrettung ein mitunter kostspieliger Service. Je nach Art und Beschädigungsgrad des Mediums beginnen die zu kalkulierenden Einstiegskosten im

vierstelligen Bereich. Zudem müssen Betroffene Zeit mitbringen. Die Wiederherstellungszeit bemisst sich in der Regel in Wochen. Für eine größtmögliche Sicherheit sollten für die Datenkopien zwei unterschiedliche Speichertechnologien genutzt werden. Man spricht hier vom sogenannten Medienbruch. Dies soll die Ausfallwahrscheinlichkeit verringern und für eine Risikoverteilung bei systembedingten Fehlern sorgen und vor Ransomware-Attacken schützen. Jede Internet-Anbindung ist ein potentielles Einfallstor für Cyberangriffe.

Daher sollte sich eine ausgelagerte Kopie zudem an einem anderen geographischen Standort befinden. Alle vorangegangenen Bemühungen bringen nichts, wenn Originaldaten und Backups am gleichen Ort beispielsweise einem Brand oder Wasserschaden zum Opfer fallen. Auch ein Diebstahl lässt sich nie ganz ausschließen.

Speziell als Rückversicherung gegen Verschlüsselungsattacken ist die 3-2-1-Backup-Regel aktueller denn je bzw. nun als 3-2-1-1 mit einer Offline-Kopie. ■



Karl Fröhlich
speicherguide.de

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
Karl Fröhlich
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:

Michael Baumann, Karl Fröhlich,
Peter Marwan

Schlussredaktion:

Brigitte Scholz

Titelbild:

Dall-E (KI)

Layout/Grafik:

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

Mediaberatung:

Bettina Röber
E-Mail: media@speicherguide.de

Webkonzeption und Technik:

IT Verlag GmbH
Ludwig-Ganghofer-Str. 51
Otterfing 83624
E-Mail: webmaster@speicherguide.de

Urheberrecht:

Alle in »storage-magazin.de« erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte (Übersetzung, Zweitverwertung) vorbehalten. Reproduktion, gleich welcher Art, sowie elektronische Auswertungen nur mit schriftlicher Genehmigung der Redaktion. Aus der Veröffentlichung kann nicht geschlossen werden, dass die verwendeten Bezeichnungen frei von gewerblichen Schutzrechten sind.

Haftung:

Für den Fall, dass in »storage-magazin.de« unzutreffende Informationen oder Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit der Redaktion oder ihrer Mitarbeiter in Betracht.

Unser Team



” **Karl Fröhlich**
Chefredakteur
speicherguide.de



” **Michael Baumann**
Redaktion
speicherguide.de



” **Peter Marwan**
Redaktion
speicherguide.de

storage-magazin.de powered by **it-daily.net**

Eine Publikation von **speicherguide.de**