storage-magazin.de

Ausgabe **2-2022**

Eine Publikation von **speicherguide.de**

Quelle: Canva Pro

Einkaufsführer Backup

Marktüberblick Backup-Software & Tape-Librarys

Datensicherungsstrategie: Wichtiger denn je!

Liebe Leserinnen und Leser,

als wir mit den Recherchen für diese Ausgabe begonnen haben, gab es den Angriff auf die Ukraine noch nicht. Doch selbst bis dahin war das Ausmaß der Cyberkriminalität erschreckend: Laut Digitalverband Bitkom entsteht der deutschen Wirtschaft ein jährlicher Schaden von 223 Milliarden Euro. Das IT-Unternehmen Cybersecurity Ventures schätzt, dass die weltweiten Schäden bei sechs Billionen US-Dollar liegen dürften.

Eine Prognose für das laufende Jahr habe ich bisher nicht gesehen, eine Verdopplung würde mich aber nicht wundern. Der Cyberkrieg ist in vollem Gange. Laut Check Point lagen in Europa (EMEA) die durchschnittlich wöchentlichen Angriffe pro Organisation in der vergangenen Woche bei 1.068, 14 Prozent höher als vor Beginn des Krieges. Alle Sicherheitsexperten erwarten einen weiteren Anstieg, auch weil bei vielen qualifizierten russischen IT-Arbeitskräften Auftragsarbeiten für westliche Unternehmen nicht mehr gegeben seien. Wenn auch notgedrungen, aber die Internetkriminalität dürfte für einige ein (lukrativer) Ausweg sein. Die Cyberkriminalität ist ein globales Geschäft und die Bedrohungslage hat sich noch einmal dramatisch verschärft. Erschwerend kommt hinzu, dass die Angriffe mit Schadprogrammen nicht mehr ausschließlich darauf ausgelegt sind, Geld abzuschöpfen. Wir sollten davon ausgehen, dass es nun nicht mehr das Ziel ist, den Zugriff auf Daten zu unterbinden, sondern diese zu zerstören.

Karl Fröhlich, Chefredakteur speicherguide.de

Hinzu kommt noch etwas, worüber wir letztes Jahr in unserem **Backup-eMagazin** geschrieben haben: 54 Prozent aller Backups schlagen fehl. Daran dürfte sich binnen Jahresfrist kaum etwas geändert haben.

Es mag althergebracht erscheinen: Die Datensicherung ist wichtiger denn je. Deswegen beleuchten wir die Thematik in dieser Ausgabe wieder aus verschiedenen Blickwinkeln.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Inhalt

Backup für Cloud- und Objektspeicher auf Tape

PoINT Archival Gateway: Tape-basierter Object Storage mit standardisierter S3 Schnittstelle

Ihre wertvollen Daten auf Cloud- und Objektspeichern müssen durch ein Backup gesichert werden. Technische oder menschliche Fehler können zu gravierenden Datenverlusten führen. Zugleich wächst die Gefährdung durch Cybercrime und Ransomware-Angriffe. Eine Datenkopie auf einem unabhängigen Speichermedium gewährleistet die schnelle Rückkehr zum Geschäftsalltag. Die große Herausforderung dabei sind die enormen Datenmengen im Objektspeicherbereich. Schon aus Kostengründen kann ein Backup nicht auf zusätzlichen festplattenbasierten Objektspeichersystemen erfolgen.

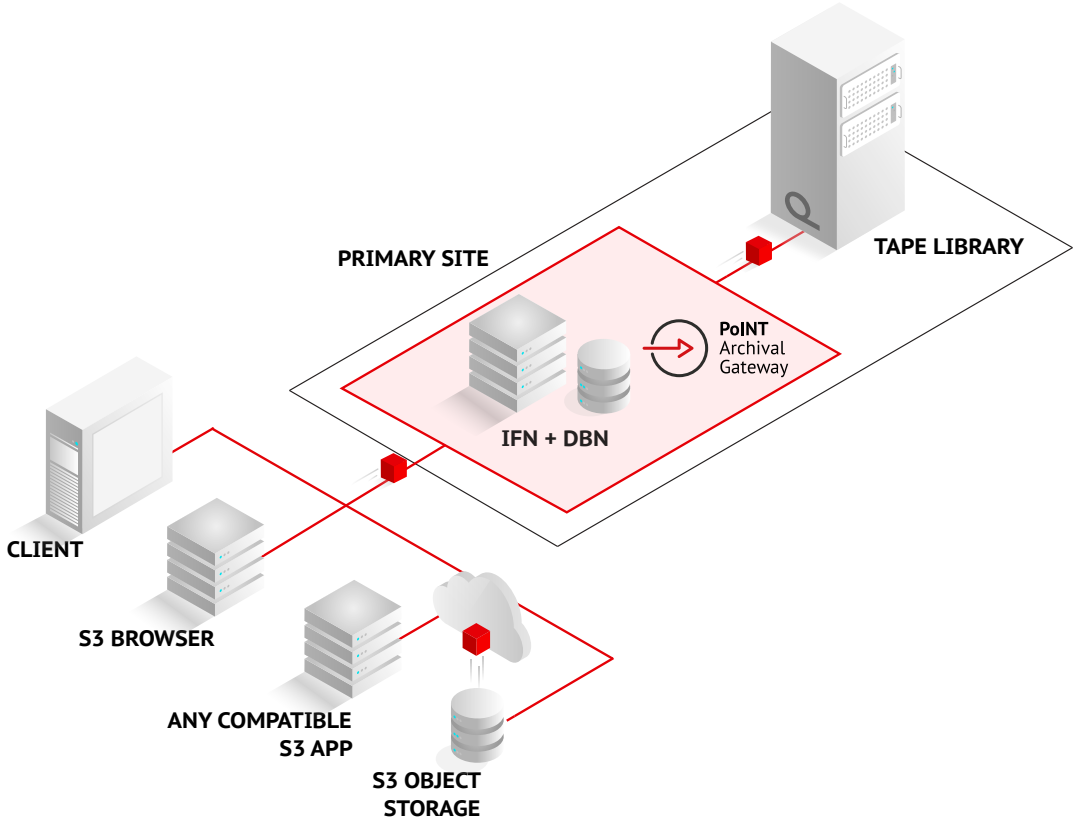
Tape ist das ideale Backup-Medium für große und stetig wachsende Datenmengen:

- Standardisierung
- Skalierbarkeit
- Kosteneffizienz
- Sicherheit durch Air Gap

PoINT Archival Gateway ist ein Tape-basierter Objektspeicher, der die Einbindung von Tape Libraries als zusätzliche, kostengünstige S3 Speicherklasse ermöglicht. PoINT Archival Gateway empfängt die Daten über die standardisierte S3 Schnittstelle und schreibt sie hochperformant auf Tape – die optimale Lösung, um große Datenmengen effizient zu speichern. Im Recovery-Fall sind die Daten ebenso schnell wieder verfügbar.

- Standardisierte S3 REST API
- Datensicherheit durch Verschlüsselung und Erasure Coding
- Direkter Zugriff auf Backup über S3 API
- Herstellerunabhängigkeit und Investitionsschutz durch Standardisierung

Weitere Informationen zu PoINT Archival Gateway finden Sie im Technical White Paper.



PoINT
software & systems

PoINT Software & Systems GmbH • +49 271 3841-0 • info@point.de

Datenmenge und Bedrohungslage steigern die Komplexität

Backup als letzte Verteidigungslinie

Datenverluste entstehen unvorbeireitet, sind kostspielig und verursachen großen Schaden. Deshalb ist eine leistungsfähige Backup-Infrastrukur unverzichtbar, um sensible Daten zu schützen und Daten-Hoheit und -Kontrolle zu behalten. Doch Backups werden schnell unübersichtlich. Mit der Datenmenge steigt auch die Komplexität. Positiv: Nie hatten IT-Manager so viele unterschiedliche Technologien und Ansätze zur Auswahl für ihre Datensicherungsstrategie.

■ Michael Baumann

Eine aktuelle Studie, der *Veeam Data Protection Trends Report 2022*, bringt einige interessante Befunde zum Stand der Datensicherung in Deutschland: 82 Prozent der IT-Entscheidungsträger sind der Auffassung, dass es in ihrem Unternehmen eine Daten-»Verfügbarkeitslücke« nach einem Ausfall geben werde. 81 Prozent empfinden eine »Datensicherungslücke« zwischen der Häufigkeit der Datensicherung und dem akzeptablen Datenverlust. 5,6 Prozent der Befragten äußern deshalb, die Ausgaben für die Datensicherung 2022 zu erhöhen. Über 70 Prozent waren bereits von Ransomware-Angriffe betroffen.

Bedrohung Ransomware – aber nicht nur

Zu den Herausforderungen gehören nicht nur Bedrohungen wie Ransomware, der zunehmende Einsatz der Cloud (bei bereits 51 Prozent der Befragten) und die Orchestrierung der Datensicherung bereiten Probleme. 20 Prozent der Unternehmen erachten eine Verbesserung der Recovery-Point-Objectives (RPOs) sowie niedrigere Recovery-Time-Objectives (RTOs) für notwendig. Ebenso viele erwägen eine Änderung ihrer Backup-Strategie, um Kosten zu senken.

Ein schwieriger Spagat, denn Ransomware-Angriffe können ein Unternehmen teuer zu stehen kommen. Nicht nur Lösegeldforderungen fallen an, sondern auch Folgekosten durch Attacken, die Systeme über Wochen und Monate außer Kraft setzen. Effektive Strategien müssen her.

Jedoch, Cyberattacken bleiben (leider) nicht die einzige Bedrohung für einen Datenverlust. Hardware-Fehler, falsche Scripts und Bedienfehler, die kein neues Phänomen sind, bleiben eine Gefahr. Der Wert der Daten wächst. Um so höher das Schutzbedürfnis.

3-2-1-Regel reicht nicht mehr aus

Im Gespräch mit *speicherguide.de* erklärt **Dennis Rotsch**, Presales Consultant bei **Arcserve**: »Backup ist die letzte Verteidigungslinie gegen Ransomware. Die Frage ist dabei nicht ob, sondern wann man angegriffen wird«. Für ihn und sein Unternehmen führt der Weg über eine multimodale Strategie aus Sicherungs- und Security-Technik, Prozessen und Vorkehrungen für eine orchestrierte Wiederherstellung. Dazu gehören Recovery-Tests, Best-Practices ebenso wie Mitarbeiter-Schulungen.

3-2-1-1 ist die neue Strategie der Stunde. Drei Kopien an zwei Orten, mit einem aus-

Dennis Rotsch, Arcserve

»Die Frage ist dabei nicht ob, sondern wann ein Unternehmen von Ransomware betroffen sein wird.«

Alexander Best, Datacore

»Objektspeicher ist ein ideales Backup-Ziel und erlaubt gleichzeitig PBytes an Daten kostengünstig zu schützen.«

Ines Wolf, Quantum

»Selten angefasste und unstrukturierte Daten sollten aus dem herkömmlichen Backup-Prozess heraus genommen werden.«

Hannes Heckel, Fast LTA

»Wachstum und neue Technologien bedeuten neue Gefährdungen, auch wegen Ausfällen, Bedienfehlern und falscher Konfiguration.«

gelagerten Medium und einer unveränderlichen Daten-Kopie. Arcserve arbeitet hierfür mit dem Security-Anbieter **Sophos** zusammen, um seine Appliance- und Software-Lösungen zu ergänzen. Die Lösungen umfassen Disk und Tape, ebenso wie die Cloud über *UDP Cloud Hybrid*.

Software-defined Datensicherung und Warnung vor Paranoia

Sogar 3-2-1-1-0 propagiert **DataCore**. Die Null muss stehen, meint damit **Alexander Best**, Regional Technologist beim Software-defined-Storage-Spezialisten. Diese Null steht für den Ausschluß von Fehlern beim Backup, unbefugtem Datenzugriff verbunden mit kontinuierlicher Prüfung der Wiederherstellung. Laut seiner Angaben kostet ein Datenverlust durch Ransonware-Attacken deutsche Unternehmen im Schnitt 2,41 Millionen Euro.

Realisiert wird dies bei Datacore mit einer On-Premises-Kopie, zusammen mit Air-Gap durch Offline-Kopien, die auch über Immutability und Object-Lock umgesetzt werden kann. Datacore realisiert dies über seine scale-out Object-Storage-Software *Swarm* als Alternative oder Ergänzung zu Cloud und Tape. Der Fokus liegt hier auf der Hochverfügbarkeit der Datensicherung und der Unabhängigkeit von Hardware.

»Objektspeicher ist ein ideales Backup-Ziel und erlaubt gleichzeitig PBytes an Daten kostengünstig zu schützen«, sagt Best. »Zu Bedenken auf Management-Ebene ist aber auch, wie weit die Paranoia geht oder gehen sollte. Sicherung ja, aber ich darf mich nicht selbst vom Zugriff auf meine Daten abschneiden.«

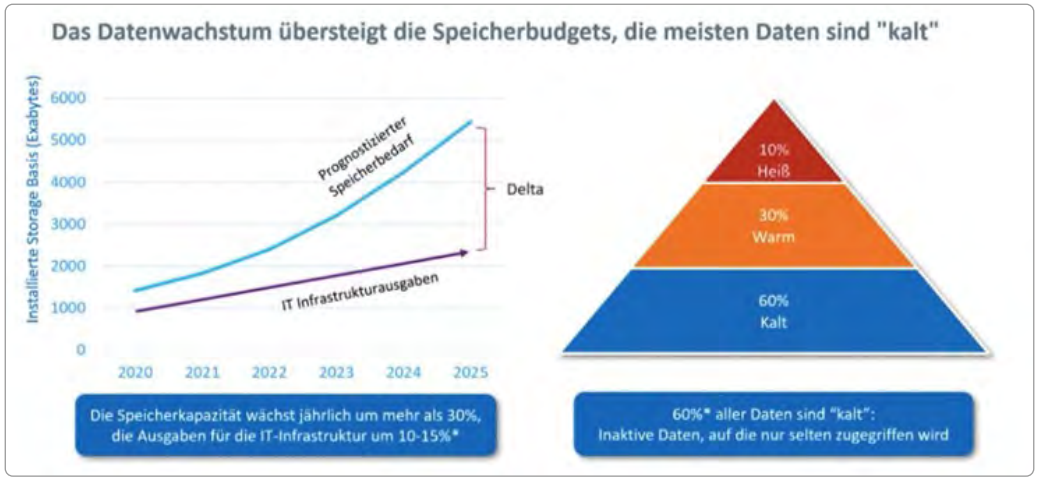
Ein weiterer Schwerpunkt liegt bei diesem Einsatzszenario auf der Integration der Datenhaltung in die Primärspeicher-Architektur auf Basis austauschbarer Standard-Hardware, wie es der Software-defined-Ansatz mitbringt.

Klassifizierung und unstrukturierte Daten

Cyberattacken sind ein Problem, aber ebenso die wachsenden Mengen von unstrukturierten Daten, die möglichst (kosten-)effektiv zu sichern sind. Genau dieses Problem geht **Quantum** mit seiner *ActiveScale Object*-Software an. »Die meisten Daten sind kalt«, weiß **Ines Wolf**, Manager Presales CE bei Quantum. »Allerdings geht es bei Objektspeicher eher um Datenredundanz als um Hardware-Redundanz. In Kombination ist Objektspeicher zusammen mit Magnetband eine Lösung zwischen Objekt- und Langzeit-Speicherung.«

Unternehmen sollten ihre Daten klar klassifizieren. »Selten angefasste, unstrukturierte Daten können eventuell aus dem herkömmlichen Backup-Prozess heraus genommen werden«, ergänzt Quantum-Managerin Wolf, »um die Sicherung strukturierter Daten zu entlasten.«

Sie empfiehlt die Kombination von Disk-basiertem S3-Objektspeicher mit Tape. Die Lösung ermöglicht die reversible Auslagerung über ein Tiering auf Tape, mit entsprechenden Kostenvorteilen für Byte-intensive Daten, auf die ohne größte RPO-Ziele



Grafik: Quantum

Auf 60 Prozent der gespeicherten Daten wird selten bis gar nicht zugegriffen.

zugegriffen werden kann. Die Lösung ermöglicht auch Geo-Redundanz zwischen zwei oder drei Sicherungszielen, um die Sicherheit und Wiederherstellungs-Optionen zu optimieren.

Zusätzliche Sicherheit lässt sich durch ein sogenanntes 2D-Erasure-Coding erzielen. Dabei werden Objekte nicht nur horizontal über mehrere Tapes wiederherstellbar. »Das 2D-Earsure-Coding erfolgt zusätzlich innerhalb eines Bandlaufwerks und erlaubt ein Recovery von einem Medium«, erklärt Quantum-Managerin Wolf.

Warum ist Backup so kompliziert?

Die Komplexität des Backup steigt, meint **Hannes Heckel**, Director Marketing bei **FAST LTA**: »Weil Ransomware kostet. Aber auch, weil die Komplexität mit den Datenmengen steigt. Wachstum und neue Technologien bedeuten neue Gefährdungen, auch wegen Hardware-Ausfällen, menschlichen Bedienfehlern, falscher Konfiguration oder nicht ausreichend skalierender Systeme.« Dafür bietet sein Unternehmen modulare *Silent Brick*-Lösungen.

Auch Backups müssten geschützt werden. Heckel postuliert einen Paradigmenwechsel. Ein einfaches Backup-to-Disk-to-Tape funkioniere nicht mehr. Ziel sei die Wiederherstellung des laufenden Betriebs sowie der Optimierung von RPO und RTO. Deshalb appelliert er für den Einsatz von Flash-Speicher zusammen mit Disk für die Datensicherung. »7-Tage-Backup funktioniert in dem herkömmlichen Sinn nicht mehr«, sagt Heckel. »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.

Tape, Disk, Flash – Block, File, Object

Wir vernehmen unterschiedliche technische Ansätze, auch bezüglich der Medien. Unisono herrscht die Meinung, dass Backup-Ansätze sowohl übergreifend sein sollen, aber auch die Komplexität reduziert werden soll. Angesichts der unterschiedlichen Unternehmensanforderungen, Branchen oder gesetzlichen Vorschriften ebenso wie bestehende Verträge und Verpflichten eine Quadratur des Kreises für die meisten Unternehmen.

Während des Digitalevents von *it-daily.net* und *speicherguide.de* gaben sechs Prozent der Besucher an, sehr unzufrieden mit ihrem Backup zu sein. 39 Prozent sehen Verbesserungspotenzial, 33 Prozent denken über eine Optimierung nach. Rund acht von zehn bereitet das Thema gewisse Schmerzen. Handlung erscheint notwendig.

Kalt heisst nicht unwichtig

Ignorieren lässt sich das Thema also nicht, auch darin sind sich die Experten einig. »Je früher Backups geschützt werden, desto weniger Aufwand, desto schneller die Wiederherstellung«, fasst Fast-LTA-Manager Heckel zusammen. Wir hören von den Experten, dass viele Wege in das Rom der Data-Protection führen kann. Cloud-only scheint nicht dazu zu gehören.

Zurück zur Studie: In Deutschland akzeptieren 59 Prozent bei Daten von hoher Priorität einen Ausfall von maximal einer Stunde. Für kältere Daten liegt der Wert bei 47 Prozent, also nicht wesentlich niedriger. Im Umkehrschluss bedeutet das, kalte Daten werden in ihrer Wichtigkeit nicht unterschätzt. ■

Weitere Informationen

- Mehr zu Backup/Recovery und Data-Protection auf speicherguide.de
- Aufzeichnung unseres Backup-Events »Data-Protection im Fokus«
- Ransom-Abwehr: Offsite-Backup & Air-Gap sind Pflicht

Marktübersicht Tape-Librarys

Automatische und skalierbare Backups

Tape erlebt mehr als eine Renaissance. Dementsprechend verzeichnen vor allem Tape-Librarys der Midrange-Klasse eine stabile Nachfrage. Ein gutes Preis-Leistungs-Verhältnis, ein geringer Energieverbrauch und der notwendige Air-Gap-Sicherungslevel, sprechen nach wie vor für den Einsatz von Magnetbändern. Richtig ausgewählt, ermöglichen sie ein bedarfsgerechtes Wachstum und schützen somit die getätigten Investitionen.

■ Karl Fröhlich

Die Einstiegsgröße für einen Bandroboter beginnt bei etwas über 4.400 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 ab zirka 4.774 Euro bzw. 5.473 Euro für LTO-9. Diese Kategorie gilt als Einstieg für kleine Unternehmen. Mit acht Bändern lässt sich eine unkomprimierte Speicherkapazität von 48 bis 144 TByte realisieren.

Bild: Overland-Tandberg

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

Ein größeres Datenwachstum erfordert dagegen skalierbare und flexibel ausbaubare Tape-Librarys. 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 5.100 bis zirka 6.500 Euro.

Tape-Renaissance ungebrochen

Die Nachfrage nach Tape-Librarys steigt kontinuierlich. »Die Renaissance des Tapes hält weiter an und ist alternativlos für das Backup, wenn es um Kapazität und Kosten geht«, meint Actidata-Vertriebsleiter **Albrecht Hestermann**.

»Die Tape-Speichertechnologie hat sich zu einer idealen Lösung für zahlreiche Anwendungen der nächsten Generation entwickelt, die schnell über ihre traditionelle Speicherinfrastruktur hinauswachsen«, ergänzt **Andreas Arndt**, VP Sales EMEA & APAC bei Overland-Tandberg. »Zu diesen Anwendungen gehören neben der klassischen Datenspeicherung und -archivierung auch Surveillance, Internet-of-Things, Hyper-Scale-Computing, Media und Entertainment, Cloud-Speicherdienste und Big-Data-Applikationen.«

Zudem verändern Software-Lösungen für das Verwalten von unstrukturierten Daten die Kaufentscheidungen für Datenspeicher. Basierend auf ihrem Wert und Lebenszyklus würden die Daten nicht auf eine separate Ebene in einem teuren Datenspeicher verschoben, sondern auf ein kostengünstigeres System, wie eben Tape.

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

Haupttreiber für Tape bleiben aber Cyberattacken und Ransomware-Angriffe. Bänder bzw. ganze Magazine lassen sich relativ leicht aus den Librarys entnehmen und offline an einem anderen Standort aufbewahren.

Midrange- und Highend-Librarys mit hoher Skalierbarkeit

»Aktuell sind LTO-7 und LTO-8 gleichauf, jedoch geht der Trend nach LTO-8 und LTO-9«, beschreibt Hestermann die momentane Nachfrage. »SAS-Tape-Librarys in 2U-Bauhöhe werden aktuell am meisten angefragt, überraschenderweise 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-Librarys (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 sowie 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.

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

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. ■

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	actiLib 1U LTO-Autoloader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.444
www.actidata.com	actiLib 1U LTO-Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.774
	actiLib 1U LTO-Autoloader	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 5.473
	actiLib 2U LTO Tape Library	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.631
	actiLib 2U LTO Tape Library	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.905
	actiLib 2U LTO Tape Library	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 6.427
	actiLib Kodiak 3407	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	ab 8.121
	actiLib Kodiak 3407	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 8.449
	actiLib Kodiak 3407	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 9.149
	actiLib Kodiak 6807	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 12.058
	actiLib Kodiak 6807	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 12.386
	actiLib Kodiak 6807	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 13.086
Fujitsu	Eternus LT20 S2	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 5.500
www.fujitsu.com/de/	Eternus LT20 S2	LTO-8	8	1	96	1,1	SAS 6G, FC 8Gb	1U	ab 5.800
	Eternus LT140	LTO-7	20	1-3	120	22,7	SAS 6G, FC 8Gb	3U	ab 6.300
	Eternus LT140	LTO-8	20	1-3	240	22,7	SAS 6G, FC 8Gb	3U	ab 6.800
	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
	Eternus LT270 S2	LTO-7	138	2-20	828	2,7	FC 8Gb	42U	k.A.
	Eternus LT270 S2	LTO-8	138	2-20	1.536	2,7	FC 8Gb	42U	k.A.
HPE	StoreEver MSL 1/8 Tape Autoloader	LTO-6	8	1	20	0,6	SAS 6G/12G, FC 8Gb	1U	ab 3.000
www.hpe.com	StoreEver MSL 1/8 Tape Autoloader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 5.469
	StoreEver MSL 1/8 Tape Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 6.500
	StoreEver MSL 1/8 Tape Autoloader	LTO-9	8	1	144	2,2	SAS 6G/12G, FC 8Gb	1U	ab 7.990
	StoreEver MSL2024	LTO-6	24	1-2	60	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.260
	StoreEver MSL2024	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.500
	StoreEver MSL2024	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 9.400
	StoreEver MSL2024	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	k.A.
	StoreEver MSL3040	LTO-6	40	1-3	100	22,5	SAS 6G/12G, FC 8Gb	3U	ab 8.200
	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 8.500
	StoreEver MSL3040	LTO-9	40	1-21	720	22,5	SAS 6G/12G, FC 8Gb	3U	k.A.
	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 18.200
	StoreEver MSL6480	LTO-8	80	1-6	960	6,48	SAS 6G/12G, FC 8Gb	6U	ab 18.800
	StoreEver MSL6480	LTO-9	80	1-6	1.440	6,48	SAS 6G/12G, FC 8Gb	6U	k.A.
IBM	TS2900	LTO-5	9	1	13,5	0,3	SAS 6G	1U	ab 6.800
www.ibm.com	TS2900	LTO-6	9	1	22,5	0,6	SAS 6G	1U	ab 7100
	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 8.211
	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 6.570
	TS4300	LTO-8	40	1-3	480	3	SAS 6G, FC 8Gb	3U	ab 6.820
NEC	T30A	LTO-6	30	1-2	75 TByte	1,1	SAS 6G, FC 8Gb	2U	ab 5.066
www.nec.com	T30A	LTO-7	30	1-2	187,5	1,1	SAS 6G, FC 8Gb	2U	ab 5.600
www.starline.de	T60A	LTO-6	60	1-4	150	2,3	SAS 6G, FC 8Gb	4U	ab 6.866
	T60A	LTO-7	60	1-4	360	2,3	SAS 6G, FC 8Gb	4U	ab 7.300

Hersteller	**Produktname**	**Bandformat**	**Max. Tape-Slots/ Basiseinheit**	**Tape-Drives**	**Max. Kapazität** in TByte	**Transferrate in** TByte/h	**Schnittstellen**	**Formfaktor** (Rackmount)	**Nettopreis** (Euro)
Oracle	StorageTek SL4000	LTO-7	339	1-24	2.000	24,7	FC, Ficon	42U	ab 9.700
www.oracle.com/de/	StorageTek SL4000	LTO-8	339	1-24	4.000	29,7	FC, Ficon	42U	ab 10.500
	StorageTek SL8500	LTO-7	2.000	64	12.000	65,9	FC, FCoE, Ficon	42U	k.A.
	StorageTek SL8500	LTO-8	2.000	64	24.000	82,9	FC, FCoE, Ficon	42U	k.A.
Overland-Tandberg	NEOs StorageLoader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.100
www.overlandtandberg.com	NEOs StorageLoader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.350
	NEOs StorageLoader	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.806
	NEOs T24	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.100
	NEOs T24	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 5.450
	NEOs T24	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	k.A.
	NEOxl 40	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	ab 8.320
	NEOxl 40	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 8.500
	NEOxl 40	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	k.A.
	NEOxl 80	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 16.539
	NEOxl 80	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 16.910
	NEOxl 80	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 20.300
Qualstar	Q8	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 5.330
www.qualstar.com	Q8	LTO-8	8	1	96	1,1	SAS 6G, FC 8Gb	1U	ab 5.410
	Q8	LTO-9	8	1	144	1,1	SAS 6G, FC 8Gb	1U	ab 8.180
	Q24	LTO-7	24	1-2	144	2,2	SAS 6G, FC 8Gb	2U	ab 4.300
	Q24	LTO-8	24	1-2	288	2,2	SAS 6G, FC 8Gb	2U	ab 5.360
	Q24	LTO-9	24	1-2	432	2,2	SAS 6G, FC 8Gb	2U	ab 6.180
	Q40	LTO-7	40	1-3	240	3	SAS 6G/12G, FC 8Gb	3U	ab 6.480
	Q40	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 7.160
	Q40	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 8.100
	Q80	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 11.010
	Q80	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 12.100
	Q80	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 11.820
Quantum	Scalar i3	LTO-7	25-400	1-24	150	0,54	SAS 6G/12G, FC 8Gb	3U-24U	ab 10.020
www.quantum.com	Scalar i3	LTO-8	25-400	1-24	300	1,08	SAS 6G/12G, FC 8Gb	3U-24U	ab 11.188
	Scalar i3	LTO-9	25-400	1-24	450	1,62	SAS 6G/12G, FC 8Gb	3U-24U	ab 13.020
	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	Spectra T380	LTO-6	380	12	950	6.900	SAS 6G, FC 8Gb	24U	k.A.
spectralogic.com	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

Kombination von Disk- & Tape zur Systemplattform für Backup-to-Disk-to-Tape

actidata Ti-NAS 2200: Die Quasi-Standard-Datensicherungs-Plattform

Appliances geben dem Anwender eine Datensicherungslösung vor. Flexibilität, um die Backup-Strategie nach Vorgaben und Richtlinien umzusetzen, sind begrenzt. Jedoch wird diese Flexibilität vermehrt gefordert. Hier setzt actidata an und bietet mit actidata Ti-NAS eine Systemplattform an, die einen Windows-basierenden Server als NAS-System mit einer LTO-Tape Automation kombiniert, mit freier Wahl der Backup-Software.

■ Albrecht Hestermann, actidata

Ein 2U-Server und eine 2U-LTO-Tape-Library bilden die Systemplattform *actidata Ti-NAS 2200*. Mit der Kombination aus einem Festplattenspeicher bis zu 240 TByte Bruttokapazität und einer Bandbibliothek mit ein oder zwei LTO-Streamern (SAS) und 24 Medien-Stellplätzen bietet sich die Ti-NAS-2200-Plattform für den Einsatz im Rahmen einer Backup-to-Disk-to-Tape-Strategie (B2D2T) an. Anbindung an das vorhandene LAN erfolgt über optische 10-Gbit-Ethernet-Anschlüsse, so dass sich hier eine Datei-Freigabe als Backup-Ziel für die Backup-Jobs nutzen lässt. Das Übertragen der Daten von dem Festplatten-RAID auf die LTO-Tape-Library erfolgt innerhalb der Plattform, ohne das produktive Netz zu belasten.

Dank Windows Server IoT offen für die meisten Applikationen

Unterstützt werden alle gängigen Backup-, Datenmanagement- und Archiv-Software-Anbieter, wie beispielsweise *Arcserve*, *Archiware*, *Novastor*, *SEP*, *Veeam* und *Veritas BackupExec*. Mit der »IoT for Storage«-Variante des *Windows Servers* von *Microsoft* werden die Anforderungen für Storage bestens erfüllt. Nicht nur, dass für den externen Zugriff keine üblichen CALs hinzugekauft werden müssen, auch zwei Gast-Systeme lassen sich lizenzfrei betreiben. Darüber hinaus steht hier auch ein Server zur Verfügung, der im Fehlerfall für den schnellen Wiederaufbau der produktiven Server mit genutzt werden kann.

Konzeptmerkmale actidata Ti-NAS

- **Komplette Systemplattform** bestehend aus NAS und LTO-Backup
- **Freie Wahl** der Backup-, Archiv- oder Management-SW in eigener Regie
- **NAS-Server** mit Hardware-RAID optimiert für LTO-Tape Streamer
- **Ausschließlich Server-Komponenten** mit 10-Gbit-Ethernet, separate Gbit-Ethernet-Service-Schnittstelle
- **System-Plattform aus einer Hand:** Hauptsitz, Service, Support in Dortmund
- **Eine Bestell-Adresse – eine Artikelnummer:** Eine Service-Position für Server und LTO-Backup
- **36 Monate Gewährleistung** inklusive Vorabaustausch, optional bis 60 Monate erweiterbar

actidata Ti-NAS Tape-in-NAS Produktübersicht:

Ti-NAS 1000	1U Rackmount LTO-Tape Autoloader, 8 LTO-Stellplätze (Slots) + NAS- und Backup-Server in Rackmount-Ausführung (1U, 4 Bay/2U, 12 Bay/2U, 25 Bay/4U, 24 Bay)
Ti-NAS 2000	2U Rackmount LTO-Tape Library, 24 LTO- Stellplätze (Slots) + NAS- und Backup-Server in Rackmount-Ausführung (1U, 4 Bay/2U, 12 Bay/2U, 25 Bay/4U, 24 Bay)
Ti-NAS 3000	3U Rackmount LTO-Tape Library, 40 LTO- Stellplätze (Slots) + NAS- und Backup-Server in Rackmount-Ausführung (1U, 4 Bay/2U, 12 Bay/2U, 25 Bay/4U, 24 Bay)
Ti-NAS 6000	6U Rackmount LTO-Tape Autoloader, 80 LTO- Stellplätze (Slots) + NAS- und Backup-Server in Rackmount-Ausführung (1U, 4 Bay/2U, 12 Bay/2U, 25 Bay/4U, 24 Bay)
Ti-NAS RT	Integrierter LTO-Tape Streamer im NAS- und Backup-Server im 2U Rackmount-Gehäuse, 6 Bay
Ti-NAS QT	Integrierter LTO-Tape Streamer im NAS- und Backup-Server im Desktop-Gehäuse, 5 Bay

actidata Ti-NAS 2219 – Backup-Server mit 240 TByte Brutto-Kapazität und angeschlossener 24-Slot LTO-Tape-Library mit LTO-9 Laufwerken

Die Produktfamilie actidata Ti-NAS lässt sich frei konfigurieren und flexibel zusammenstellen, so wie es im Unternehmen konzeptionell am besten passt. Die Systemplattformen umfassen grundsätzlich einen Backup-Server inklusive eines Hardware-RAID-Controllers, der die Festplatten in einem performanten RAID-Set als Disk-basierenden Backup-Pool zur Verfügung stellt. Komplettiert werden die Systemplattformen mit Geräten der LTO-Bandtechnologie, die entweder als integrierter LTO-Streamer oder als angeschlossene LTO-Tape-Automation realisiert wird. Als Betriebssystem ist der Microsoft Windows Sever in der CAL-free-Version IoT-for-Storage installiert. Dank optischer dual 10-GbE-Schnittstellen sind Ti-NAS-Systeme auch entfernt von den Produktionssystem, beispielsweise in einem anderen Brandabschnitt, zu betreiben.

Ti-NAS-Plattformen von actidata sind ab sofort verfügbar. Selbstverständlich mit einer 3-jährigen Gewährleistung inklusive des bewährten *Fast Exchange Service* (Vorabaustausch defekter Komponenten). Die Konfiguration wird nach dem aktuellen Speicherbedarf nebst dem zu erwartenden Zuwachs sowie der Datensicherungsstrategie ermittelt.

Systeme mit einem LTO-Laufwerk und 100 TByte Festplattenkapazität starten mit einem empfohlenen Verkaufspreis von ca. 10.000 Euro, netto. Angebote werden individuell kalkuliert und auf Anfrage erstellt. ■

Weitere Informationen

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

Cloud-Backup allein ist nicht ausreichend

RDX für flexible Einsatzbereiche der Datensicherung

Moderne, heterogene Daten- und Anwendungsinfrastrukturen erfordern eine flexibel einsetzbare Technologie für die Datensicherung. Im Idealfall deckt sie sowohl die Anforderungen an Backup, Archivierung und Compliance ab. Für den richtigen Air-Gap bleiben hierfür Wechseldatenträger ein Muss. Die »Removable Disk Technology« (RDX) stellt dabei eine effiziente Alternative zu Bandlaufwerken dar.

■ Von Anja Scholl, Tandberg Data

Die gesetzlich von Unternehmen geforderte Konformität zu DSGVO, SEC17a-4(f), SOX, GoBD, StgB oder Basel III sowie die Ausbreitung von Schad-Software wie Ransomware verschaffen dem häufig vernachlässigten Thema Datensicherung neue Prominenz. Im Idealfall sollte die Datensicherung schnellen Datenzugriff auf Offline-Daten, das Backup für schnelle Wiederherstellung im Falle von Datenverlust sowie die Archivierung zur Einhaltung gesetzlicher Vorschriften gewährleisten. Wie aktuelle Studien zeigen, sind deutsche Unternehmen aber von der Zuverlässigkeit ihrer Backup-Technologie keineswegs überzeugt. Viele bezweifeln, dass ihre Backups vollständig gelingen oder eine komplette Wiederherstellung ermöglichen.

Foto: Overland-Tandberg

RDX-Lösungen sind als Einzellaufwerk oder Appliances verfügbar.

Cloud-only beim Backup überdenken

Es ist bekannt, dass Cyber-Kriminelle verstärkt Backup- und Sicherungsdaten im Visier haben. Gleichzeitig tendieren immer mehr Unternehmen zur Verlagerung ihrer kompletten Backup-Strategie in die Cloud, ob public oder private. Das birgt durchaus Risiken, wie prominente Fälle des Daten-Kidnapping und -Raubs auch bei Hostern, MSPs und Hyperscalern zeigen. Anwender müssen sich bewusst sein, Cloud-Backup bleibt auch immer ein Online-Backup. Auch Immutable-Lösungen ändern das prinzipiell nicht. Für die alte 3-2-1-(0)-Regel und damit des neuen Air-Gap, also die physische Trennung von Medien, sind nach wie vor Wechseldatenträger unabdingbar.

Tape oder RDX?

Backup und Archivierung sind zwar unterschiedliche Aufgaben, können aber sowohl durch die RDX- als auch die Tape-Technologie mit der aktuellen LTO-9-Generation effizient umgesetzt werden. Letztendlich bildet meist die Datenmenge die Entscheidungsgrundlage für die jeweilige Technologie.

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. Befolgt man die Idee der 3-2-1-Backup-Regel konsequent, so speichert man insgesamt drei Versionen der zu sichernden Daten auf zwei unterschiedlichen Technologien und lagert eine dieser Kopien extern.

Wechseldatenträger wie RDX sind aufgrund geringer Betriebskosten eine Option für beide Anwendungsfälle – Backup und Archivierung. Sie eignen sich auch auf

Grafik: Overland-Tandberg

Empfohlene Einsatzgebiete für HDD- und SSD-RDX-Medien.

Grund ihrer Flexibilität, Robustheit und einfachen Handhabung besonders für KMU und Mittelstand als Alternative.

Medienrotation und Archivierung mit einem System

RDX-Medien kombinieren die Portabilität und Zuverlässigkeit des Bandes mit der Geschwindigkeit einer Festplatte. Zu den Leistungsmerkmalen von RDX gehören Widerstandsfähigkeit und Robustheit: Das elektrostatisch geschützte und stoßfeste Design ermöglicht den Einsatz unterwegs, außerhalb des Standorts und für die räumlich getrennte Speicherung, die eine schnellere Notfallwiederherstellung ermöglicht.

HDD-Cartridges mit einer Lebensdauer von mehr als zehn Jahren kommen dabei heute in gängigen Festplattengrößen eher für die Archivierung zum Einsatz, während die neuen SSD-Varianten (von 500 GByte bis 8 TByte) eher für das schnelle Backup genutzt werden. Beide Medien-Typen sind vollständig rückwärts- und querkompatibel und können in allen RDX-Systemen eingesetzt werden.

Zur Anwendung kommen sie in Einzellaufwerken 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 ist für eine effektive Backup-Strategie mit Medienrotation geeignet.

Revisionssichere Archivierung

Neben dem reinen Schutz vor Datenverlust muss die Backup-Strategie die Einhaltung gesetzlicher Vorschriften gewährleisten. Beispielsweise müssen in Enterprise Content Management und Dokument-Management-Systemen 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 abrufbar 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 10 Jahre revisionssicher für die Betriebsprüfung vorzuhalten. Dazu ermöglicht der Einsatz eines speziellen WORM (Write Once Read Many)-Mediums zusammen mit der Bord-Software rdxLock WORM-Software die revisionssichere Archivierung von Geschäftsdaten nach HGB, GDPdU, GoBS, SOX und weiteren gesetzlichen Vorschriften, nach denen Dokumente unveränderbar gespeichert werden müssen.

RansomBlock: Schutz vor Ransomware

Ransomware hat sich zu einer großen Gefahr in der Cyberkriminalität für Unternehmen jeder Größe entwickelt. Eine funktionierende Backupstrategie 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 ande-

Weitere Informationen

Tandberg Data GmbH
Nikolaus-Groß-Straße 13
44329 Dortmund
Tel: +49 (0)231 5436-0
E-Mail:
salesemea@overlandtandberg.com
www.overlandtandberg.com

ren Computern und NAS-Systemen abgelegt werden.

Die WORM-Fähigkeit zusammen mit der integrierten AES-256-Hardware-Verschlüsselung bieten auch Schutz vor Ransomware-Attacken. Dazu setzt eine RansomBlock-Funktion zunächst alle Daten auf dem WORM-Medium in den »Nur Lese«-Modus. 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.

Für KMU optimiert

Für Unternehmen, die ihre bestehende LTO-Bandautomatisierung ersetzen, aber weiterhin gewohnte Datenmanagement-Verfahren nutzen möchten, kann RDX auch als Virtual-Tape-Library (VTL) integriert werden oder im Hybrid-Modus mit einer Kombination als Einzellaufwerk und Tape-Emulation in einem Gerät genutzt werden.

In Summe ist die RDX-Technologie damit optimiert für die Geschäftskontinuität kleiner und mittelständischer Umgebungen und ermöglicht eine einfache Sicherung und Notfallwiederherstellung mit Medienrotation. ■

Actidata

Die actidata Storage Systems GmbH mit Sitz in Dortmund ist ein innovativer IT-Hersteller mit Schwerpunkten im Bereich Backup, Storage und Archivierung. Das Unternehmen konzentriert sich mit einem Netzwerk professioneller Systemhäusern auf das Industrie- und Geschäftskundensegment mit dem Ziel, professionelle Speicherlösungen zu platzieren.

Sitz der Gesellschaft:
Dortmund

Niederlassung in Deutschland:
Dortmund

Jahr der Gründung:
2009

Zielgruppe:
Systemhäuser, VARs und Industriekunden

www.actidata.com

NovaStor

Als deutscher Hersteller und Lösungsanbieter entwickelt NovaStor Software für Backup, Restore und Archivierung und entlastet IT-Abteilungen mit Dienstleistungen von der initialen Konzeption bis in den laufenden Betrieb. Mit bewährten Datensicherungs- und Archivierungslösungen schützt NovaStor Daten auf sämtlichen Speichertechnologien von Disk über Tape bis Cloud. NovaStor ist inhabergeführt und entwickelt seine Lösungen zu 100% in Deutschland.

Sitz der Gesellschaft:
Hamburg

Niederlassung in Deutschland:
Hamburg

Jahr der Gründung:
1987

Zielgruppe:
Systemhäuser, VARs, KMUs und Industriekunden

www.novastor.de

N-TEC GmbH

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 revisionssichere 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.

Sitz der Gesellschaft:
Ismaning

Jahr der Gründung:
2001

Zielgruppe:
Vor allem KMU + öffentliche Auftraggeber

www.n-tec.eu

Quest Software

Quest entwickelt Software-Lösungen, um die Vorteile neuer Technologien in einer zunehmend komplexen IT-Umgebung nutzbar zu machen. Das Unternehmen hilft seinen Kunden, ihre nächste IT-Herausforderung zu bewältigen, von Datenbank- und System-Management über die Verwaltung von Active Directory und Office 365 bis hin zum Schutz vor Cyberbedrohungen.

Sitz der Gesellschaft:
Cork, Ireland

Niederlassung in Deutschland:
Köln

Jahr der Gründung:
1987

Zielgruppe: **Systemhäuser, VARs, KMUs und Industriekunden**

www.quest.com/de-de/

Die neue Komplexität der Datensicherung

Backup-to-Disk: Zentrales Element der modernen Datensicherung

Schon mehrfach wurden verschiedene Technologien, die zur Datensicherung eingesetzt werden, für »tot« erklärt. Neben dem Dauerbrenner Tape ging es auch der Festplatte immer wieder an den Kragen. Flash-Storage werde alles ersetzen, Disk-Backups gehörten der Vergangenheit an. Die Realität sieht anders aus: Disk-Backups gewinnen an Bedeutung und helfen, Kosten und Aufwand von Flash-Speichern und »last line of defense«-Technologien zu reduzieren.

■ Hannes Heckel, FAST LTA

Durch die verstärkte Bedrohung durch Ransomware und Cyberangriffe hat sich der Fokus vom reinen Backup (also der Sicherung) hin zur Datensicherung mit schnell und sicher funktionierendem Recovery verschoben. Dadurch steigt die Komplexität im Storage-Bereich. Neben dem klassischen Backup-to-Disk sorgt Backup-to-Flash dafür, dass moderne Technologien wie Continuous-Data-Protection (CDP), Forever-Incrementals und Instant-Recovery zum niedrigen RTO beitragen können.

Auch Backup-to-(Virtual)-Tape erlebt einen unerwarteten Höhenflug, freilich unter neuem Namen: Air-Gap. Physisch aus dem System entnehmbare Medien gelten als Wunderwaffe gegen die Folgen eines Ransomware-Angriffs, sind sie doch zu 100 Prozent vor manipulativem Zugriff geschützt. Und zur günstigen Ablage großer Datenmengen wie zum Beispiel Backup-Archiven sollen Online-Speicher dienen, in denen Daten zusätzlich durch Immutability geschützt werden können.

Verlassen Sie sich nicht nur auf Air-Gap und Immutability

Es gibt verschiedene Technologien, Daten vor unerlaubtem Zugriff und so vor Manipulation zu schützen. Am bekanntesten ist Air-Gap, was oft mit Tape gleichgesetzt wird. Inzwischen gilt auch das Prinzip der Immutability auf einem entfernten Server »in der Cloud« als betrachtenswerte Alternative zum Air-Gap. Auch ein per Hardware-WORM versiegeltes Archiv kann diese Funktion erfüllen.

Dennoch werden diese Technologien nicht umsonst als »last line of defense« betrachtet, also als allerletzte Möglichkeit der Wiederherstellung von Daten. Dies ist jedoch nicht die Lösung für die Gefahr durch Cyberangriffe, da auf solchen »kalten« Medien meist ältere Datensätze abgelegt werden, die zudem in der Regel nicht unmittelbar für einen Restore zur Verfügung stehen. Tape-Archive sind rein linear und erfordern beim Erstellen und beim Restore hohen manuellen und zeitraubenden Aufwand. Cloud-Archive sind per Definition nicht lokal verfügbar. Im Fall eines Cyberangriffs sollte die Verbindung zum Internet als erstes gekappt werden, was auch den Zugriff auf diese Daten verhindert.

Da der Ausfall der IT den größten Kostenblock bei einem erfolgten Ransomware-An-

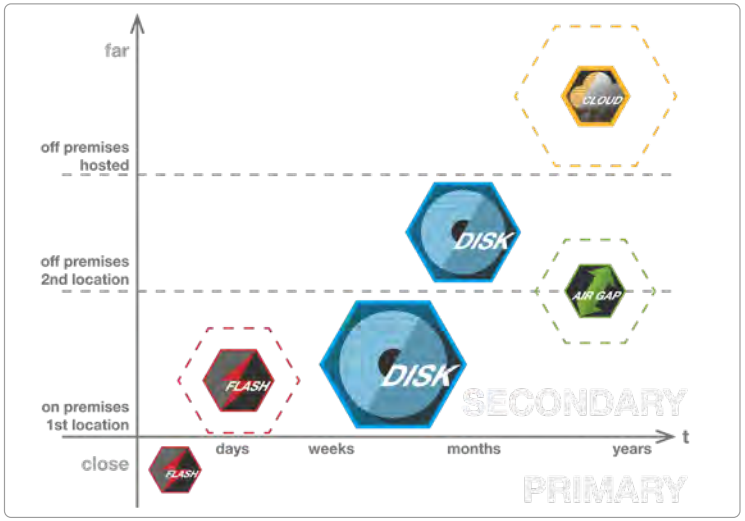


Bild: FAST LTA

Sollte ein Cyberangriff gelingen, muss die »last line of defense« greifen. Ausschließlich auf Air-Gap und Immutability sollten sich IT-Manager aber nicht verlassen.

griff darstellt, helfen diese schlecht zugänglichen Archive kaum, die Folgen einer solchen Attacke zu mindern. Sie sind tatsächlich eben nur als allerletztes Mittel zu sehen, wenn alle anderen Daten verloren sind.

Die Zentrale: Backup-to-Disk

Disk-Backups gibt es seit Jahrzehnten, um Daten schnell zu sichern und auf gesicherte Daten schnell und wahlfrei zugreifen zu können. Durch stark angestiegene Datenmengen reichen herkömmliche RAID-Speicher nicht mehr aus. Moderne Disk-Arrays müssen quasi unbegrenzt skalierbar sein, ohne dass Änderungen an der Konfiguration notwendig sind (Scale Up).

Die Reduzierung der aufwändigen letzten Instanz gelingt aber nur, wenn beim Disk-Backup umfassende Maßnahmen zur Absicherung gegen Ausfall und Angriffe durchgeführt werden. Immer stärker wird nämlich die Bedrohung durch gezielte Angriffe, die zunächst – oft über Monate – die IT-Infrastruktur ausspähen und dann zuerst versuchen Backups unzugänglich zu machen. Sollte das gelingen, muss tatsächlich die »last line of defense« greifen. Damit es nicht so weit kommt, gibt es mehrere Maßnahmen zum Schutz des Disk-Backups.

1. Zugang erschweren: Zu oft haben normale Netzwerk-Admins oder gar »Chefs« Zugriff auf Backup-Server, meist durch die Integration in die Standard-Authentifizierung per Active Directory (AD). Dies stellt die offensichtlichste Sicherheitslücke dar. NAS-Speicher für Backups sollten nicht direkt als Laufwerke, sondern über geschützte UNC-Pfade eingebunden werden. Der Zugang zu allen Backup-Maschinen sollte nicht per AD erfolgen, sondern per Mehr-Faktor-Authentifizierung geschützt sein.

2. Automatische, unzugängliche Snapshots: In regelmäßigen Abständen sollte das Backup-Storage selbständig Snapshots erstellen, die nur vom System und nach Ablauf der eingestellten Aufbewahrungsdauer gelöscht werden können. Die Häufigkeit und Dauer müssen so eingestellt werden, dass sie höchstmögliche Sicherheit bei gerade noch vertretbarer Auslastung ermöglichen. Da Angreifer sich oft mehrere Wochen im IT-System »umsehen«, sollte die Aufbewahrungsdauer möglichst lang gewählt werden. Auch die Auslagerung von Snapshots, beispielsweise auf Air-Gap-Medien oder Cloud-Storage hängt von diesen Einstellungen ab.

3. Geo-Redundanz: Zum Schutz vor Ausfall ganzer Instanzen bzw. Standorte sollten Backups auf einen zweiten Standort repliziert werden, möglichst durch rein im Storage verankerte Funktionen, die nicht im normal zugänglichen Netzwerk liegen. Der Datenspeicher am zweiten Standort darf, außer zum Zweck der Replizierung, nicht vom Hauptnetzwerk erreichbar sein.

Da es zur Optimierung der RTO (schnellstmögliche Wiederherstellung) notwendig ist, dass die Datensicherung dort stattfindet, wo die Daten auch anfallen bzw. wieder benötigt werden, sollte dieser zentrale Backup-Bereich On-Premises, also vor Ort, realisiert werden.

Das geht doch auch mit Flash-Storage...?

Flash-Storage ist schnell, aber eben auch teuer – (immer noch) deutlich teurer als Festplatten-Speicher. Beim Primary-Storage gilt Flash inzwischen als gesetzt. Bei einzelnen Instanzen mit begrenzter Kapazität ist der Geschwindigkeitsvorteil höher zu bewerten als die höheren Kosten.

Anders sieht es bei Implementation der oben ausgeführten Sicherheitsmaßnahmen aus. Werden diese auch auf dem Primary-Target, dem Flash-Storage durchgeführt, multipliziert sich die Kostendifferenz im Vergleich zu Festplattenspeicher. Die längere Speicherdauer und dadurch notwendige Kapazität tut dazu ihr Übriges, um die Kosten in Bereiche zu treiben, die in keinem Verhältnis zum erzielbaren Geschwindigkeitsvorteil stehen. Eine direkte Auslagerung langfristiger Backups via Air-Gap oder Cloud-Storage ist aus den eingangs beschriebenen Gründen nicht zielführend, was RTO und RPO betrifft.

Fazit: Investieren Sie in sicheres Disk-Backup

Zusammenfassend lässt sich feststellen: Je sicherer und umfassender der zentrale Bereich des Backup-to-Disk realisiert wird, desto weniger Aufwand muss in schlecht verfügbare und unter Umständen mit hohem manuellem Aufwand behaftete Zusatztechnologien investiert werden. Der Bereich des Primary-Target – Flash-Storage – kann so groß wie notwendig und so klein wie möglich gewählt werden, was Kosten und Zusatzaufwand reduziert. Da Angriffe vermehrt gezielt zunächst die Backup-Infrastruktur attackieren, müssen Disk-Backups nicht nur gegen Datenträgerausfälle, sondern auch gegen diese Angriffe besonders geschützt werden. ■

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
» Downloads und Hintergrund-Informationen

Lokaler Objektspeicher mit N-TEC rapidCore SWARM

On-Premises-Backup für mehr Sicherheit

Wachsende Datenmengen insbesondere durch unstrukturierte Daten verlangen nach neuen, effizienten Backup-Lösungen. Magnetband ist zwar günstig, aber schwer handzuhaben und nicht sofort abrufbar. In einer Public-Cloud sind die Kosten auf Dauer schwer kalkulierbar und Performance sowie Datenschutz oft unwägbar. Die zeitgemäße Alternative ist ein lokaler S3-Objektspeicher für lokale und Private-Cloud Umgebungen.

■ Sven Meyerhofer, N-TEC

Die Nachfrage von On-Premises S3-Speicherlösungen in einer Private-Cloud steigt. Der Grund ist, dass mit der Digitalisierung und den wachsenden Datenmengen auch der Wert der Daten für Unternehmen permanent steigt. Gleichzeitig verlangen äußere Bedrohungen wie Ransomware oder innere Gefahren wie Bedienfehler oder Hardware-Ausfälle ein absolut konsistentes, performantes Backup, das unter Kontrolle und jederzeit verfügbar ist.

Herausforderung Backup

Herkömmliches Tape oder der Gang in die Public-Cloud können aktuelle Anforderungen jedoch kaum mehr abbilden. Ersterem widerspricht die Zugriffsgeschwindigkeit und das zum Teil komplexe Datenmanagement, die beispielsweise die Nutzung als aktives Archiv kaum möglich macht. Zweiterem, der Public-Cloud, steht nicht nur die unwägbare und kostspielige Performance in einer externen Infrastruktur entgegen, sondern auch unkalkulierbare Kosten bei der Wiederherstellung oder anderweitigen Nutzung (KI, Analytics) entgegen. Was also tun?

Moderne Unternehmen müssen sich folgende Fragen stellen:

- **Ransomware:** Wie können Unternehmen im Falle eines Angriffs den Schutz Ihrer Daten sicherstellen?
- **Backup-Daten:** Wie gewährleisten Unternehmen, dass Daten nicht manipuliert werden und jederzeit für eine Wiederherstellung zur Verfügung stehen?
- **Handhabungsfehler:** Können Daten verlässlich vor versehentlichem Löschen und Verfälschung geschützt werden?
- **Hardware-Fehler:** Können verloren gegangene Daten des betroffenen Speichers, Servers oder Standorts wiederhergestellt werden?
- **Archiv:** Kann die Integrität der Daten sichergestellt werden?

Hardware: schlüsselfertig – skalierbar – sicher

N-TEC, Storage-Hersteller aus Ismaning, beantwortet diese Fragen an Backup und Archivierung mit seiner neuen *rapidCore SWARM*-Serie. Sie bündelt Hardware-Plattformen aus eigenem Haus mit der Objektspeicher-Plattform *SWARM* von **DataCore**.

Hardware-seitig skaliert rapidCore SWARM von 24- bis 74-Bay-Systemen in einer Scale-out Architektur. Wie von einer Objektspeicher-Lösung zu erwarten, skalieren die Backup- und Archiv-Speicher bis in den PByte-Bereich. Aber auch spezielle Konfigurationen für kleinere und mittlere Unternehmen ab 50 TByte stehen rentabel zu Verfügung.

Software-defined: Backup und Archiv in Einem

Software-definierter Objektspeicher wie Datacore Swarm beinhaltet zahlreiche spezielle Sicherheitsfunktionen und schützt Daten vor dem Zugriff durch Angreifer. Mit

mehrschichtigen Sicherheits-, Verschlüsselungs-, Unveränderbarkeits- und Replikationsfunktionen schützt Swarm Daten zuverlässig vor Verletzungen durch interne und externe Parteien.

Auch der klassische Einsatz von WORM-Medien (Write Once Read Many) mit dazugehörigen Systemen wird damit quasi obsolet. *S3 Object Lock* und andere Technologien zur Sicherstellung der Unveränderbarkeit der Daten sorgen dafür, dass Insel-Lösungen speziell für Backup und Archivierung nicht mehr isoliert betrieben, verwaltet, gewartet und letztlich gekauft werden müssen.

Das leistet Software-defined Objektspeicher:

- Unveränderbarkeit (Immutability/ WORM) der Daten durch S3-Objektsperrung verhindert die absichtliche oder versehentliche Änderung oder Löschung von Daten
- Kein Dateisystem, keine Login-Shell und keine ausführbaren Dateien, sodass dadurch keine Angriffsfläche geboten wird
- Keine Administration der Speicherknoten verringert die Gefahr von Social-Engineering-Angriffen
- Automatisierte Replikation an einen sekundären Standort ermöglicht logisches oder physisches Air-Gapping – gewährleistet eine vollständige Isolierung
- Aktivitätsprotokollierung und Hashing, um potenzielle Angreifer aufzudecken und zu prüfen, ob Daten manipuliert wurden
- Verschlüsselung »in-flight« und »at-rest« verhindert unbefugtes Lesen des Inhalts

Scale-out mit Hochverfügbarkeit

rapidCore SWARM ist als Scale-out-Architektur beliebig erweiterbar und arbeitet in einer Cluster-Konfiguration nach dem Schema n+1 beim Bedarf der Erweiterung. Der Datenzugriff erfolgt dabei innerhalb des Intranets oder gesicherte WAN-Verbindung über S3, http oder NFS. Unterstützt wird neben synchroner Redundanz auch Replikation. Erasure-Coding sorgt dafür , dass die Systeme über verschiedene Brandabschnitte oder auch georedundant über diverse Standorte verteilt werden können.

Der paritätsbasierte Datenschutz durch Erasure-Coding bietet darüber hinaus eine hohe Verfügbarkeit und bewirkt, dass bei gleichzeitigem Ausfall von mehreren Festplatten oder eines Speicherknotens, alle weiteren Server des rapidCore SWARM Clusters, parallel an der Wiederherstellung des Gesamtsystems arbeiten.

Einsatzbereiche: Wer braucht das?

Enterprise-IT: Im Unternehmen werden die Lösungen als kostengünstiger Sekundärspeicher, oft auch in Verbindung zur Hybrid-Cloud als zusätzliche Instanz, eingesetzt. Backup und Disaster-Recovery mit schnellem Zugriff sind der Einsatzbereich.

Medien und Unterhaltung: Unstrukturierte Datenmengen wachsen massiv durch Video-on-Demand und Streaming, die als aktives Archiv kostengünstig abrufbar sein sollen.

Gesundheitswesen: Medizinische Aufnahmen und elektronische Krankenakten belasten die ohnehin engen Budgets im Gesundheitswesen. Hier dient der Objektspeicher als herstellerneutrales Archiv.

Automotive / IoT: Autonome Fahrzeugdaten und Fahrdatenspeicher belasten Performance und Kapazitäten von Herstellern, Entwicklern und Zulieferern. Der Objektspeicher wird zunehmend zur erweiterter Analyse (Deep Analytics) genutzt.

High Performance Computing (HPC): Dort müssen Geodaten und Mandantenmanagement mit Multi-Protokollzugriff verwaltet werden.

Öffentliche Einrichtungen: In angespannten Budget-Lagen ist der öffentliche Auftrag, Information und Asservate zur Verfügung zu stellen, personenbezogene Daten gleichzeitig zu schützen und bereit zu stellen. Auch die Videoüberwachung muss gegebenenfalls sichergestellt werden.

Objektspeicher »Made in Germany«

Der große Vorteil der N-TEC-Lösung ist, dass der Kunde hier eine maßgeschneiderte skalierbare Gesamtlösung »Made in Germany« inklusive Servicekonzept aus einer Hand erhält und somit auch eine feste Ansprechperson im Post-Sales hat.

rapidCore SWARM findet neben Backup seinen Einsatz auch im Bereich der Archivierung und überall dort, wo ein (Private-) Cloud-Speicher benötigt wird. Das Scale-out-Konzept erlaubt jederzeit eine bequeme Erweiterung des Clusters ohne großen Administrationsaufwand. Schlüsselfertige Komplettlösungen inklusive Installation mit Erasure-Coding und 100 TByte Nutzkapazität sind je nach Konfiguration und Service-Level ab 40.000 Euro (netto) erhältlich. ■

Weitere Informationen

N-Tec GmbH
Oskar-Messter-Str. 14, 85737 Ismaning
Tel.: + 49 (0)89 – 95 84 07-0
www.n-tec.eu/service/hosting-und-cloud/datacore-swarm/

Rechtliche Aspekte beim Einsatz von Backup-Software

Vorsicht vor Datenschutzverletzungen

Unternehmen sind per Gesetz zur Datensicherung verpflichtet. Zur Einhaltung dieser Pflicht ranken sich einige Mythen. Die DSGVO verlangt ausdrücklich, dass Daten wiederhergestellt werden müssen. Die ebenfalls verpflichtende Datensparsamkeit schränkt aber die Anzahl der Sicherungskopien nicht ein. Vorsicht ist geboten, wenn Support-Fälle aus einem Nicht-EU-Land bearbeitet werden. Hier droht eine mögliche Datenschutzverletzung.

■ Karl Fröhlich

In Unternehmen gehört eine Backup-Software zum Standard. Für Aktiengesellschaften besteht laut § 91 Akt.2 AktG eine Pflicht zur Datensicherung. Diese Norm wird auch für andere Unternehmensformen, wie GmbH und Personengesellschaft abgeleitet. Die Geschäftsleitungen und Vorstände haften nach den gleichen Grundsätzen. Speziell für personenbezogene Daten fordert die DSGVO ebenfalls ein angemessenes Sicherheitsniveau. Art. 32 Abs. 1 lit. c DSGVO verlangt »die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.«

Bild: via Canva Pro

Wie diese Sicherheit herzustellen ist, obliegt den Unternehmen. Die Gesetze verlangen technische und organisatorische Maßnahmen (TOMs) nach dem Stand der Technik, geben aber keine Handlungsanweisungen vor.

Backup und die DSGVO

Die DSGVO verlangt zwar eine Datensparsamkeit, Backups gelten aber als unverzichtbar. Diesbezüglich gibt es kein Limit für mögliche Kopien und Aufbewahrungsfristen. Ebenso ist immer wieder zu lesen, dass die Löschpflicht verlangt, personenbezogene Daten auch aus Backups zu entfernen. Das ist so nicht richtig und in der Praxis auch nicht sinnvoll durchführbar. Sicherzustellen ist, dass Daten, die aus welchem Grund auch immer zu löschen sind, bei einer möglichen Rücksicherung nicht mehr in den aktiven Kreislauf zurückkehren und kein Anwender darauf zugreifen kann.

Festzuhalten ist dies in einem Datensicherungs-Konzept. Hier lautet der Rat der Experten, »dokumentieren Sie alles möglichst detailliert und umfassend«. Auch sollten Maßnahmen begründet werden, vor allem, wenn man zum Beispiel auf Produkte von US-Anbietern zurückgreift, obwohl es EU-Alternativen gibt. Sollte tatsächlich eine Da-

tenschutzverletzung auftreten, kann das Unternehmen so belegen, welche Maßnahmen getroffen wurden und aus welchen Gründen. Wer sich ausreichend Gedanken gemacht und nicht fahrlässig gehandelt hat, muss in der Regel keine Strafen befürchten. Die Aufsichtsbehörden können aber die getroffenen Maßnahmen als ungeeignet oder verbesserungswürdig erachten und eine Änderung anordnen.

Support: Vorsicht vor Datenschutzverletzungen

Vorsicht ist auch beim Support geboten: Bei Updates und technischen Problemen ist es gängige Praxis, dass dem Anbieter ein Remote-Zugriff auf die Backup-Umgebung gewährt wird. Befinden sich die Techniker bzw. Server des Anbieters nicht in der EU, findet eine Übertragung in ein Drittland statt. Die DSGVO stellt hier einige Anforderungen, in punkto Sicherheit, Verträge und Dokumentation.

Aus Datenschutzsicht gelten beispielsweise Indien und die USA nicht als sicheres Drittland. Deutsche Unternehmen müssten sich im Prinzip davon überzeugen, dass in den jeweiligen Ländern ein angemessenes Datenschutzniveau eingehalten wird. Dies ist aber kaum möglich, auch nicht mit den neuen EU-Standardvertragsklauseln. Nun darf man davon ausgehen, dass die Herstel-

Bild: via Canva Pro

ler von Backup-Programmen vertrauenswürdig sind und keine unlauteren Absichten hegen. Trotzdem entstehen offene Tore (Ports), die auch ein Einfallstor für Cyberangriffe sein können.

Die deutschen Alternativen lauten beispielsweise **NovaStor** und **SEP**. Produktentwicklung und Support kommt bei beiden Herstellern komplett aus Deutschland.

»Daten und Logfiles gelangen im Unterstützungsfalle nicht außerhalb von Deutschland und auch die Dateneinsicht beispielsweise bei *TeamViewer*-Sessions durch den SEP-Support bleibt komplett in Deutschland, so dass auch hier Compliance und DSGVO-Anforderungen gewahrt bleiben«, bestätigt **Andreas Mayer**, Senior Marketing Manager bei SEP, gegenüber **speicherguide.de**. »Ebenfalls arbeiten wir mit deutschen und europäischen MSP-Partnern zusammen, so dass auch hier keine Probleme wegen dem abgekündigten Privacy-Shield-Abkommen entstehen. Das heißt, die Daten landen nicht in den USA oder anderen nicht-europäischen Ländern. Denn auch bei der Beauftragung eines MSPs ist der Auftraggeber verantwortlich, dass die Richtlinien zur Datenhaltung (DSGVO) eingehalten werden und die Verantwortung kann nicht auf den MSP abgegeben werden.«

Backup-Software: Risiko Backdoors

Etwas worüber kontrovers diskutiert wird, sind sogenannte Backdoors. Hintertürchen, die von Herstellern im Auftrag der Regierung eingebaut werden. So gilt es beispielsweise als erwiesen, dass es in den Netzwerkgeräten von *Juniper* eine NSA-Hintertür gibt oder zumindest gab. Bereits 2015 hatte ein anderer Staat, vermutlich China, diese Backdoor ausgenutzt.

Bisher sind keine Fälle bekannt, die darauf schließen lassen, dass in Backup-Anwendungen Hintertüren eingebaut sind. Die Behauptung, US-Firmen wären per Gesetz dazu verpflichtet Backdoors zu implementieren stimmt so übrigens nicht. Was eher zutrifft, Schlüssel zur Entschlüsselung zu hinterlegen bzw. verschlüsselte Daten entschlüsselbar zu machen. Mit dem sogenannten *Lawful Access to Encrypted Data Act* (LAED) würde dies zwar verpflichtend, dieser ist aber noch nicht in Kraft. Der Gesetzesentwurf wird selbst in den USA sehr kritisch gesehen und derzeit sieht es nicht danach aus, als ob es das Gesetz in näherer Zukunft durch die Gremien schaffen wird.

Vor diesem Hintergrund ist der Einsatz einer aus den USA stammenden Backup-Software weiterhin legitim. Entscheidend ist, ob der Backup-Dienst dem Kunden die Möglichkeit gibt, einen eigenen ›Key‹ zur Verschlüsselung zu nutzen und sich dieser Key auch nicht vom Anbieter auslesen lässt.

»Wenn das sichergestellt ist, spricht aus rein rechtlicher Sicht nicht viel gegen den Einsatz von Diensten im Drittland«, erklärt der auf Datenschutz und IT-Recht spezialisierte Rechtsanwalt ist **Stephan Hansen-Oest**. »Die Daten sind für das Unternehmen aber immer noch personenbezogene Daten, trotz Verschlüsselung, deswegen müssen dennoch zum Beispiel EU-Standardvertragsklauseln abgeschlossen werden. Das nach Klausel 14 der EU-Standardvertragsklauseln vorzunehmende *Transfer Impact Assessment* kann dann aber positiv ausfallen, weil die Daten ›Ende-zu-Ende‹-verschlüsselt sind.« ■

Rechts- und Datenschutz-konforme Data-Protection

Datensicherung: Baustein der digitalen Souveränität Deutschlands

Cyberanschläge ohne Datenverlust und lange Ausfälle überstehen: Verhindern lassen sich Cyberattacken kaum, aber mit Lösungen aus Deutschland können Sie Ihre Datensicherung krisensicher machen und ein durchdachtes, effizientes IT-Risikomanagement aufsetzen. Wie können Backup und Restore in diesem Spannungsfeld helfen?

■ Stefan Utzinger, NovaStor

Im Kontext des russischen Angriffskrieges befürchtet die Bundesregierung russische Cyberangriffe, insbesondere auf Behörden und Unternehmen der kritischen Infrastruktur. In Sicherheitskreisen gelten Cyberangriffe als ernstzunehmende Bedrohung für Wohlstand und Freiheit. Experten raten daher, im Hinblick auf die Technologiesouveränität, bei IT-Sicherheitsprodukten auf lokale Alternativen zurückzugreifen.

Cyberangriffe lassen sich kaum verhindern, aber eine gute Backup-Lösung als letzte Verteidigungslinie kann den Schaden in Grenzen halten und dafür sorgen, dass die Unternehmen schnell wieder operativ arbeiten können. Damit der mögliche Schaden nicht den IT-Verantwortlichen zur Last gelegt wird, sollte bei der Auswahl der Datensicherung generell auf Folgendes geachtet werden:

Deutscher Hersteller

Eine lokale Lösung mit deutschen AGB und EULA sichert eine rechtskonforme Datensicherung sowie die Einhaltung der Datenschutzgesetze. So sind Kunden wie Partner zu jeder Zeit rechtlich abgesichert, im Normalbetrieb wie in der Notfallsituation.

Im Notfall sind der lokale technische Support, schnelle Reaktionen und kurze Kommunikationswege sowie der Zugriff auf die Entwicklungsabteilung des Backup-Herstellers entscheidende Kriterien. Denn Datensicherungs-Software erfüllt nur dann ihr Ziel, wenn verloren gegangene Daten sich schnell und sicher wiederherstellen lassen.

Wenn ein Unternehmen allen Schutzmaßnahmen zum Trotz von einem Ransomware-Angriff betroffen ist, braucht es sofortige und kompetente Hilfe – optimalerweise von einem deutschsprachigen und lokalen Team. So geht keine wertvolle Zeit verloren.

Ganzheitliche Lösung

Datensicherung muss ganzheitlich gedacht werden: vom Backup-Konzept, über einen aktuellen IT-Notfallplan bis zum Betrieb der Lösung. Zur Entlastung der IT-Abteilungen und Systemhäuser muss der Hersteller der Backup-Lösung einen Rund-um-Service bieten und Verantwortung für die Datensicherung übernehmen. Dazu gehört neben dem Angebot von Managed-Backup auch eine Cloud-Sicherung.

Modernes Produkt

Im Zentrum einer professionellen Datensicherung steht ein modernes und leistungsfähiges Produkt: *NovaStor DataCenter* bietet eine professionelle Komplettlösung für physische und virtuelle Systeme. NovaStor DataCenter ermöglicht, dass alle Backup Jobs in nur einer Oberfläche verwaltet und die Daten lokal oder in die Cloud gesichert werden können.

NovaStor steht für 100 Prozent Zuverlässigkeit sowie garantierte Datensicherung und -wiederherstellung. ■

Weitere Informationen

NovaStor GmbH
Neumann-Reichardt-Str. 27-33,
22041 Hamburg
Tel. +49 (0)40/63809 0
E-Mail: kontakt@novastor.de
www.novastor.de

Gesetzeskonformes Auditing für hybride Microsoft-Umgebungen

Sicherheitsrisiken proaktiv erkennen und minimieren

Gesetzeskonforme IT-Audits in Echtzeit für Microsoft Windows-Umgebungen sind elementarer Bestandteil einer Sicherungsstrategie im modernen Unternehmen. Die Berichterstellung im Hinblick auf Änderungen und die Zugriffsprotokollierung für Active Directory (AD), Office 365 und andere Unternehmensanwendungen können jedoch aufwendig, langwierig und in einigen Fällen mit nativen IT-Prüf-Tools unmöglich sein.

■ Stefan von Dreusche, Quest

Die Verwendung von nativen Audits in einer Windows-Umgebung ist zwar nützlich, aber weder umfassend noch intuitiv genug, um Audits in Echtzeit zu ermöglichen, was bei der weiteren Umstellung wichtige Sicherheitsbedenken aufwirft. Dies führt oftmals zu Datensicherheitsverletzungen und zu Insider-Bedrohungen, die ohne entsprechende Sicherheitsmaßnahmen unter Umständen nicht erkannt werden.

Bedrohungen proaktiv verhindern

Im Idealfall kann eine Audit-Lösung proaktiv über Gruppenänderungen und Zugriffe informieren. Der *Change Auditor* von **Quest** bietet dafür IT-Prüfungen in Echtzeit, eingehende Analysen und umfassende Sicherheitsüberwachung für alle wichtigen Änderungen durch Benutzer und Administratoren in *Microsoft Windows*-Umgebungen.

Diese Funktionalität erlaubt es einem Administrator oder einer Sicherheitsabteilung, Active-Directory-Objekte wie Gruppen, Attribute oder GPO's zu auditieren. IT-Verantwortlich können so verdächtige Bewegungen im Active Directory einschränken.

Ransomware frühzeitig identifizieren und ausschalten

Der Befall durch Schad-Software ereignet sich oftmals Wochen und Monate vor die eigentlich Attacke ausgeführt wird. Um dem vorzubeugen, verfügt der Change Auditor über die Fähigkeit, Object-Protection zu implementieren. Die Sicherheitsabteilung kann Gruppenmitgliedschaften aktualisieren oder im Notfall sperren, wobei aufgelistet wird, wer versucht hat, die Änderung vorzunehmen, welche Änderung versucht wurde, wann der Versuch unternommen wurde und von wo aus der Versuch unternommen wurde. Und zwar bevor die Attacke erfolgreich war.

On-Demand Audit für hybride Umgebungen

Für erhöhte Sicherheitsanforderungen sollte die Berichterfassung und -bereitstellung nicht nur On-Premises, sondern auch in der Cloud vorgehalten werden. Dafür kann die *Quest On-Demand Audit Hybrid Suite* genutzt werden.

On Demand Audit ist eine in *Azure* gehostete SaaS-Lösung, die Transparenz und Einblick in alle Konfigurations-, Benutzer- und Administratoränderungen in *AD*, *Azure AD*, *Exchange Online*, *SharePoint Online*, *OneDrive for Business* und *Teams* bietet. Damit kann der Audit-Verlauf für bis zu zehn Jahre On-Demand gespeichert werden.

Die Integration mit Change Auditor reduziert nicht nur den Bedarf an einer On-Premises-SQL-Datenbank zur Speicherung von Change-Auditor-Ereignissen, sondern gibt auch einen vollständigen Überblick über alle zugehörigen hybriden Audit-Informationen in einer einfach zu bedienenden Webkonsole. ■

Weitere Informationen

Quest
Im Mediapark 4e, 50670 Köln
E-Mail: infomail.ireland@quest.com
www.quest.com/de-de/
Quest Change Auditor
Quest On Demand Audit

Marktüberblick Backup-Software

Backup & Recovery für Mittelstand und Enterprise

Die Auswahl an Backup-Software für Mittelstands- und Enterprise-Umgebungen ist über die Jahre beachtlich gewachsen. Neben der Hardware sind die richtigen Programme von entscheidender Bedeutung um die Anforderungen an moderne Datensicherung im Rechenzentrum zu erfüllen. IT-Manager haben die Wahl zwischen Spezialisten und umfangreichen Plattform-Produkten, die zunehmend als Abomodell zu erwerben sind.

■ Michael Baumann

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 Jaglion
Veeam	V11A
Veritas	NetBackup

Natürlich steht dabei 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-Librarys, 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. Die meisten Anbieter scheuen die Angabe von Preisen, um eine Vergleichbarkeit zu vermeiden. Die offizielle Begründung lautet freilich, dass die Anforderungen der Unternehmen zu unterschiedlich sind. Unsere Angaben sind lediglich Näherungen, soweit möglich. Die Preismodelle richten sich nach Kapazität, Applikation und Funktionsumfang.

Marktübersichten können nie komplett sein. Bei unserem Überblick spielt zunächst die weltweite Marktdurchdringung bei Großunternehmen (nach **Gartner** und **Forrester**) eine Rolle, wir berücksichtigen aber auch Produkte, die hauptsächlich im deutschsprachigen Raum ihre Liebhaber finden und tendenziell am Mittelstand orientiert sind.

Acronis Cyber Protect

Neben seinem Angebot für Privatanwender und KMUs wendet sich der Hersteller auch an professionelle Anwender: **Acronis** *Cyber Protect* will dabei durch besonders benutzerfreundliches Backup für Unternehmen jeder Größe punkten. Das Tool sichert Cloud-Workloads, Hypervisor-Umgebungen, Applikationen und Mobilgeräte. Dazu werden über 20 Plattformen unterstützt. Ergänzt

wird es durch *Acronis Disaster Recovery* (as-a-Service) und durch *Acronis Cloud Storage*.

Cyber Protect beherrscht Instant, Universal, automatisiertes Bare-Metal und Remote-Recovery, vmFlashback, Blockchain-Verarbeitung, Deduplizierung und kann Validierungs-, Konsolidierungs- und Replikations-Prozesse auf andere Systeme auslagern, um Produktiv-Ressourcen zu schonen. Zudem ist ein proaktiver Ransomware-Schutz auf Basis von maschinellem Lernen (ML) integriert. Ebenso unterstützt es Cloud-zu-Cloud-Backup von *Microsoft Office 365*-Daten und *G Suite* sowie die Auslagerung von *VMware*-VM-Snapshots.

Die Acronis-Software steht im Ruf einer Mittelstandslösung, ist aber auch im Enterprise-Segment gefragt, wenn die Datensicherung in der Cloud/SaaS ergänzt wird durch On-Premises. Demnach punktet die Software durch einfache Handhabung und überschaubare Kosten. Die *Essentials*-Suite ist ab 59 Euro erhältlich, Unternehmens-Lizenzen erreichen aber auch dreistellige Bereiche und höher pro Server oder Virtual Host. Kostenlose Testversionen sind verfügbar.

Altaro VM Backup

Altaro *VM Backup* unterstützt die Sicherung von Hyper-V- und VMware-Maschinen und ermöglicht ein lokales Backup auf einen Netzwerk-Share sowie mehrere Offsite-Kopien sowohl an einen anderen Altaro-Server als auch an unterschiedliche Cloud-Anbieter wie Amazon S3, Azure oder Wasabi.

Lizenzen werden per Backup-System ausgegeben, weder per CPU noch per Kern oder nach Workload. In der Unlimited Edition beginnt der Preis bei 595 Euro netto pro Backup-Host.

Lesen Sie mehr in der Produkt-Review auf speicherguide.de.

Arcserve Backup und UDP

Arcserve *Backup* und *Unified Data Protection* (UDP) für mittlere und große Unternehmen basiert auf den Wurzeln von Arcserve Backup und letztlich auf der Weiterentwicklung des Erbes von *CA Technologies*. In der Regel findet die Software eher Anwendung bei mittelständischen Anwendern, große *Oracle*-Umgebungen beispielsweise sind eher die Ausnahme, glaubt man den Analysten. Der Hersteller verspricht Ransomware-Schutz On- und Off-Premises und orchestrierte Wiederherstellung.

Arcserve UDP kombiniert Image-basiertes Backup, Disaster-Recovery-Technologien und Deduplizierung zu einer Komplettlösung. In Zentrale und Außenstellen werden dazu Recovery-Point-Server (RPS) installiert, über den die Host-Plattformen angebunden werden. Die RPS kommunizieren dann mit Disaster-Recovery- und Cloud-Zielen, die sich als Shared-Folder ansprechen lassen.

Zur Liste unterstützter Plattformen gehören Windows, Linux, *Amazon EC2*, *Microsoft Azure*, *Office 365* (*Exchange Online*, *SharePoint Online* und *OneDrive for Business*), Exchange, *MS SQL*, Dateiserver, *Microsoft IIS*, *Active Directory*, *Oracle Database*, *PostgreSQL*, *VMware vSphere* (agentenlos), *Hyper-V* (agentenlos) und *Nutanix AHV*.

Cohesity DataProtect

Zusammen mit *Rubrik* gehört **Cohesity**, vor allem hierzulande, zu den Senkrechtstartern im Bereich der Backup-Anbieter für Unternehmen. Forrester ordnet beide bereits im Bereich der Marktführer ein. *Cohesity DataProtect* ist eine Cloud-native Datenmanagement-Lösung. Sie zielt auf Backup, Wiederherstellung, Replikation und Notfallwiederherstellung von Daten, aber auch auf die weiterführende Verarbeitung von Metadaten, etwa für Tests, Entwicklung und Analytics. Spezialisiert ist Cohesity etwa auf *Hadoop Distributed File Systems*, verteilte *NoSQL*-Datenbanken sowie Container- und SaaS-Anwendungen, aber auch herkömmliche Daten bzw. Workflows aus lokalen Quellen werden in der Cloud gesichert, wiederhergestellt und über eine Plattform verwaltet. Dazu dienen Dienste wie Tiering, Archiv und Replikation, richtlinienbasierte Automatisierung sowie webbasierte Deduplizierung und weitere Apps. Anwender sollen von störungsfreien Upgrades und Erweiterungen in der Cloud sowie vom Schutz vor Ransomware-Attacken profitieren.

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

Commvault Complete Data Protection

CommVault ist im Gartner- und Forrester-Ranking Marktführer 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.

Mit Commvaults Flaggschiff *Complete Data Protection* kombiniert das bekannte *Complete Backup und Recovery* mit Recovery-Diensten. Es stehen über 40 Cloud-Speicherungsoptionen in öffentlichen und privaten Clouds zur Verfügung. 16 Hypervisoren, quasi alle File-Systeme und 15 Datenbanken werden unterstützt. Auf der Kompatibilitätsliste stehen über 30 Primär-

Backup für Cloud- und Objektspeicher auf Tape

PoINT Archival Gateway: Tape-basierter Object Storage mit standardisierter S3 Schnittstelle

Ihre wertvollen Daten auf Cloud- und Objektspeichern müssen durch ein Backup gesichert werden. Technische oder menschliche Fehler können zu gravierenden Datenverlusten führen. Zugleich wächst die Gefährdung durch Cybercrime und Ransomware-Angriffe. Eine Datenkopie auf einem unabhängigen Speichermedium gewährleistet die schnelle Rückkehr zum Geschäftsalltag. Die große Herausforderung dabei sind die enormen Datenmengen im Objektspeicherbereich. Schon aus Kostengründen kann ein Backup nicht auf zusätzlichen festplattenbasierten Objektspeichersystemen erfolgen.

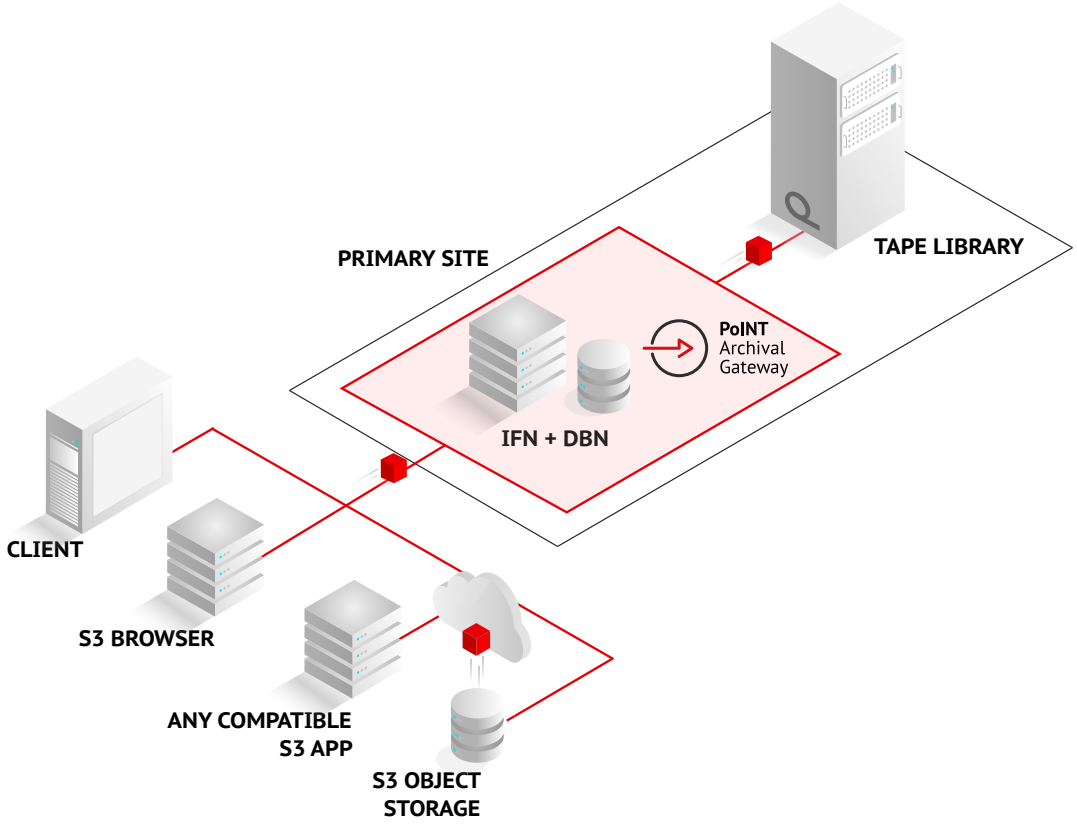
Tape ist das ideale Backup-Medium für große und stetig wachsende Datenmengen:

- Standardisierung
- Skalierbarkeit
- Kosteneffizienz
- Sicherheit durch Air Gap

PoINT Archival Gateway ist ein Tape-basierter Objektspeicher, der die Einbindung von Tape Libraries als zusätzliche, kostengünstige S3 Speicherklasse ermöglicht. PoINT Archival Gateway empfängt die Daten über die standardisierte S3 Schnittstelle und schreibt sie hochperformant auf Tape – die optimale Lösung, um große Datenmengen effizient zu speichern. Im Recovery-Fall sind die Daten ebenso schnell wieder verfügbar.

- Standardisierte S3 REST API
- Datensicherheit durch Verschlüsselung und Erasure Coding
- Direkter Zugriff auf Backup über S3 API
- Herstellerunabhängigkeit und Investitionsschutz durch Standardisierung

Weitere Informationen zu PoINT Archival Gateway finden Sie im Technical White Paper.



PoINT
software & systems

PoINT Software & Systems GmbH • +49 271 3841-0 • info@point.de

Collage: speicherguide.de und die jeweiligen Hersteller

Storage-Plattformen und eine Vielzahl an Tape-Systemen (Adic, Dell EMC, H3C, HPE, IBM, Quantum, Spectra Logic).

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 die Leistung optimieren, Muster analysieren und Anomalien melden, erklärt der Hersteller. Flankiert wird Commvault Complete Backup und Recovery vom SaaS-Angebot *Commvault Metallic Core* und der Scale-out Backup-Appliance *HyperScale*.

In Online-Shops rangiert Commvault Complete Backup und Recovery als Lizenz für einen physischen Server bzw. eine OS-Instanz bei etwa 1.500 Euro.

Dell EMC Networker Data Protection Suite

Die **Dell EMC** *Networker Data Protection Suite* bietet neben den Basis-Funktionen einer Unternehmenslösung zahlreiche Erweiterungsmöglichkeiten bis zur Unterstützung von Big-Data-Workloads. Stand-Alone oder als virtuelle Komponente der Suite ist die *Dell EMC NetWorker*-Software als einheitliche Backup- und Recovery-Lösung für Unternehmensanwendungen und Datenbanken konzipiert.

Networker bietet eine zentralisierte Verwaltung mit Deduplizierung, Backup-to-Disk und Backup-to-Tape, Snapshots, Replikation und NAS-Support und unterstützt physische und virtuelle Umgebungen wie Vmware und Hyper-V und natürlich auch Cloud-Umgebungen.

Die Software ergänzt sich nicht nur, aber auch, mit Hardware des Herstellers wie der *Avamar*-Appliance oder *PowerProtect DD* (Data Domain) für virtuelle Umgebungen. Neben der Data-Domain-Integration betont der Hersteller Security-Aspekte wie 256-Bit AES-Encryption, Secure-Lockbox-Kontrolle, User- und rollenbasierte Authentifizierung.

Effizienz auf Enterprise-Level soll über *VMware vStorage*-APIs und diverse Wizards für Verwaltung und Monitoring realisierbar sein. Ferngesteuerte Server-Optionen sowie Web-Zugriffe für die Restaurierung werden wohl nicht unterstützt.

Mit *PowerOne* bietet Dell eine übergreifende Infrastruktur-Lösung, in die auch Networker als Data-Protection-Lösung passt. Dort gibt es unterschiedliche, flexible Preismodelle wie »Pay as you grow«, »Flex on Demand« (mit monatlicher Berechnung) und »Data Centre Utility« (Pay-per-use über die gesamte Dell-IT-Infrastruktur hinweg).

IBM Spectrum Protect

IBM *Spectrum Protect* als Komponente der Spectrum-Plattform bietet Sicherungs-, Archivierungs- und Speicherverwaltungsfunktionen für Dateiserver, Workstations, virtuelle Maschinen und Anwendungen. Das Erbe aus der Großrechnerwelt deutet auf das Know-how für hohe Skalierbarkeit und Transferraten hin, heute unterstützt IBM natürlich auch diverse Clouds, Betriebssysteme und Speicher-Hardware.

Automatisierte, zentral geplante, richtlinienverwaltete Datensicherung soll IBM Spectrum Protect ermöglichen. Laut Hersteller können Milliarden von Objekten pro Sicherungsserver verwaltet werden. Inklusive integrierter Funktionen für Dateneffizienz und der Möglichkeit, Daten auf Bandlaufwerke, Public-Cloud-Services und lokalen Objektspeicher zu migrieren, stehen Anwendern alle technischen Möglichkeiten offen, so wie man dies auch von IBM erwartet.

Novastor Datacenter

Das in Hamburg ansässige Unternehmen **NovaStor** bietet mit *DataCenter* eine Komplettlösung für Backup, Restore und Archivierung. Adressaten sind eher kleine bis mittelständische Unternehmen, wie Arztpraxen, Kanzleien und Handwerksbetriebe.

Novastor Datacenter bietet universelles Backup und Restore für Windows-Server, SQL-Backup im laufenden Betrieb, Sicherung von Exchange-Datenbanken, Vmware- und HyperV-Sicherungen von beliebig vielen virtuellen Maschinen und Image-Backups zum Schutz vor einem Systemausfall oder Festplattenfehlern. Unterstützt werden lokale Speichermedien (USB, Tape, RDX, NAS) sowie Cloud-/File-Sharing-Dienste (z.B. Sharepoint, Onedrive, Dropbox, Amazon S3). Eine NovaStor DataCenter-Lizenz inklusiv einem Jahr *NovaCare*-Support für 5 TByte finden wir im Online-Handel ab etwa 850 Euro netto.

Quest NetVault

Quest bietet diverse Produkte im Umfeld der Datensicherung, darunter den Recovery Manager für AD, Recovery On-Demand und das Datensicherungsprodukt *NetVault*. Es handelt sich um eine Cloud-fähige Sicherungs-Software für Unternehmen und hybride Rechenzentren. Die skalierbare Software-Lösung macht die Datensicherungen unveränderlich und schützt sie so effektiv gegen Ransomware-Angriffe. Quest Netvault unterstützt verschiedene Server- und Anwendungsplattformen sowohl in physischen als auch in virtuellen Umgebungen.

Quest skaliert bis in den PByte-Bereich und unterstützt verschiedene Betriebssysteme, Anwendungen und Datenbanken sowie Massenspeichergeräte. Dank dieser plattformübergreifenden Vielseitigkeit soll es einfach sein, die Lösung anzupassen, wenn sich IT-Infrastrukren ändern.

Rubrik Cloud Data Management

Neben Cohesity ist **Rubrik** ein neuer »Stern« am Data-Protection-Himmel. Dynamisch wie die Datenwelt präsentiert sich das Unternehmen mit seinem übergreifenden Cloud-Data-Management-Angebot. On-Premises-, Edge- und Multi-Cloud-Workloads können mit *Rubrik* gesichert werden, in der Cloud. Der Service beinhaltet Data-Protection, Ransomware-Recovery, Compliance nach individuellen Vorgaben und generell Datenmobilität durch die Sicherung in der Wolke mit einem gewissen Grad an Automation und API-Offenheit. Datenklassifizierung, Archivierung, Disaster-Recovery und Migration will der Dienst bieten. Dies soll Endgeräte ebenso beinhalten wie VMs und Datenbanken. Mit P*olaris Sonar* bzw. *Polaris GPS* bietet der Hersteller zudem eine Online-Plattform zur Datenklassifizierung.

Banal ist der Service nicht: Integriert ist eine selbstheilende Masterless-Architektur, eine nativ integrierte und Vmware-zertifizierte CDP-Funktion (Continuous-Data-Protection) als Option in SLA-Domains, mit der Firmen ihre Datenschutzrichtlinien definieren können. Smart-Data-Tiering-to-Azure, SaaS-basiertes Polaris GPS, verteilte Metadaten und Namespaces, richtliniengesteuerte Datenverwaltung, rollenbasierte Zugriffskontrolle, Nutzungs- und Compliance-Reports sowie die Integration mit Automatisierungs-Frameworks sollen zum Datensicherungsnutzen beitragen.

Veeam V11A-Suite

Aus der Virtualisierungsszene kommend, gehört Veeam nach Umsatz mittlerweile zu den Top 5 der Data-Protection-Anbieter, so die Analysten. Für das Backup virtueller Vmware-Maschinen fast schon Standard, aber auch Hyper-V wird unterstützt. Dementsprechend wird bei der neuen Veeam V11A-Suite unkomplizierte Administration von Cloud-nativen Sicherungen für AWS, Azure und Goole, Kubernetes-basiertes Backup, verbesserten Ransomware-Schutz und Contiuous Data Protection (CDP) beim Backup und Restore von VMs. Die dazugehörige Backup-Komponente heisst Veeam Backup und Restore v11.

Die V11A-Suite behauptet, alle Clouds, alle Workloads (Vmware, Hyper-V, Windows, Linux, MacOS, Nutanix OS, UNIX) und alle Applikationen zu unterstützen, darunter Active Directory, Exchange, SQL und Oracle. Auch der Einsatz von Storage-Systemen stehe dem Anwender frei. Damit hat sich der Anbieter deutlich von früheren Restriktionen befreit.

SEP Sesam Jaglion v5.0

Mit Jaglion erhält SEP Sesam ein neues Major-Release und ist nun in der Version 5 erhältlich. Der erweiterte Umfang betrifft die Unterstützung von Nutanix AHV, des 10. unterstützten Hypervisors, eine vergrößerte Supportmatrix der unterstützten Lösungen, sowie die Optimierung der Benutzerumgebung. Mit Jaglion hält auch ein neues Authentifizierungskonzept Einzug: Jetzt kann nur noch ein Benutzer mit Superuser-Rechten die Authentifizierung konfigurieren und Berechtigungen (ACLs) an angelegte Benutzer vergeben. SEP sesam Jaglion ist in verschiedene Lizenzmodellen verfügbar. Diese reichen von der einfachen Lizenzierung nach TByte-Datenvolumen, bis hin zur speziellen Lösung und Lizenzierung für MSPs. SEP sesam VM Essential beginnt beispielsweise bei 750 Euro netto (2 Sockel).

Weitere Details auf speicherguide.de

Weitere Informationen

Lesen Sie eine ausführliche Fassung des Marktüberblicks auf 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 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:
Michael Baumann, Karl Fröhlich, Peter Marwan

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:
via Canva Pro

Mediaberatung:
Bettina Röber
E-Mail: media@speicherguide.de

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

speicherguide.de
Das Storage-Magazin

Unser Team

Karl Fröhlich
Chefredakteur
speicherguide.de

Michael Baumann
Redaktion
speicherguide.de

Peter Marwan
Redaktion
speicherguide.de

Bettina Röber
Mediaberatung
speicherguide.de

Partner

DATACORE FAST LTA FUJIFILM iTernity SEP Hybrid Backup

speicherguide.de
Das Storage-Magazin

itmanagement

#storage2022

it-daily.net/storage/

Storage im Fokus

6. April 2022 | Digitalevent

Hier anmelden