storage-magazin.de

Eine Publikation von speicherguide.de

Backup für den Mittelstand

Bild: Dall-E (KI)

Immutable & Backup-Software aus Europa

2025
02

Editorial

WILLKOMMEN IN DER NEUEN REALITÄT

Karl Fröhlich
Chefredakteur
speicherguide.de

Liebe Leserinnen und Leser,

die 2020er Jahre stehen wahrlich nicht unter einem Glückstern. Vor etwas über fünf Jahren nahm Corona seinen Lauf und wir durften uns in der Pandemiebekämpfung üben. Als wir dachten, wir hätten den Virus im Griff, überfällt Russland die Ukraine. Seit etwas über drei Jahren herrscht nun Krieg. Und weil das alles noch nicht blöd genug ist, stellt die neue US-Regierung die halbe Welt auf den Kopf.

Die IT-Branche steht jedes Mal mitten im Geschehen. Zuerst durften IT-Abteilungen in Windeseile Home-Office-Strukturen schaffen, damit Kolleginnen und Kollegen von zuhause aus Arbeiten konnten. Damit einher gingen allerdings auch Sicherheitsrisiken, die der Ukraine-Krieg zusätzlich verschärft. Laut Bitkom wächst in Deutschland die Sorge vor Cyberangriffen und der potenziellen Gefahr eines Cyberkriegs. Für die IT ist es vielerorts ein ungleicher Kampf mit zu geringen Mitteln wie Budget und Personal.

Nun bugsiert die neue US-Regierung das Datenschutzabkommen zwischen Europa und den USA ins Aus. Nachdem kurzerhand bis auf ein Aufsichtsratsmitglied alle im zuständigen Kontrollgremium entlassen wurden, kann die USA das zugesicherte Datenschutzniveau nicht mehr einhalten. Datenschutzexperten gehen davon aus, dass die EU-Kommission aktiv werden muss und das »EU-US Data Privacy Framework« als ungültig erklären wird.

Das ist grundsätzlich nicht neu, bereits zwei Mal hatte das EuGH die Abkommen einkassiert. Nach allem, was wir derzeit hören und sehen, können wir den Amerikanern aber keine Bereitschaft zur Zusammenarbeit mehr attestieren.

Gleichzeitig können wir auch den US-Cloud-Act nicht mehr einfach als unrealistisch abtun. Für die Storage- und Backup-Branche hat das massive Auswirkungen. Aus rechtlicher Sicht (DSGVO) sollten personenbezogene Daten nicht mehr auf as-a-Service-Angeboten von US-Firmen gespeichert werden. Und auch Backup-Software-Produkte sind zu nah dran an unternehmenskritischen Daten.

Wir werden gerade Zeugen, dass sich die US-Regierung nicht an Abmachungen hält und auch richterliche Anweisungen ignoriert. Nun besteht die Befürchtung, dass US-Anbieter im Zweifel gezwungen werden ihre Dienste einzuschränken oder gar abzuschalten. Nun ist es in der Praxis natürlich unmöglich, sich komplett von US-Herstellern zu befreien. Allerdings sollten wir uns mit dem Gedanken anfreunden, dass wir unsere IT künftig unabhängiger aufstellen.

Durch die neue Realität hat dieses Storage-Magazin einen klein wenig anderen »Drive« bekommen. Wir wünschen trotzdem viel Spaß beim Schmökern.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de


SEITE 5

Bild: DALL-E

Geopolitische Unsicherheiten erfordern neue Data-Protection-Strategien

BACKUP FÜR DEN MITTELSTAND – ALLES ANDERS

Neben der Zunahme von Cyberbedrohungen steigern geopolitische Unsicherheiten die Bedeutung von Datenschutz und Datensicherheit. Unternehmen benötigen robuste Backup- und Wiederherstellungs-Strategien, um die Betriebskontinuität zu sichern. Nachdem die USA als verlässlicher Partner auszufallen scheinen, sollten Firmen europäische Data-Protection-Alternativen in Betracht ziehen.

Ransom-Abwehr: Offsite-Backup & Air-Gap sind Pflicht

BACKUP-MEDIEN MÜSSEN UNANGREIFBAR SEIN

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.


SEITE 26

Bild: DALL-E

Backup-Software im Überblick

POLITIK BEEINFLUSST BACKUP-STRATEGIE


SEITE 21

Bild: DALL-E

Übersicht

Storage-Anbieter

SEITE 15

Sicherer Schutz vor Ransomware mit Veeam

ES-3024 Server mit 24 Disk Slots

z.B. 24-Slot Server, teilbestückt mit 12 x 20 TB SAS Disks, 128 GB RAM, 2 x 10 GbE, Ubuntu Linux auf Wunsch vorinstalliert

inkl. MwSt. € 12.971,-

exkl. MwSt. € 10.900,-

„Hardened Linux Immutable Repositories“ bieten einen besonderen Schutz vor der Veränderung von Backups durch **Ransomware** oder **irrtümliches Löschen**.

Auf diese **zweite Backupstufe** hat nur der Veeam Backupserver Zugriff.

Zusätzlich werden die Daten über eine **vorgegebene Retention Zeit** vor jeder Änderung oder Löschung geschützt.

Im Falle eines Ransomware Angriffs werden die Backups vor der Wiederherstellung durch **Veeam DataLabs™ Secure Restore** auf Malware geprüft.

- **Server mit bis zu 36 Disk Slots**
- **AMD EPYC Rome 7282 Prozessor, 16 Core, 2,8 GHz**
- **bis zu 1 TB RAM**
- **Linux Betriebssystem auf gespiegelten 1 TB NVMe M.2 SSDs**
- **optimiert für den Einsatz als Hardened Backup Repository**
- **Areca Hardware RAID Controller mit dediziertem Management Port**
- **optional Erweiterungsports 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**

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 und außerdem Connectivity Produkte wie z.B. 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.

Natürlich bieten wir auch Veeam Server für die erste Backupstufe mit SAS, SATA und NVMe SSDs an.

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

Bild: via DALL-E

Karl Fröhlich
speicherguide.de

Geopolitische Unsicherheiten erfordern neue Data-Protection-Strategien

BACKUP FÜR DEN MITTELSTAND – **ALLES ANDERS**

Neben der Zunahme von Cyberbedrohungen steigern geopolitische Unsicherheiten die Bedeutung von Datenschutz und Datensicherheit. Unternehmen benötigen robuste Backup- und Wiederherstellungs-Strategien, um die Betriebskontinuität zu sichern. Nachdem die USA als verlässlicher Partner auszufallen scheinen, sollten Firmen europäische Data-Protection-Alternativen in Betracht ziehen.

Unabhängig davon, wie Unternehmen es betrachten, die Bedeutung von Datenschutz und Datensicherung nimmt nicht ab. Das Risiko von IT-Ausfällen betont die Notwendigkeit regelmäßiger Backup- und Wiederherstellungs-Maßnahmen für alle Arten von Unternehmensdaten. Bedrohung Nummer 1 kommt aus dem Cyberraum: »Deutschland wird täglich digital angegriffen«, sagt **Bitkom**-Präsident **Dr. Ralf Wintergerst**. »Die Grenzen zwischen Cybercrime und hybrider Kriegsführung, zwischen privaten und staatlichen Akteuren sind inzwischen fließend.«

Im Zuge der fortschreitenden Digitalisierung und globalen Vernetzung steigt die Relevanz der Cybersicherheit kontinuierlich. Insbesondere der anhaltende Konflikt zwischen Russland und der Ukraine hat die Sicherheitslage in den letzten drei Jahren verschärft. Für Unternehmen – egal welcher Größen – bedeutet dies, ihre Daten stehen unter Beschuss.

Keine Firma ist klein genug, um nicht doch von einer Cyberattacke betroffen zu sein. Daher kann es nur einen Weg geben, sich proaktiv vorzubereiten. Das heißt, Sicherheitsmaßnahmen zu ergreifen und mit einer Datensicherungsstrategie dafür zu sorgen, dass sich im Schadensfall Daten zuverlässig wieder herstellen lassen.

In der Umsetzung gibt es noch viel zu tun, doch laut **Stefan Utzinger**, Geschäftsführer bei **NovaStor** versteht der Mittelstand allmählich in der Breite die Gefahr von Cyberangriffen. Das heißt, auch der Geschäftsführung sei klar, dass es keinen 100%igen Schutz gibt.

»Dadurch wird die Datensicherung und insbesondere der Restore immer wichtiger«, sagt Utzinger. »Diese müssen in Notfallsituationen einwandfrei und schnell funktionieren.« Auch reift die Erkenntnis, sich im Notfall um Hilfe zu bemühen.

Modernisierung und Anpassung der Backup-Systeme

Laut dem »State of Backup and Recovery Report 2025« von **Kaseya**/**Unitrends** sind viele der bestehenden

Backup-Lösungen veraltet und haben sich seit Jahren nicht weiterentwickelt. Dies mache sie anfällig für Cyberbedrohungen, aber auch ineffizient in der Handhabung der heutigen Datenmengen und -arten. Verschiedene Studien belegen zudem, dass ein signifikanter Anteil der IT-Experten den Fähigkeiten ihrer Backup-Systeme nur bedingt vertrauen. Marktbeobachter gehen zudem davon aus, dass der Anteil an Firmen mit einem funktionstüchtigen Notfallplan bestenfalls bei 50 Prozent liege. Dem Kaseya-Report zufolge testen nur 25 Prozent ihr Disaster-Recovery einmal pro Jahr oder seltener, was die mangelnde Vorbereitung ebenfalls unterstreicht.

Backup-Strategie muss umfassend sein

Eine moderne Datensicherungsstrategie setzt auf möglichst wenig Programme. Die Backup-Software soll sich sowohl zur Sicherung von physischen und virtuellen Systemen eignen wie auch für Cloud-Strukturen sowie Edge-Umgebungen. Wobei es in der Praxis weniger um die Anzahl der Produkte ankommt, sondern darauf den gesamten Prozess über eine einheitliche Management-Oberfläche zu verwalten.

Als Nummer-1-Trend gilt die Stärkung der Cyber-Resilienz. Präventive Sicherheitsmaßnahmen sollen Schwachstellen minimieren und Angriffe möglichst vermeiden. Ziel ist, Ausfallzeiten so kurz wie möglich zu halten, damit Geschäftsprozesse schnell wieder anlaufen können.

Backup-Lösungen spielen daher eine zentrale Rolle in der Cyber-Resilienz-Strategie. Im Kern sorgen sie dafür, dass Daten nicht verloren gehen, sondern sich möglichst schnell und vor allem sicher wiederherstellen lassen. Dabei ist es egal, ob die Bedrohung von einem Cyberangriff ausgelöst wurde, von einer Datenlöschung (versehentlich oder absichtlich), einem Brand oder einer Naturkatastrophe.

Regelmäßige Backups stellen sicher, dass Unternehmen immer auf eine aktuelle Kopie ihrer Daten zurückgreifen können. Gleichzeitig lassen sich auch Lösegeldforderungen bei Ransomware-Angriffen umgehen – sofern die Backups nicht selbst betroffen sind. Deswegen empfehlen Experten die Sicherheit der Daten während der Übertragung und Speicherung durch Verschlüsselungsmethoden zu gewährleisten und die Sicherungen durch Immutable-Maßnahmen unveränderbar zu machen.

Alle Vorkehrungen sind aber nur wirksam, wenn Backup- und Recovery-Prozesse regelmäßig getestet werden, um die Effektivität der Cyber-Resilienz-Strategie zu bewerten. Nur so lassen sich Schwachstellen identifizieren und die Prozesse vor einem tatsächlichen Vorfall verbessern.

Weitere Infos:

➔ **EU/USA: Storage/Backup-as-a-Service & Abomodelle vor dem Aus**

➔ **SaaS Backup/Recovery 2025: Gravierende Strategiemängel**

Ständig neue Baustellen: Alle US-Hersteller auf dem Prüfstand

Mit **Broadcom**/**VMware** hat sich im vergangenen Jahr eine große Baustelle in den IT-Abteilungen aufgetan. Nachdem Vmware-Produkte zum Teil abgekündigt wurden bzw. massive Preiserhöhungen erlebten, werden vielerorts Virtualisierungs-Alternativen geprüft. Dies hat auch Auswirkung auf die Datensicherung, denn IT-Manager müssen sicherstellen, dass der neue Hypervisor auch von der Backup-Software unterstütz wird. Dieser Prozess ist noch im vollen Gange und schon öffnet sich die nächste Baustelle: US-Anbieter.

Angefangen hat das Dilemma mit Entlassungen in vielen Behörden, wie unter anderem der Aufsichtsstelle für das »*EU-US Data Privacy Framework*« (DPF). Diese Regelung sollte die Überwachung durch US-Geheimdienste regulieren und europäischen Bürgern einen angemessenen Datenschutz garantieren. Nun ist das bestehende Datentransferabkommen zwischen der USA und der EU gefährdet. Datenschutzexperten gehen davon aus, dass dies so nicht weitergeführt werden kann und die EU-Kommission gesetzlich dazu verpflichtet ist, die Angemessenheit des Datenschutzniveaus für unwirksam zu erklären. Die Folgen für die Wirtschaft wären erheblich.

BaaS und SaaS stolpern über US-Cloud-Act

Beim Datenschutz kann man sich vermutlich noch mit den Standardvertragsklauseln behelfen, beim US-Cloud-Act wird es nicht so einfach. Dieses US-Gesetz ermöglicht es US-Behörden auf Daten zuzugreifen, die von US-Unternehmen gespeichert wurden, unabhängig davon, ob die Daten auf Servern in den USA oder im Ausland gespeichert sind. Bisher wurde dieses bestehende Problem mit Argumenten, »was soll schon passieren« heruntergespielt. So einfach können es sich Geschäftsleitungen und IT-Verantwortliche nicht mehr machen.

Wurde bisher vor allem über den Einsatz von Hyperscalern gesprochen, muss die Diskussion auf Backup- und Storage-as-a-Service ausgeweitet werden sowie auf Systeme, die über Abo- und Pay-as-you-go-Modelle von US-Herstellern gemietet werden. Die Speicher und Server befinden sich nach wie vor im Besitz des jeweiligen US-Herstellers und sind daher ebenfalls direkt vom US-Cloud-Act betroffen. Dabei ist es egal, ob die Speicher beim Anbieter oder lokal im Rechenzentrum betrieben werden.

Die USA erweisen sich seit dem Regierungswechsel als nicht mehr verlässlicher Partner, der seine Hoheit über IT-Prozesse als politisches Druckmittel nutzen kann und wird, wie zuletzt die Ukraine erleben musste.

»Die US-Administration setzt auch wirtschaftlich unabhängige Unternehmen unter Druck, sich den politischen Zielen entsprechend zu verhalten«, sagt Stefan Utzinger, Geschäftsführer bei NovaStor.

Jedes System, auch Backup-Software, kann heute vom Hersteller »ausgeschaltet« oder »manipuliert« werden – diese Diskussion gab es schon mit **Kaspersky**. »Heute muss das auf US-Amerikanische Hersteller ausgedehnt werden«, mahnt Novastor-Chef Utzinger. »Wenn große US-Betriebssystem- oder Backup-Software-Hersteller den Stecker ziehen, geht kein Teams, kein E-Mail und auch kein Backup mehr in den Unternehmen. Daher darf eigentlich kein Entscheider mehr auf US-Lösungen setzen, wenn es europäische Alternativen gibt.« ■

On-Premises oder Cloud für Backup?

STRATEGISCHE UND WIRTSCHAFTLICHE VORTEILE DURCH ON-PREMISES-SPEICHER

Hannes Heckel
FAST LTA

Angesichts jährlich um 30 Prozent steigender Datenvolumina und zunehmender Cyberrisiken steht die Wahl der Backup-Infrastruktur im Zentrum unternehmerischer Entscheidungen. Analysen zeigen, dass On-Premises-Lösungen wie die neuen Silent Bricks Systeme mit Controller X und Silent Brick Pro nicht nur sicherheitstechnische, sondern auch ökonomische Vorteile bieten.

Die physische Kontrolle über Backup-Infrastrukturen gewinnt vor dem Hintergrund von Richtlinien wie der NIS-2-Direktive und DSGVO an Bedeutung. On-Premises-Systeme ermöglichen die Implementierung von Air-Gapped-Architekturen, bei denen Backup-Module mechanisch vom Netzwerk getrennt werden.

Dieser Schutzmechanismus übertrifft Cloud-basierte Immutable-Storage-Lösungen durch seine physikalische Natur. Untersuchungen des **BSI** belegen, dass 68 Prozent der Ransomware-Angriffe auf Cloud-Backups abzielen, häufig durch Kompromittierung von Zugangsdaten. Moderne On-Premises-Lösungen kombinieren multiple Immutability-Methoden mit einem Chargen-Mix-Ansatz, bei dem jedes Speichermodul Komponenten aus mindestens drei Produktionschargen verschiedener Hersteller integriert.

Diese Methode reduziert Serienfehlerrisiken um 92 Prozent, ein Schutz, den standardisierte Cloud-Hardwarepools nicht leisten können.

Bild: FAST LTA

Jeder Silent Brick Pro enthält zwölf M.2-NVMe-Module mit je bis zu 8 TByte, die aus drei verschiedenen Produktions-Chargen stammen (Chargen-Mix).

TCO-Analyse am Praxisbeispiel

Ein mittelständisches Industrieunternehmen mit 250 TByte Quelldaten und 25 Prozent Datenwachstum für Backup & Recovery realisiert mit einer On-Premises-Lösung Kosteneffizienz durch transparente Investitions- und Betriebskosten. In 5 Jahren gehen die angenommenen Kosten einer führenden Cloud-Lösung schnell in den Millionenbereich. Obwohl kein Investment in eigene Infrastruktur notwendig ist, sorgt die intransparente Kostenstruktur, inklusive Kosten für Einlagerung, Tiering, API-Nutzung und Wiederherstellung für enorme Summen, die umso höher ausfallen, je länger der Dienst in Anspruch genommen wird und je häufiger Daten abgerufen werden. Gerade unvorhergesehene Ereignisse wie Cyber-Angriffe erzeugen sofort hohe Egress-Kosten.

Dem gegenüber stehen moderne, effiziente On-Premises-Speicher, die nicht nur viel schneller sind und volle Souveränität bieten, sondern auch bis zu 60 Prozent niedrigere TCO verursachen. Zudem sind die Kosten durch transparente Preisgestaltung besser kalkulierbar.

Technologische Leistungsparameter

Vergleichstests zwischen On-Premises- und Cloud-Lösungen zeigen signifikante Geschwindigkeitsunterschiede. Während NVMe-optimierte Systeme konstante Schreibraten von 5 GByte/s erreichen, limitieren Protokoll-Overheads und geteilte Bandbreiten Cloud-Dienste auf maximal 1,2 GByte/s. Bei der Wiederherstellung eines 50-TByte-VM-Clusters benötigt die On-Premises-Lösung 2,8 Stunden gegenüber 8,5 Stunden in der Cloud. Diese Differenz resultiert aus lokalem Direct-Access und der Vermeidung von Netzwerklatenzen. Für Unternehmen mit RTO-Anforderungen (Recovery Time Objective) unter einer Stunde wird On-Premises somit zur technischen Notwendigkeit.

Die Skalierbarkeit moderner Systeme ermöglicht zudem Wachstum ohne Migrationskosten. Während manche Cloud-Nutzer bei Überschreiten von 500 TByte pro Account von aufwändigen Bucket-Migrationen mit bis zu 28 Tagen Downtime berichten, skaliert die On-Premises-Architektur durch modulare Erweiterungen im laufenden Betrieb.

Der Slot-basierte Controller X nimmt bis zu acht Silent Brick Pro mit je bis zu 96 TByte auf und lässt sich mit Silent Brick Max auf bis über 6 PByte Gesamtkapazität erweitern.

Bild: FAST LTA

Energieeffizienz und Hardware-Lebenszyklen

Die modulare Architektur gewährleistet lange Nutzungsdauern durch schrittweise Upgrades. Vorhandene *Silent Brick Max* lassen sich ohne Migration auch am neuen *Controller X* betreiben. Diese Flexibilität senkt die Total Cost of Ownership weiter, da Hardware-Komponenten über sieben bis zehn Jahre genutzt werden können. Gebrauchte Systeme erzielen zudem nach fünf Jahren noch 25 bis 35 Prozent des Neuwerts als Restwert – ein Gegenwert, der Cloud-Investitionen komplett fehlt.

Energieeffizienz wird durch Abschalten ungenutzter NVMe-Module und dynamisches Spindown inaktiver HDDs bis zur kompletten Abschaltung optimiert. Messungen belegen einen 15 Prozent geringeren Stromverbrauch gegenüber herkömmlichen Speichersystemen. Bei Stromkosten von 0,32 Euro/kHz ergibt dies jährliche Einsparungen von 1.280 Euro gegenüber vergleichbaren Cloud-Rechenzentren.

Fazit: Die ökonomische Rationalität der Kontrolle

Die Analyse belegt, dass On-Premises-Backuplösungen keine Alternative, sondern eine betriebswirtschaftliche Notwendigkeit darstellen. Die Kombination aus fixen Betriebskosten, wegfallenden Cloud-Zusatzgebühren und langfristiger Skalierbarkeit schafft Planungssicherheit in Zeiten volatiler Preismodelle. Technologische Vorteile wie Air-Gapped-Architekturen und hardwarebasierte Immutability adressieren zudem kritische Sicherheitsanforderungen, die Cloud-Dienste aufgrund ihrer strukturellen Abhängigkeiten nicht erfüllen können.

Für Unternehmen, die Datensouveränität mit ökonomischer Rationalität verbinden wollen, markiert dies den Weg zur zukunftsfesten Backup-Strategie – eine Investition, die nicht nur Kosten kontrolliert, sondern auch die Resilienz kritischer IT-Infrastrukturen nachhaltig stärkt. ■

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

Daten- und System-Management in einer Software vereint

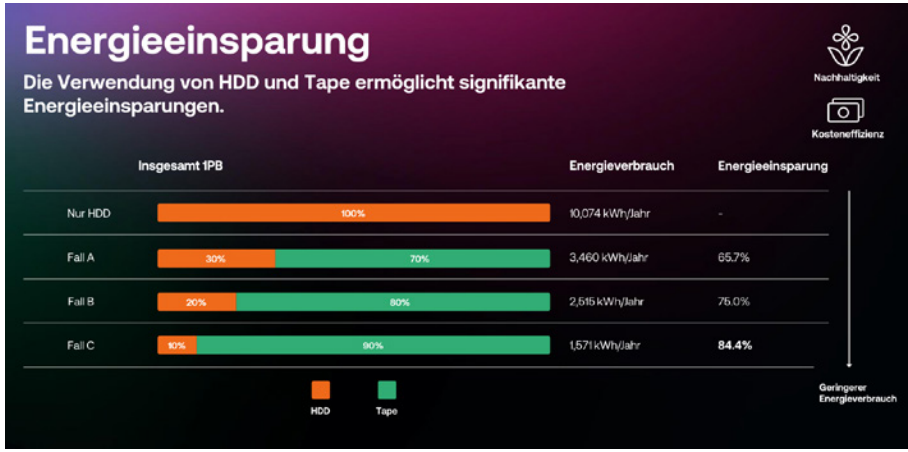
MIT TAPE-TECHNOLOGIE DAS COLD-DATA-PROBLEM LÖSEN

Datenberge wachsen ständig weiter. Die meisten Datenberge sind aber Eisberge: 70 Prozent ihrer Daten sind Archivdaten und liegen auf ungeeigneten und viel zu teuren Speichermedien. Das bindet Ressourcen. Mit Tape und geeigneter Software lassen sich diese loseisen.

Philipp Stevens
Business Development Manager DACH FUJIFILM Recording Media

Unternehmen hungern nach Daten. Man hofft, durch die Auswertung großer Datenmengen neue Erkenntnisse zu gewinnen, KI-Modelle zu trainieren, Geschäftsprozesse zu optimieren und Marketingstrategien zu revolutionieren. In den vergangenen Jahren wurden diese Hoffnungen durch erstaunliche Ergebnisse weiter genährt. Oft haben die Beteiligten dabei aber aus dem Blick verloren, dass längst nicht alle Daten, die in einem Unternehmen vorhanden sind, ständig ausgewertet werden müssen. Denn je nach Branche verfügen Unternehmen über riesige Datenmengen, die zwar weiterhin aufbewahrt werden müssen, von denen aber nur selten und wenn, dann wenige benötigt werden.

Für diese Daten hat sich der Begriff Cold-Data eingebürgert. So kalt sind diese Daten aber gar nicht. Seriösen Schätzungen zufolge gehören 70 Prozent der Datenmengen in Unternehmen dazu – diese liegen überwiegend auf Festplatten. Die dafür genutzten Systeme sind überwiegend nicht auf die Archivierung von Daten ausgelegt, sondern für den tagtäglichen Zugriff also für Daten, die regelmäßig benötigt werden. Diese Lagerung ist kostenintensiv und darüber hinaus wenig nachhaltig, da Festplattensysteme verglichen mit Tape-Systemen, einen ungleich höheren Energiebedarf aufweisen.



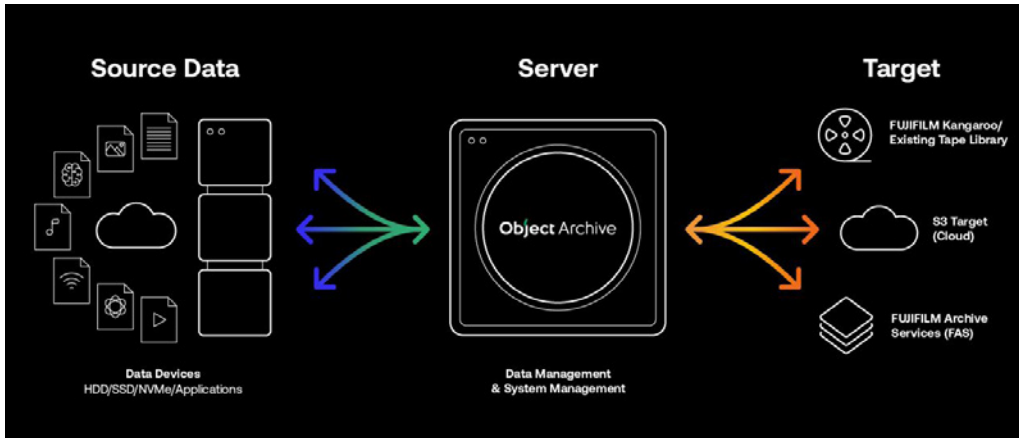
Grafik: Fujifilm

Tape-Speicher kommen mit deutlich weniger Energie aus als HDD-Systeme – was bei Archivierung über die Jahre deutlich ins Gewicht fällt.

Cold-Storage – kostenoptimierte Lagerung

Das lässt sich mit der Festplatte des heimischen PCs vergleichen: Da liegen die alten Kontoauszüge neben längst vergessenen PDF-Dateien mit Einladungen zu früheren Schulfesten der Kinder und bei Suche nach neuen Möbeln vor Jahren heruntergeladenen Produktbildern neben der regelmäßig genutzten Excel-Tabelle für die Haushaltsausgaben und der Word-Vorlage für Behördenanschreiben.

Was im Kleinen nur lästig ist, ist im Großen kostspielig. Beispielberechnungen von **Fujifilm** zeigen, dass die Speicherung von 1 PByte an Daten (wofür 15 Server angenommen wurden) auf HDDs pro Jahr über 10.000 kWh Strom erfordert. Dazu kommt, dass HDDs in der Regel eine Nutzungsdauer von etwa fünf Jahren haben.



Grafik: Fujifilm

FUJIFILM Object Archive Software verbindet nicht nur Archivquellen mit geeigneten Archivzielen, sondern übernimmt auch das physische Management der zur Archivierung genutzten Tapes

Das heißt, dass Daten, die 20 oder gar 30 Jahre aufbewahrt werden sollen, drei oder fünfmal migriert werden müssen. Dabei fällt nicht nur die Ersatzbeschaffung der Hardware ins Gewicht – auch gilt es die Migration vorzubereiten und durchzuführen – nur um nachher dasselbe Ergebnis zu haben wie vorher.

LTO-Tapes für Cold-Data prädestiniert

Bei LTO-Tapes ist das anders. Ein *LTO 9*-Tape mit 18 TByte von Fujifilm etwa wird mit 30 Jahren Garantie geliefert. Damit sind die allermeisten Archivierungsanforderungen abgedeckt – mit einmaliger Beschaffung und einem Schreibvorgang.

Theoretisch. Da es in der Praxis komplexer ist und Daten durchaus unterschiedliche Lebenszyklen haben, hat Fujifilm in den vergangenen Jahren am deutschen Firmensitz in Kleve eine intelligente Management-Software entwickelt. Sie ist inzwischen gut zwei Jahre bei Kunden im Einsatz, und hat sich – nicht zuletzt nach dem Feedback der Kunden – kontinuierlich weiterentwickelt.

Mehrwert durch Software

Eine Besonderheit der *FUJIFILM Object Archive Software* ist, dass sie Daten- und System-Management in einer Software vereint. Das bedeutet, dass die Verwaltung des Speicher-Systems und die Steuerung des Datenflusses vom Backup zum Archiv aus einer Oberfläche heraus möglich ist. Dass sich nicht nur die Daten managen lassen, sondern auch die zur Speicherung verwendeten Tape-Systeme ist in mehrerlei Hinsicht hilfreich. Zum Beispiel sind damit physische Checks der Tapes durch die Software möglich, mit denen sich die Qualität und die verbleibende Lifetime der Speichermedien bestimmen lässt. In Abhängigkeit davon, lassen sich dann wiederum die Daten verwalten und verschieben.

Wichtig bei Archivierungstechnologien ist immer die Frage nach der späteren Lesbarkeit. Schließlich ändert sich IT-Technologie rasch – und Archivierungszyklen sind oft lang. 1995 etwa war DVD der letzte Schrei – 30 Jahre später ist es schwer, in Firmen noch Lesegeräte dafür zu finden. Um langfristig Zugriff zu ermöglichen, hält Fujifilm die Software offen. Auch die Daten werden in einem offenen Format archiviert. So ist es zum Beispiel möglich, mit jeder Linux-Oberfläche die Daten wieder lesbar zu machen. Kunden sind nicht an bestimmte Systeme gebundenen oder von einem Hersteller abhängig.

Datenhoheit behalten

Nicht erst seit Anfang 2025 und insbesondere in den derzeit volatilen Zeiten stellt sich die Frage, ob die Cloud der richtige Ort für Cold-Data ist. Zum einen summieren sich die zunächst niedrig erscheinenden Kosten im Lauf der Jahre zu höheren Beträgen und zum anderen verlangen die Anbieter hohe Gebühren für schnellen Zugriff bei Datenexport. Zudem können gerade Bereiche mit hohem Archivierungsbedarf, etwa im Gesundheitswesen, Justizwesen, Finanz- und Versicherungsbranche oder öffentliche Einrichtungen, aufgrund regulatorischer Vorgaben Cloud-Anbieter nicht bedenkenlos nutzen – oder nur mit hohem, zusätzlichem Aufwand, etwa bei Verschlüsselung, Schlüssel- und Rechte-Management und zusätzlichen Sicherheitsvorkehrungen.

Für Fälle, in denen die Cloud eine Option ist, bietet die FUJIFILM Object Archive Software eine S3-Anbindung. Mit dem von *AWS* entwickelten Protokoll lassen sich alle gängigen Cloud-Anbieter ansteuern. Zusätzlich besteht die Möglichkeit, Daten generell oder als Kopie in Fujifilms eigenem Rechenzentrum in Kleve zu sichern. Das ist auch dann möglich, wenn die Daten grundsätzliche On-Premises vorgehalten werden sollen.

Dafür bieten sich die Komplettsysteme der *Kangaroo*-Reihe an. Der jüngste Neuzugang dieser Produktreihe heißt *FUJIFILM Kangaroo LITE* und richtet sich mit einer Kapazität ab 100 TByte an kleine und mittelständische Unternehmen. Das könnten Anwalts- und Steuerberaterkanzleien, Firmen im Medienbereich oder Architekturbüros und Baufirmen sein.

Für größere Unternehmen oder Bildungseinrichtungen gibt es das FUJIFILM Kangaroo mit einer nutzbaren Kapazität von 1 PByte. Die drei Varianten S, M und L stehen nicht für die Speicherkapazität, sondern für den Funktionsumfang. In robustem Rollcontainer sind sie auch für den mobilen Einsatz geeignet. ■

Weitere Informationen:

FUJIFILM Recording Media GmbH

Fujistrasse 1
47533 Kleve

Regionale Kontakte:
Philipp Stevens
Tel.+49 2821 509 371
E-Mail: Philipp.Stevens@fujifilm.com

Datenhoheit: Wissen, wo die Daten bleiben

LOKALE SOFTWARE-HERSTELLER: WEIL IHRE DATEN NUR IHNEN GEHÖREN

Jetzt mal ‚Butter bei die Fische' – wie wir in Hamburg sagen: Wer liest AGBs wirklich durch bzw. weiß, wo die eingesetzte Backup-Software entwickelt wird oder die eigenen Daten gespeichert werden? Wir bei NovaStor wissen um diese wichtigen Details, um Firmendaten vor Cyberangriffen, regulatorischen Fallstricken und geopolitischen Risiken zu schützen. Die gute Nachricht: Es gibt eine einfache Lösung – lokale Software-Hersteller.

Bei der Datensicherung setzen viele Unternehmen mittlerweile neben On-Prem-Lösungen auch auf die Sicherung in die Cloud. Wer hierbei globale Anbieter nutzt, sollte sich allerdings bewusst sein, dass immer einige Daten in Rechenzentren außerhalb der EU gespeichert werden und durch Gesetze wie zum Beispiel den *US CLOUD Act* von Behörden eingesehen werden können (wenn diese Behörden gängige Gesetze überhaupt beachten).

Als norddeutscher Software-Hersteller bietet **NovaStor** Unternehmen Datensicherung »Made in Hamburg« – mit allen Vorteilen in Sachen Datenschutz und DSGVO-Konformität. Aus diesem Grund setzen wir gerade auch beim Thema Cloud-Sicherung auf eine enge Zusammenarbeit mit unserem deutschen Cloud-Partner **IONOS**, um

Stefan Utzinger
NovaStor

eine durchgehend sichere und souveräne Lösung für Unternehmen und Systemhäuser zu garantieren. So behalten Sie die volle Kontrolle über Ihre Daten und vermeiden unnötige Risiken durch ausländische Rechtsvorschriften. Eine durchdachte Backup-Strategie mit lokalen Lösungen sorgt für maximale Sicherheit und Verlässlichkeit.

Wenn die Lichter ausgehen: Software, die bleibt

Klingt nach Science-Fiction, ist aber real: Unternehmen weltweit haben in den letzten Jahren erlebt, was passiert, wenn plötzlich Sanktionen greifen oder geopolitische Spannungen dazu führen, dass Software nicht mehr verfügbar ist oder vom Hersteller einfach »abgeschaltet« wird. Wer sich auf lokale Software-Hersteller verlässt, muss sich keine Sorgen machen, dass kritische Systeme von heute auf morgen einfach abgeschaltet werden.

»Please hold the line« – ein Satz, den man an Support-Hotlines nur allzu oft hört. Wer ihn kennt, weiß, wie frustrierend schlechter Support sein kann.

Doch wenn ein Cyberangriff erfolgt ist oder ein IT-Notfall eintritt, darf Support nicht nur aus »Tickets closen« bestehen – dann braucht es Experten, die sofort helfen. Lokale Anbieter wie NovaStor punkten mit direktem Kontakt zu echten Spezialisten, die nicht nur wissen, wie die Software funktioniert, sondern sie selbst entwickelt haben. Dabei geht es nicht nur um schnelle Hilfe in Krisensituationen, sondern auch um Unterstützung bei der Einrichtung, Optimierung und Weiterentwicklung der Backup-Strategie. Das spart nicht nur Zeit, sondern auch Nerven – besonders, wenn es um so etwas Kritisches wie die Wiederherstellung von Daten und eine schnelle Wiederaufnahme des Geschäftsbetriebs geht.

Die wirtschaftliche Komponente: IT-Souveränität als Standortvorteil

Lokale Software-Hersteller sind mehr als nur eine Alternative zu globalen Anbietern – sie sind eine strategische Entscheidung. Wer in lokale IT investiert, hält Know-how im eigenen Land, stärkt die Wirtschaft und sorgt für Innovationskraft. In Zeiten, in denen digitale Souveränität immer wichtiger wird, ist das ein nicht zu unterschätzender Faktor. Zudem bieten lokale Hersteller wie NovaStor wirtschaftlich attraktive Lizenzmodelle für Unternehmen und bessere Margen für Systemhäuser – ein klarer Vorteil für alle Beteiligten.

Fazit: Zeit, umzudenken

Die IT-Welt wird immer komplexer – aber einige Entscheidungen sind ganz einfach. Wer seine Datensicherung auf eine langfristig sichere, unabhängige und verlässliche Basis stellen will, sollte sich lokale Anbieter genauer ansehen. Also: Wenn Sie das nächste Mal über Ihre Backup-Strategie nachdenken – rufen Sie uns doch einfach mal in Hamburg an. ■

Weitere Informationen:

NovaStor GmbH

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

SaaS: Vom klassischen Backup zur umfassenden Data-Protection

DIE BEDEUTUNG MODERNER BACKUP-STRATEGIEN

In der heutigen digitalen Wirtschaft sind Daten eines der wertvollsten Güter eines Unternehmens. Doch mit der zunehmenden Verlagerung von Geschäftsprozessen in die Cloud und einer stetig wachsenden Bedrohung durch Cyberangriffe müssen Unternehmen ihre Backup- und Datensicherungsstrategien neu bewerten. Traditionelle Backup-Methoden stoßen an ihre Grenzen, und eine moderne, strategische Data-Protection ist notwendig, um Unternehmensdaten effektiv zu schützen. Hier setzen MTI Technology und Dell Technologies mit innovativen Lösungen neue Maßstäbe.

Nikola Grujicic
MTI Technology

Lange Zeit war Backup eine rein betriebliche Funktion: Daten wurden regelmäßig gesichert, meist auf physischen Medien wie Festplatten oder Magnetbändern. Die 3-2-1-Regel galt als bewährte Methode: Drei Kopien der Daten, auf zwei verschiedenen Speichermedien, davon eine an einem externen Standort. Doch mit der zunehmenden Dezentralisierung von IT-Infrastrukturen und der Verlagerung in hybride und Multi-Cloud-Umgebungen reicht diese traditionelle Vorgehensweise nicht mehr aus.

Moderne Data-Protection geht über einfache Backups hinaus. Sie betrachtet Daten als strategisches Unternehmensvermögen, das vor Bedrohungen wie Ransomware, Hardware-Ausfällen oder menschlichen Fehlern geschützt werden muss. Die Fähigkeit, Daten schnell und effizient wiederherzustellen, wird zu einem entscheidenden Wettbewerbsfaktor.

Strategische Data-Protection: Warum Unternehmen umdenken müssen

Die klassische Backup-Mentalität ist überholt. Unternehmen benötigen einen strategischen Ansatz, der über reine Datenspeicherung hinausgeht. Wie **Michael Lischewski**, Data Protecion Lead für die DACH-Region bei **Dell Technologies**, betont: »Beim Schutz von Unternehmenswerten sprechen wir von einer Investition in die Zukunft, nicht nur von Backup-Kosten.«

Das bedeutet, dass Datensicherung nicht nur eine IT-Angelegenheit ist, sondern als zentrales Element der Geschäftskontinuität betrachtet werden muss. Unternehmen stehen heute vor Herausforderungen wie:

- **Wachsende Datenmengen:** Die Datenexplosion erfordert flexible und skalierbare Speicherlösungen.
- **Erhöhte Cyber-Bedrohungen:** Ransomware-Angriffe nehmen zu, was sichere und schnelle Wiederherstellungsmöglichkeiten notwendig macht.
- **Strenge Compliance-Anforderungen:** DSGVO und andere regulatorische Vorgaben verlangen robuste Datenschutzmaßnahmen.

Moderne Backup- und Data-Protection-Lösungen im Überblick

Um diesen Herausforderungen zu begegnen, setzen moderne Unternehmen auf innovative Data Protection-Strategien. Lösungen wie *Dell APEX Backup Services* bieten:

- **Effizienz und Automatisierung:** Eine vollständig SaaS-basierte Backup-Lösung, die ohne Hardware- und Software-Verwaltung auskommt und mit ihrer dynamischen Skalierbarkeit eine langfristige Datensicherung gewährleistet.
- **Kosteneffizienz:** Die Nutzung der Cloud eliminiert hohe Investitionskosten für Hardware und reduziert den Wartungsaufwand.
- **Compliance und Datenschutz:** Automatisierte Funktionen zur Sicherstellung gesetzlicher Vorgaben und integrierte Ransomware-Schutzmechanismen.
- **Nahtlose Cloud-Integration:** Die

Möglichkeit, Workloads sicher in einer Cloud-Umgebung zu schützen.

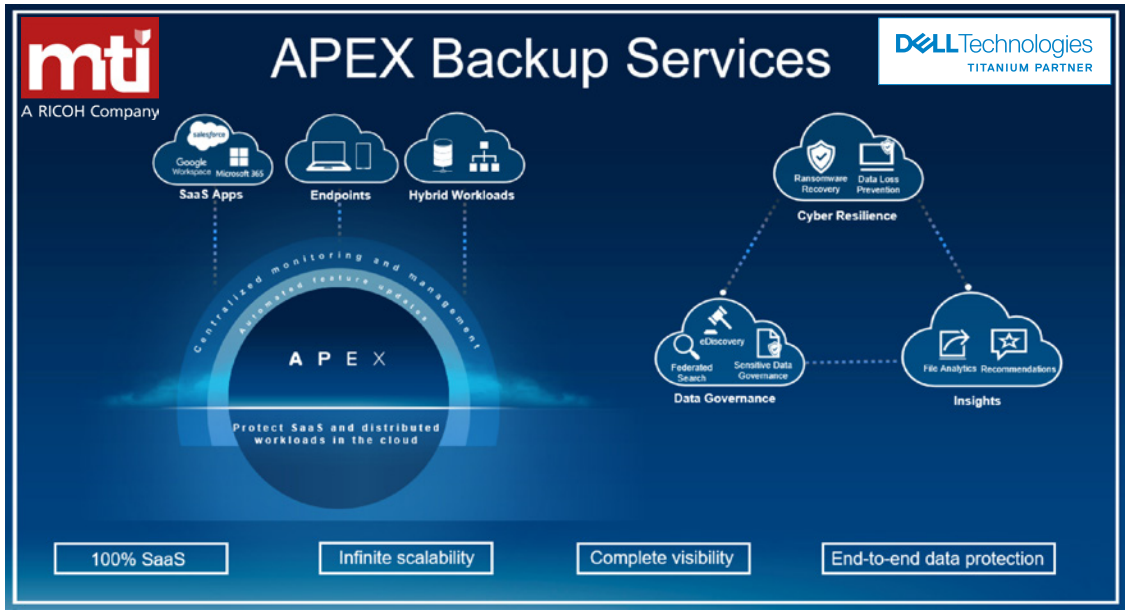
Gerade für Unternehmen, die eine Migration von *Windows 10* auf *Windows 11* durchführen, ist ein durchdachter Backup- und Wiederherstellungsprozess essenziell, um Datenverluste und Sicherheitsrisiken zu vermeiden.

MTI Technology: Der richtige Partner für zukunftssichere Backup-Lösungen

Die Wahl der richtigen Backup-Strategie ist komplex und erfordert Expertise. **MTI Technology** unterstützt Unternehmen nicht nur bei der Auswahl der passenden Data-Protection-Lösung, sondern begleitet sie auch bei der Implementierung und dem laufenden Betrieb. »Unternehmen benötigen heute eine Data-Protection-Strategie, die vom Edge zum Core zur Cloud reicht und in Ergänzung mit AI diese automatisiert und gleichzeitig GenAI per Design in diese Strategie mit einbezieht«, sagt Dell-Technologies-Manager Lischewski. »Zudem wollen sie einen strategischen Partner, der Datenschutz in einen geschäftlichen Mehrwert verwandelt.«

Durch umfassendes Know-how und langjährige Erfahrung hilft MTI seinen Kunden, ihre Datensicherung auf die nächste Stufe zu heben. Der ganzheitliche Ansatz sorgt für einen reibungslosen Betrieb und eine zukunftssichere IT-Strategie. Mit tiefgreifendem Know-how und langjähriger Erfahrung entwickelt MTI maßgeschneiderte Sicherheitskonzepte, die Verfügbarkeit, Skalierbarkeit und Compliance-Anforderungen vereinen. Der ganzheitliche Ansatz ermöglicht es Unternehmen, sich auf ihr Kerngeschäft zu konzentrieren, während MTI für den reibungslosen Schutz geschäftskritischer Daten sorgt.

Unsere Kunden profitieren von einer zukunftssicheren Data-Protection-Strategie, die höchste Sicherheit mit betrieblicher Effizienz kombiniert. Dell Technologies gemeinsam mit MTI realisiert integrierte Lösungen, die den Anforderungen der digitalen Transformation umfassend gerecht werden.



Grafik: Dell

APEX Backup Services bietet einen Cloud-basierten Rundumschutz mit Backup, Notfallwiederherstellung und langfristiger Aufbewahrung zu vorhersehbaren und kontrollierbaren Kosten. Unternehmen profitieren von höherer Sicherheit (Solve), optimierter Skalierbarkeit und Effizienz (Increase) sowie reduzierten Investitions- und Betriebskosten (Safe). Durch die Automatisierung und Compliance-Integration ermöglicht APEX zudem eine sorgenfreie IT-Landschaft – weil Datensicherheit eine Frage des Vertrauens ist (Emotion).

Individuelle Datacenter-Lösungen für maximale Effizienz

Seit über 35 Jahren steht MTI Technology für vertrauensvolle IT-Beratung und praxisorientierte Lösungen in den Bereichen Datacenter, Cloud und Cyber-Security. Unternehmen profitieren von:

- Individuell angepassten Backup- und Ransomware-Schutzlösungen.
- Hochverfügbaren und automatisierten IT-Infrastrukturen.
- Rund-um-die-Uhr-Support mit deutschsprachigem Service.
- Zertifizierten Technikern für Implementierung, Wartung und Schulung.
- Umfassenden Managed Services und strategischer IT-Beratung aus einer Hand.

MTI Technology bietet Unternehmen nicht nur zuverlässigen Datenschutz, sondern schafft eine resiliente IT-Landschaft, die sich flexibel an künftige Herausforderungen anpassen lässt.

Fazit: Warum Unternehmen jetzt handeln sollten

Die digitale Transformation erfordert ein neues Verständnis von Backup und Datensicherheit. Unternehmen müssen weg von isolierten Backup-Lösungen und hin zu einer ganzheitlichen Data-Protection-Strategie. Dell APEX Backup Services bieten eine leistungsstarke, cloudbasierte Lösung, die Effizienz, Sicherheit und Compliance vereint. In Zusammenarbeit mit MTI Technology profitieren Unternehmen nicht nur von innovativen Technologien, sondern auch von einer praxisnahen Beratung und Implementierung.

Jetzt ist der richtige Zeitpunkt, um in eine moderne Backup-Strategie zu investieren und die Zukunft des Unternehmens zu sichern. ■

Weitere Informationen:

MTI Technology GmbH

Borsigstraße 36
65205 Wiesbaden
Tel. +49 (0) 6122 995-0
E-Mail: deinfo@mti.com
https://de.mti.com/get-in-touch/

NovaStor GmbH

www.novastor.de

NovaStor ist ein deutscher Softwarehersteller aus Hamburg und bietet mit NovaStor DataCenter eine einfache, zuverlässige und cyber-resiliente Lösung für Datensicherung und -wiederherstellung – 100 % Made in Hamburg.
Kunden aus dem Mittelstand, KRITIS-Unternehmen, Behörden, Kommunen sowie Systemhäuser und MSPs profitieren von einer ganzheitlichen Beratung zu Datensicherungskonzepten und deutschsprachigem, technischem Support. Transparente Preismodelle und spezielle Partnerprogramme für Systemhäuser und MSPs runden das Angebot ab.

Sitz der Gesellschaft:
Hamburg

Jahr der Gründung:
1999

Zielgruppe:
Mittelstand, KRITIS-Unternehmen, Behörden, Kommunen sowie Systemhäuser und MSPs

MTI Technology

de.mti.com

Die MTI Technology GmbH ist spezialisiert auf die Planung, Umsetzung und Betreuung hochverfügbarer und sicherer Datacenter-Infrastrukturen. Besonders Managed Services rund um die Themen Storage, Backup, Cloud und Cyber-/IT-Security stehen im Mittelpunkt des 1988 gegründeten IT-Systemhauses. Durch enge Partnerschaften mit führenden Herstellern stellt MTI ein Portfolio zukunftssicherer Lösungen zur Verfügung. Als Teil der Ricoh-Konzernfamilie bietet MTI mit seinen eigenen Servicemitarbeitern einen 24/7-Business-Support – 100 Prozent Made-in-Germany.

Sitz der Gesellschaft:
Wiesbaden

Jahr der Gründung:
1988

Zielgruppe:
KMU, Netzbetreiber, Energieversorger, öffentliche Auftraggeber, Banken und Versicherungen

N-TEC GmbH

n-tec.eu

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

EUROSTOR

www.eurostor.com

EUROstor ist ein europaweit tätiger Hersteller von Speichersubsystemen, 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

DataCore Software

www.datacore.com/de/

DataCore Software bietet die branchenweit flexibelsten, intelligentesten und leistungsstärksten Software-Defined Storage-Lösungen für Block-, Datei - und Objektspeicher. Das Unternehmen unterstützt mehr als 10.000 Kunden weltweit bei der Speichermodernisierung, sowie dem Schutz und dem Zugriff auf ihre Daten. Mit einem umfassenden und auf eigenen Patenten basierenden Produktportfolio, sowie konkurrenzloser Erfahrung im Umfeld von Speicher Virtualisierung inklusive hochwertiger Datendienste ist DataCore das Maß der Dinge für Software-Defined Storage.

Sitz der Gesellschaft:
USA

Jahr der Gründung:
1998

Zielgruppe:
Fachhandel, KMU, Enterprise

FAST LTA

www.fast-lta.de

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.

Sitz der Gesellschaft:
München

Jahr der Gründung:
1999

Zielgruppe:
KMUs, VARs und Industriekunden

Dell Technologies

www.dell.com/de-de/shop/scc/sc/storage-products

Dell Technologies unterstützt Organisationen und Privatpersonen dabei, ihre Zukunft digital zu gestalten und Arbeitsplätze sowie private Lebensbereiche zu transformieren. Das Unternehmen bietet Kunden das branchenweit umfangreichste und innovativste Technologie- und Services-Portfolio für das KI-Zeitalter.

Sitz der Gesellschaft:
USA

Jahr der Gründung:
1984

Zielgruppe:
Großkunden, KMUs, Behörden, Bildungseinrichtungen, Systemhäuser, VARs und Industriekunden

Fujifilm Recording Media

www.fujifilm.com/de/de/business/data-management

FUJIFILM Recording Media ist der weltweit größte Hersteller von Bandmedien und bietet Industriepartnern und Kunden aus den verschiedensten Branchen eine breite Palette innovativer bandbasierter Archivierungslösungen. Das Unternehmen hat kürzlich zwei neue bandbasierte Plug-and-Play-Datenarchivierungslösungen entwickelt, die Kunden dabei helfen, ihre Daten sicher und nachhaltig zu archivieren - FUJIFILM Kangaroo und FUJIFILM Kangaroo LITE.

Sitz der Gesellschaft:
Kleve

Jahr der Gründung:
1987

Zielgruppe:
KMUs, Behörden, Bildungseinrichtungen, Systemhäuser, VARs und Industriekunden

Marktübersicht Tape-Librarys

AUTOMATISCHE UND SKALIERBARE BACKUPS

Karl Fröhlich
speicherguide.de

Nicht zuletzt Ransomware und die steigende Zahl an Cyberangriffen sorgen für einen steten Bedarf an Tape-Lösungen. Ein gutes Preis-Leistungs-Verhältnis, ein geringer Energieverbrauch und der notwendige Medienbruch in der Backup-Strategie, inklusive Air-Gap, sprechen für den Einsatz von Magnetbändern. Richtig ausgewählt, ermöglichen sie ein bedarfsgerechtes Wachstum und schützen somit die getätigten Investitionen.

Bild: Actidata

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

Das laufende Jahr könnte wieder einmal Bewegungen in den Tape-Markt bringen: LTO-10 ist für das zweite Quartal 2025 avisiert. Derzeit gibt es dazu aber noch keine offizielle Mitteilung. Die *speicherguide.de*-Redaktion geht davon aus, dass wir vermutlich im ersten Halbjahr eine Ankündigung sehen werden. Möglicherweise erhalten dann auch OEM-Kunden erste Evaluierungsmuster. Erfahrungsgemäß dürften die ersten Serienlaufwerke frühstens gegen Ende des Jahres den Markt erreichen. Richtig verfügbar dürfte LTO-10 erst ab 2026 sein.

LTO-10 wird voraussichtlich eine native Kapazität von bis zu 36 TByte (unkomprimiert) aufs Band bringen. Komprimiert sollen bis zu 90 TByte möglich sein. Gegenüber der aktuellen LTO-9-Kapazität von 18 TByte nativ und 45 TByte komprimiert, wäre dies wieder eine Verdopplung. Zur Datenübertragung gibt es derzeit noch keine Verlautbarung.

Overland-Tandberg musste aufgeben

Offiziell nicht mehr dabei ist **Overland-Tandberg**. Der Hersteller hat zum 20. Februar seinen Betrieb eingestellt. Die deutsche Niederlassung hatte am 01. Januar am Amtsgericht Dortmund das Insolvenzverfahren eröffnet. Damit ging auch die Liquidierung der Tandberg Data GmbH einher. Ursprünglich hieß es, man trenne sich vom Tape-Business, stelle sich neu auf und wolle künftig auf die *RDX*-Technologie setzen. Dazu ist es nicht mehr gekommen.

Wieso es für Overland-Tandberg in einem eigentlich boomenden Segment nicht mehr weitergeht, ist durchaus ein Rätsel. Auch wenn sich technologisch über Jahre nicht viel tut, der Bedarf an Bandsystemen ist ungebrochen.

Tape als Bestandteil einer Cyber-Security-Strategie

»Bei unseren Mittelstandkunden herrscht nach wie vor die Notwendigkeit, sich gegen Cyberangriffe zu schützen«, erklärt **Albrecht Hestermann**, Vertriebsleiter bei **actidata**. »Die Datensicherung selbst ist ein wichtiger Bestandteil im Rahmen einer Cyber-Security-Strategie – das hat sich etabliert. Jedoch wird verstärkt auf Lösungen im eigenen Hause geschaut. Cloud als Backup ist nicht aus dem Rennen, wird aber kritischer gesehen. So haben immer öfter sowohl das Cloud-Backup als auch das Backup auf Systemen im eigenen Hause eine steigende Beliebtheitskurve. Also: Doppelt bis dreifach hält besser.«

Zudem bieten Tape-Lösungen, speziell um sich vor den Folgen von Cyber- und Ransomware-Attacken zu schützen, das so wichtige Feature Air-Gap: Air-Gap erhöht die Datensicherheit massiv und machen Backups bzw. andere Datenbestände tatsächlich immun gegen Ransomware-Angriffe.

»Kaufentscheidungen für Tape-Librarys werden aktuell hauptsächlich im Hinblick auf Skalierbarkeit, Langlebigkeit mit entsprechenden Service-Leveln sowie Nachhaltigkeit getroffen«, sagt **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 zugriffsicher gelagert.« Daher gehe es in diesem Bereich auch nicht um irgendwelche tollen Zusatzfunktionen. Die Technik müsse »einfach nur« zuverlässig funktionieren.

Trotz aller Kritik und Gegenwind, vor allem aus der Festplatten-Branche, gilt Tape als das Medium für die langfristige Datenspeicherung und Archivierung. Für Tape spricht zudem die geringeren Kosten pro GByte und der geringerer Stromverbrauch. In Zeiten begrenzter Budgets und volatiler Energiekosten verlieren diese Faktoren bei

IT-Entscheider nicht an Bedeutung. Die Einstiegsgröße für einen Bandroboter beginnt bei knapp 4.775 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 6.000 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-Librarys. Hier bilden 2U-Geräten den Einstieg, die mit bis zu 24 Tape-Slots unkomprimiert eine Gesamtkapazität zwischen 144 TByte (LTO-7) und 432 TByte (LTO-9) bereitstellen. Die *Q24*-Serie von **Qualstar** beginnt in der Anschaffung bei rund 7.000 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 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.

Midrange- und Highend-Librarys mit hoher Skalierbarkeit

Vor rund drei 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-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.

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 zwei Höheneinheiten ein und bietet bis zu acht Slots für mobile Silent Brick Pro. Extern kann die Kapazität

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.

mit stationären Silent Brick Max erweitert werden. 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 100-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 Brick Pro von Fast LTA. Es handelt sich dabei um Container, die jeweils zwölf NVMe-Module aufnehmen. Sie stecken in stabilen Aluminium-Gehäusen, die dank des geringen Gewichts von 520g gut für mobile Anwendungen vorbereitet sind. Die Laufwerke in einem Brick stammen immer aus verschiedenen Chargen, um die Wahrscheinlichkeit von Ausfällen aufgrund von Produktionsfehlern zu minimieren. Dank einer Konfiguration mit Triple-Parity (SecureNAS 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 Fileserver-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 Sekundär-Speichersysteme 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	actiLib 1U LTO-Autoloader	LTO-7	8	1	48	1,1	SAS 6G/12G, FC 8Gb	1U	ab 4.170
www.actidata.com	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	Eternus LT20 S2	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 4.300
www.fujitsu.com/de/	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	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 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	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 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	StorageTek SL4000	LTO-7	339	1-24	2.000	24,7	FC, Ficon	42U	ab 129.000
www.oracle.com/de/	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.
Qualstar	Q8	LTO-7	8	1	48	1,1	SAS 6G, FC 8Gb	1U	ab 5.100
www.qualstar.com	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	Scalar i3	LTO-7	25-400	1-24	150	0,54	SAS 6G/12G, FC 8Gb	3U-24U	ab 10.370
www.quantum.com	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	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

Bild: DALL-E

Karl Fröhlich
speicherguide.de

Backup-Software im Überblick

GEOPOLITIK & IT-SICHERHEIT: POLITIK BEEINFLUSST BACKUP-STRATEGIE

Der Markt für Backup-Software steht möglicherweise vor einem Umbruch. Das US-EU-Datenschutzabkommen steht auf der Kippe, der US-Cloud-Act wird zu einem Problem. In kleinen und mittelständischen Unternehmen müssen sich IT-Abteilungen und Geschäftsführende daher überlegen, ob sie weiterhin auf US-Anbieter vertrauen oder europäische Alternativen prüfen.

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 sowie ein Air-Gap gewährleistet werden. Zudem wird die 3-2-1-Backup-Regel um eine Kopie auf einem unveränderlichen Medium bzw. in einer unveränderlichen Form gespeichert.

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. Viele Anbieter scheuen davor zurück, Preisangabe zu veröffentlichen. Die offizielle Begründung lautet freilich, dass die Anforderungen der Unternehmen zu unterschiedlich sind. Für die *speicherguide.de*-Redaktion ist dies schlicht Quatsch, die Anbieter scheuen lediglich die Vergleichbarkeit.

Backup-Software muss noch einfacher werden

Gartners letzter Magic Quadrant »Magic Quadrant für Enterprise Backup und Recovery Software Solutions« stammt aus dem Juni 2024. Als Leader führen die Marktforscher **Veeam**, **Commvault**, **Rubrik**, **Cohesity**, **Veritas** und **Dell**.

Laut Gartner reagiert der Markt für Sicherungs- und Recovery-Software für Unternehmen auf die steigenden Herausforderungen und Bedrohungen mit einer größeren Abdeckung von Arbeitslasten, Wiederherstellungs-Funktionen und Bereitstellungsmodellen für Ransomware sowie einer Konzentration auf Einfachheit. Bis 2028 sollen 90 Prozent der Backup- und Recovery-Produkte für Unternehmen eingebettete Technologien zur Erkennung und Identifizierung von Cyberbedrohungen enthalten. Aktuell sind es noch weniger als 45 Prozent.

KI ist heute noch kein Thema. Bisher sind lediglich fünf Prozent der Backup- und Recovery-Produkte mit generativer KI (GenAI) ausgestattet. Bis 2028 sollen es 75 Prozent sein.

Bis 2028 sollen 75 Prozent der Unternehmen das Backup von SaaS-Anwendungen als kritische Anforderung priorisieren, verglichen mit 15 Prozent im Jahr 2024. Momentan nutzen 20 Prozent der Unternehmen eine gemeinsame Lösung für Backup und Recovery von Daten vor Ort und in der Cloud-Infrastruktur. Bis in drei Jahren soll dies in ebenfalls 75 Prozent der Firmen der Fall sein.

Backup-Strategien müssen weitergedacht werden

Der **Forrester**-Wave (Data Resilience Solutions, Q4 2024) zufolge steigen zudem die Anforderungen bezüglich Datensicherheit und -governance. Diese Bedürfnisse haben sich in den letzten Jahren erheblich weiterentwickelt, bedingt durch die zunehmende Nutzung von Cloud-Infrastrukturen als Service (IaaS), Software-as-a-Service (SaaS), Kubernetes und neuen Virtualisierungs-Plattformen. Bedenken hinsichtlich der Datensicherheit erfordern eine Hinwendung zu ganzheitlicheren Lösungen: Sicherheitsbedenken und insbesondere Ransomware, veranlassen Unternehmen dazu neue Fähigkeiten zu adoptieren, um zum Beispiel im Falle einer Cyberbedrohung kompromittierte Daten schneller wiederherzustellen.

Um den Bedarf an Datensicherheit zu decken, müssen Lösungen in der Lage sein, beschädigte Daten, beispielsweise von Produktionssystemen, zu identifizieren und eine Möglichkeit bereitstellen, unbeschädigte Daten aus einem früheren Backup wiederherzustellen.

Anbieter	Produkt
Acronis	Cyber Protect
Arcserve	UDP (Unified Data Protection)
Archiware	P5 Software Plattform
Bacula	Bacula Enterprise
Cohesity	Data Protect
Commvault	Commvault Cloud
Dell EMC	Networker Data Protection Suite
IBM	Spectrum Protect
Novastor	DataCenter
Quest	NetVault
Rubrik	Security Cloud
SEP	SEP sesam
Hornetsecurity	VM Backup
Veeam	Bac
Veritas	NetBackup

US-Produkte könnten zu einem Problem werden

Die wenigen deutschen Hersteller von Backup-Programmen betonen schon seit Jahren, dass eine komplett deutsche Entwicklung sowie Service und Support wichtige Argumente seien. Für **Andreas Mayer**, Senior Marketing Manager bei **SEP**, sind das zum Beispiel Produkte garantiert ohne Backdoors und Spyware, dafür mit BSI-Konformität: »Als deutscher/europäischer Hersteller unterliegen wir keinen Regularien, die uns zwingen dagegen zu verstoßen«, erklärt Mayer im *speicherguide.de*-Interview. »Somit sind auch

keine Schwachstellen und Sicherheitslücken in unserer Software eingebaut. Beim Service und Support gelangen im Unterstützungsfalle Daten und Logfiles nicht außerhalb von Deutschland. 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.«

»Ein meist unterschätztes Problem ist der Kontakt zu den Support-Teams, die bei globalen Anbietern meist in Regionen ohne ausreichenden Datenschutz sitzen«, ergänzt **Stefan Utzinger**, Geschäftsführer bei **NovaStor**. »Oft werden nicht nur Log-Files oder Benutzerdaten ausgetauscht, sondern sogar Zugang zur Infrastruktur gewährt, um ein Problem nachzustellen. Neben möglichen Datenschutzproblemen können hierdurch auch Einfallstore für Cyberkriminelle entstehen.«

So richtig gehört hat der Markt und die Kundschaft die Botschaft der deutschen Anbieter nicht. Mit den aktuellen geopolitischen Geschehnissen bekommen Produkte aus Europa allerdings noch einmal eine ganz neue Wichtigkeit.

Auch wenn es Branchenvertreter noch nicht zugeben, aber das Vorgehen der US-Regierung können EU-Unternehmen nicht so einfach tolerieren. In diversen Behörden wurden wahllos Mitarbeiter entlassen, unter anderem steht nun das Datenschutzabkommen zwischen den US und der EU vor dem Aus. Eigentlich verbündete Länder wurden erpresst, die Ukraine mit eingestellten Waffenlieferungen und Geheimdienstdaten. Das US-Unternehmen *SpaceX* drohte damit der Ukraine das Satelliten-Internet abzustellen. Die Amerikaner drohen zudem damit den Panama-Kanal und Grönland zu übernehmen und Kanada zu einem US-Bundesstat zu machen.

Wer sich gegen die USA stellt, muss mit Konsequenzen rechnen. Nachdem der südafrikanische Botschafter *Ebrahim Rasool* Kritik an der US-Regierung geäußert hatte, wurde er prompt ausgewiesen.

US-Cloud-Act ist ein Problem

Egal, wie man die US-Politik selbst bewertet, deutsche Unternehmenslenker müssen den *US CLOUD Act* neu bewerten. Dieser gestattet es US-Behörden, mit einer gültigen Gerichtsanordnung auf Daten zuzugreifen, die von US-Unternehmen gespeichert wurden, unabhängig davon, ob die Daten auf Servern in den USA oder im Ausland gespeichert sind. Dies wirft mehrere Probleme auf, insbesondere im Kontext des EU-US-Datenschutzrahmens und des allgemeinen Datenschutzbedarfs europäischer Unternehmen, die US-basierte Cloud-Dienste nutzen.

Problem: Der US-Cloud-Act ermöglicht es US-Behörden, auf Daten zuzugreifen, ohne dass der Datenbesitzer oder -verarbeiter im Ausland darüber informiert wird oder eingreifen kann. Dies führt unweigerlich zu einer Verletzung der Vertraulichkeit.

Auch dies ist nicht neu, wurde aber bisher – vor allem von den US-Anbietern selbst – als unwahrscheinliches Szenario angesehen. Das kann man nun nicht mehr so sehen. Das von Tech-Milliardär Musk gesteuerten Department of Government Efficiency (DOGE) hat sich bereits Zugriff auf das Zahlungssystem des US-Finanzministeriums verschafft – eine eigentlich bestens abgesicherte Behörde. Mit, wie zu hören ist, nicht ausreichend ausgebildeten Personal, die zudem mit ungesicherten Privat-Laptops unterwegs waren.

Daher müssen deutsche Unternehmen davon ausgehen, dass ihre auf US-Servern gespeicherten Daten nicht mehr zwangsläufig sicher sind. Im Sinne des Backup müssen Backup-as-a-Service-Angebote von US-Herstellern ebenfalls kritisch auf den Prüfstand.

Quelle: die jeweiligen Hersteller, Collage: speicherguide.de

Backup-Software aus Europa

Insbesondere im Licht des US-Cloud-Acts bieten europäische Lösungen eine höhere Unabhängigkeit und bieten auch aus Sicht der DSGVO (Datenschutz-Grundverordnung) eine größere Sicherheit in Bezug auf die Legalität der Datenverarbeitung und -speicherung. Europäische Anbieter bieten in der Regel Support in der Landessprache an, was die Kommunikation vereinfacht und Missverständnisse reduziert. Für IT-Manager ist dies besonders bei technischen Problemen oder spezifischen Anpassungen der Software von Vorteil.

Die Auswahl an möglichen Produkten ist zwar ordentlich, aber für global agierende Unternehmen doch begrenzt. Firmen, die eine Integration von Backup-Lösungen über verschiedene Kontinente hinweg benötigen, finden möglicherweise, dass europäische Anbieter nicht dieselbe Abdeckung oder denselben Integrationsgrad, wie US-Anbieter bieten. Auch fällt es IT-Entscheidern leichter dem Marktführern zu folgen, als vermeintlich unbekannte Produkte von lokalen Software-Häusern einzusetzen. Wir haben eine Auswahl an Backup-Software-Produkten aus Deutschland und der Schweiz zusammengestellt.

Acronis Cyber Protect

Wobei das im Jahr 2003 ursprünglich in Singapur gegründete **Acronis** wahrlich auch auf dem Weltmarkt zuhause ist. Mittlerweile befindet sich der Hauptsitz in Schaffhausen, Schweiz. Der globale Hersteller sieht sich längst nicht mehr nur als Anbieter von Backup-Software, sondern von Cyber-Schutzlösungen.

Während *Cyber Protect Cloud* ein cloud-basierter Backup- und Sicherheitsdienst für den Mittelstand ist, lässt sich *Acronis Cyber Protect* auch vor Ort bereitstellen und kombiniert Backup, Disaster-Recovery, Anti-Malware, Cybersecurity und Management-Tools. Die Software verarbeitet Daten und Applikationen und sieht sich als integrierte Backup-, Sicherheits- und Endpunktverwaltungslösung für physische Server, virtuelle Maschinen (VMs) vor Ort, SaaS-Workloads und Endpunkte wie Mobilgeräten. Cyber Protect unterstütz virtuelle Umgebungen von Citrix Xen, Hyper-V, Linux KVM, Nutanix, Oracle VM, oder Proxmox, Red Hat und Vmware.

Acronis bietet verschiedene Lizenzmodelle, die darauf abzielen, verschiedene Arten von Nutzern gerecht zu werden. Dazu gehören kleine und große Unternehmen sowie Managed-Service-Providers (MSP), welche die Wahl haben zwischen einem abonnementbasierten Modell, der Lizenzierung nach Workloads und Pay-as-you-go für Service-Provider. Acronis Cyber Protect Advanced kostet beispielsweise im Jahresabo für drei Server ab zirka 1.845 Euro und mit einer Laufzeit von drei Jahren ab 1.303 Euro.

Mehr zu Acronis Cyber Protect

Archiware P5

Archiware hat seinen Sitz in München und ist seit 2001 vor allem auf Archivierung spezialisiert. Die *Archiware P5 Software Suite* deckt neben der Archivierung aber Datensicherung und Synchronisation ab. Durch Parallelisierung unterstützt *P5 Backup* gleichzeitig mehrere Laufwerke, Aufgaben und Clients. Laut Hersteller sind Backups unterbrechbar und lassen sich beim nächsten Lauf automatisch komplettieren. Dabei sind selbst Teilsicherungen restaurierbar.

Als Cloud-Speicher werden unterstützt: *Amazon S3 und <i>Glacier*, *Google Cloud*, *Hitachi S3*, Microsoft Azure, *Wasabi S3*, *Backblaze B2* und *Generic S3*. Der Zugriff auf Wasabi-Speicher ist in P5 integriert. Dadurch entfällt der zusätzliche Konfigurationsschritt für die Wasabi-Autorisierung (Endpoint-DNS).

Die Preisgestaltung ist abhängig von den benötigten Modulen, der Größe des Speichers oder auch der Anzahl an Tape-Drives. Der Hersteller bietet dazu auf seiner Webseite einen P5-Produktkonfigurator. Die P5 Professional Edition beinhaltet beispielsweise alle P5-Module für die Verwendung mit fünf Server- und zehn Workstation-Agenten. Die Lizenz dafür kostet 5.950 Euro, inklusive einer Medienverwaltungs- und Speicherlizenz für 50 Slots oder 600 TByte sowie zwei Media-Drive-Lizenzen.

Mehr zur Archiware P5 Software Plattform

Bacula Enterprise

Bacula kommt aus der Open-Source-Szene und wird von **Bacula Systems** mit Sitz in Yverdon-les-Bains, Schweiz, entwickelt. Als Plattform wird physische, virtuelle, Container- und Hybrid-Cloud-Sicherung und -Wiederherstellung adressiert. Das Produkt besteht aus zwei Hauptvarianten: dem *Bacula Community*-Projekt und *Bacula Enterprise*.

Die kommerzielle Version bietet erweiterte Funktionen, professionellen Support und Zusatzmodule, die speziell für den Einsatz in großen Unternehmen und anspruchsvollen IT-Umgebungen konzipiert sind.

Bacula Enterprise soll sich durch seine Offenheit und Anpassungsfähigkeit auszeichnen. Laut Hersteller ermöglicht dies die nahtlose Integration auch komplexe IT-Umgebungen. Die Architektur ist modular ausgelegt. Kunden können die Software an ihre spezifischen Anforderungen anpassen und müssen keine unnötige Funktionen implementieren.

Die Datenmanagement-Funktionen umfassen unter anderem Deduplizierung, Kompression und Verschlüsselung. Bacula skaliert von kleinen Systemen mit wenigen Servern bis hin zu

großen Umgebungen mit Hunderten von Maschinen und PByte an Daten. Zudem unterstützt es als Speicheroptionen Disk, Tape und Cloud-Storage. Außerdem bietet die Software Optionen für automatisierte Disaster-Recovery-Prozesse, die sicherstellen sollen, dass sich kritische Daten und Systeme schnell wiederherstellen lassen, um Ausfallzeiten zu minimieren.

Mehr zu Bacula Enterprise

Hornetsecurity VM Backup

Sicherheitsspezialist **Hornetsecurity** hat seinen Sitz in Hannover. 2021 hatte das Unternehmen die in Malta ansässigen Backup-Software-Schmiede *Altaro* übernommen und die Rechte an *VM Backup* erworben. Seitdem wurde die Software kontinuierlich weiterentwickelt und ist Mitte März auf das Release 9.6.3.0 upgedatet worden.

VM Backup sichert *Hyper-V*- und *VMware*-Maschinen und ermöglicht Backups via Immutable-Cloud-Storage wie von *Azure*, *AWS*, *BackBlaze* und *Wasabi*. Ab Mai soll auch *Proxmox* unterstützt werden.

Die Software nimmt für sich eine einfache Bedienung der Backup- und Restore-Prozeduren in Anspruch. Alle wichtigen Vorgänge sollen sich ohne Handbuch oder Hilfefunktion finden lassen. Durchaus ein Argument, wenn man bedenkt, dass andere Hersteller kostenpflichtige Trainings für ihre Programme voraussetzen.

Mit der Continuous-Data-Protection (CDP) soll sich für die zu sichernden virtuellen Maschinen bessere Recovery-Point-Objectives (RPO) erzielen lassen. Mit der Concurrency-Funktion können gleichzeitige mehrerer VMs gesichert werden und via WAN-Verbindung ist eine Replikation möglich. Komprimierungs-Algorithmen und eine Inline-Deduplizierung helfen beim Speicherplatzsparen.

In einem Notfall können IT-Manager auf eine replizierte VM umschalten und die Arbeit in kürzester Zeit wieder aufnehmen.

Zudem ist der Betrieb durchgängig agentenlos. VM Backup sichert rein blockbasiert, ohne dafür einen Agenten installieren zu müssen und dies jedes in den VMs installierte Betriebssystem, sei es auch noch so alt.

Zur Wahl stehen drei Versionen (Standard, Unlimited, Unlimited Plus) die als jährliche Subscription (pro VM) oder als Dauerlizenz (pro Host) erhältlich sind. Das Abo der Unlimited-Plus-Edition beginnt in bei unter sechs Euro netto pro VM.

Weitere Informationen zu Hornetsecurity VM Backup

Novastor Datacenter

NovaStor hat seinen Sitz in Hamburg und ist seit 1999 mit Backup- und Recovery-Lösungen im Markt vertreten. *Novastor DataCenter* ist für mittelständische Unternehmen konzipiert und Teil einer Komplettlösung für Datensicherung, die neben der Software auch Service-Leistungen und einen deutschsprachiger Support aus Hamburg beinhaltet.

Die Software unterstützt heterogene Umgebungen sowie verschiedene Betriebssysteme (Windows, Linux, Unix) und alle gängigen Hypervisoren wie Hyper-V, *Nutanix*, Proxmox und Vmware sowie Datenbanken wie *MS SQL*, *MySQL*/*MariaDB*, *PostgreSQL* und *Oracle*. Zu den Sicherheitsfunktionen gehört eine Ende-zu-Ende Verschlüsselung mit TLS 1.2/1.3 sowie Backup-Verschlüsselung mit AES-256-GCM.

Datenverarbeitungs-Algorithmen und optimierte Prozesse sollen Backup- und Wiederherstellungszeiten beschleunigen. Backups lassen sich sowohl auf lokalen Speichern als auch in der Cloud sichern. Zudem wird die Integration mit verschiedenen Cloud-Speicheranbietern unterstützt.

Für die Verwaltung aller Prozesse steht eine webbasierte Benutzeroberfläche zur Verfügung. Das Interface ermöglicht die Steuerung und Bedienung aller Prozesse, egal ob für wenige konfigurierte Systeme/Backups oder für tausende. Die Backup-Strategie wird ebenfalls transparent und zentral angezeigt.

Die Lizenzierung von Novastor Datacenter basiert auf der Anzahl der zu sichernden Server und Workstations sowie der Art der zu sichernden Daten. Die Preise sind nicht öffentlich zugänglich. Der Hersteller legt Wert darauf, dass zuerst ein Gespräch stattfindet, in dem der Bedarf geklärt wird, um den Kunden bestmöglich zu unterstützen.

Mehr zu Novastor Datacenter

SEP Sesam

Der in Holzkirchen bei München ansässige Datensicherungs-Spezialist **SEP** hat sich mit seiner Backup-Software, derzeit im Release *SEP sesam Artemis*, auf die Unterstützung von allem und jedem spezialisiert. Soll heißen, es arbeitet mit nahezu jedem Betriebssystem und Hypervisoren sowie allen gängigen Anwendungen zusammen. Ende 2024 wurde unter anderem die Möglichkeiten zur Datensicherung von Proxmox-VE-Umgebungen erweitert.

Die Software unterstützt nun erweiterte Backup-Funktionalitäten auf blockbasierten Speichertypen wie *LVM-thin*, *ZFS* (local) und *CephRBD*. Mit der parallelen Sicherung mehrerer VMs soll sich SEP Sesam auch für große Umgebungen eignen.

Zudem wird auf Immutability gesetzt: 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 speicherplatzsparende 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 rund 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 3.390 Euro.

Mehr zu SEP Sesam

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

Bild via Dall-E (KI)

Karl Fröhlich
speicherguide.de

Ransom-Abwehr: Offsite-Backup & Air-Gap sind Pflicht

BACKUP-MEDIEN MÜSSEN UNANGREIFBAR SEIN

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.

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. Um den Auswirkungen einer Ransomware-Attacken vorzubeugen, sind ein Medienbruch bzw. Offsite-Backups eine Notwendigkeit.

Ein gutes, aktuelles und vollständiges Backup an einem anderen Ort (Offsite), der idealerweise 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 drei, vier Jahren eine entsprechende Strategie noch als zu aufwändig und teuer abtaten, sind verstummt. Unangreifbare Backups sind für Unternehmen alternativlos.

Ransomware hat auch den Tape-Markt wiederbelebt. Jahrzehntelang wurde das Magnetband von der Festplattenherstellern und Branche-Größen für tot erklärt. Doch Tape ist mehr als »nur« ein Archivmedium und prädestiniert für Offsite-Backups– also eine Kopie an einem anderen Standort. Dabei bleiben durch die Backup-Applikation alle Metadaten erhalten, es ist aber kein direkter Zugriff auf die Daten mehr möglich. Zudem erzeugen IT-Manager einen 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 seinen *DX*-Geräten mehrere NAS-Systeme in unterschiedlichen Größen mit integrierter Wechselfestplatte herausgebracht, mit denen sich ebenfalls ein Air-Gap realisieren lassen.

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 mitzunutzen – 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.

Bild: IBM

Nur wenn das Sicherungsmedium physikalisch von der Hardware getrennt ist, ist das Backup unangreifbar.

Das klassische Backup wie einen Server, den es zu sichern gilt und von dessen Backup dann Kopien angelegt werden, gibt es meist nur noch in kleinen Umgebunden. Auch die Backup-Software entwickelt immer mehr Funktionen und deckt immer weitere Bereiche ab. Daher braucht man Systeme, die möglichst flexibel alle diese Aspekte abdecken. Beim Einsatz des Software-basierten Objektspeichern wird Unveränderbarkeit mit der Object-Lock-Funktion realisiert. 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 greifbarer Lösung, die zu ihrem Kostenrahmen passen«, sagt **Ines Wolf**, Presales CE bei **Quantum**.. »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 die hinlegen und wie verwalte ich die? 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.

Wobei das Storage-Medium meist gar nicht entscheidend ist: »Wichtig ist vielmehr, für sich Prozesse zu definieren, die die Backup-Strategie erst möglich machen«, sagt **Jörg Riether,** Leiter IT-Verbund bei **Vitos Haina**. Gedanken über Skalierung, Datendurchsatz und Performance seien dann erst der zweite Schritt – und ohnehin in jedem Fall erforderlich. ■

Weitere Infos:

➔ Ransom-Abwehr: Offsite-Backup & Air-Gap sind Pflicht

Sicherer Schutz vor Ransomware mit Veeam

ES-3024 Server mit 24 Disk Slots

z.B. 24-Slot Server, teilbestückt mit 12 x 20 TB SAS Disks, 128 GB RAM, 2 x 10 GbE, Ubuntu Linux auf Wunsch vorinstalliert

inkl. MwSt. € 12.971,-

exkl. MwSt. € 10.900,-

„Hardened Linux Immutable Repositories“ bieten einen besonderen Schutz vor der Veränderung von Backups durch **Ransomware** oder **irrtümliches Löschen**.

Auf diese **zweite Backupstufe** hat nur der Veeam Backupserver Zugriff.

Zusätzlich werden die Daten über eine **vorgegebene Retention Zeit** vor jeder Änderung oder Löschung geschützt.

Im Falle eines Ransomware Angriffs werden die Backups vor der Wiederherstellung durch **Veeam DataLabs™ Secure Restore** auf Malware geprüft.

- **Server mit bis zu 36 Disk Slots**
- **AMD EPYC Rome 7282 Prozessor, 16 Core, 2,8 GHz**
- **bis zu 1 TB RAM**
- **Linux Betriebssystem auf gespiegelten 1 TB NVMe M.2 SSDs**
- **optimiert für den Einsatz als Hardened Backup Repository**
- **Areca Hardware RAID Controller mit dediziertem Management Port**
- **optional Erweiterungsports 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**

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 und außerdem Connectivity Produkte wie z.B. 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.

Natürlich bieten wir auch Veeam Server für die erste Backupstufe mit SAS, SATA und NVMe SSDs an.

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

Backup-as-a-Service als Teil der Datensicherungsstrategie

DATENSICHERUNG AUS SAAS-ANWENDUNGEN NOCH KEIN STANDARD

Daten aus SaaS-Anwendungen sind überwiegend ungeschützt. Nur wenige Firmen verstehen bisher, dass Software-as-a-Service zwar eine cloud-basierte Software-Infrastruktur zur Verfügung stellt, sie aber selbst für die Datensicherheit verantwortlich sind. Gartner rechnet daher bis 2028 mit umfangreichen Investitionen in SaaS-Anwendungs-Backups sowie Backup-as-a-Service.

Karl Fröhlich
speicherguide.de

Zur Datensicherungsstrategie muss künftig verstärkt auch die Sicherung von SaaS-Anwendungen als kritische Notwendigkeit eingestuft werden. Firmen beziehen zwar zunehmend Software aus der Cloud, sehen bisher aber noch nicht den Bedarf die dort generierten Daten zu sichern. **Gartner** ist hier aber hoffnungsfroh: Bis 2028 sollen 75 Prozent der Großunternehmen die Sicherung von SaaS-Anwendungen als kritische Notwendigkeit einstufen, ein erheblicher Anstieg von 15 Prozent im Jahr 2024. Die wachsende Abhängigkeit von SaaS fordert robuste Backup-Lösungen, um Daten gegen Cyberangriffe und Anbieterfehler zu schützen.

Hybridarbeit hat sich als Norm etabliert, und Unternehmen adaptieren in hoher Geschwindigkeit cloud-basierte Software-as-a-Service-Anwendungen (SaaS) wie *Microsoft 365* und *Google Workspace*. Laut **Kaseya** bilden diese mittlerweile das Rückgrat der Geschäftsprozesse. Jedoch ziehe die zunehmende Abhängigkeit von SaaS-Lösungen auch eine Welle von Cyberbedrohungen nach sich.

»SaaS-basierte Anwendungen sind zu einer bevorzugten Wahl für neue und modernisierte Implementierungen geworden, wobei die von diesen Anwendungen generierten Daten voraussichtlich zu den am schnellsten wachsenden Sets kritischer Unternehmensdaten in den nächsten fünf Jahren gehören werden«, ergänzt **Michael Hoeck**, Senior Director Analyst bei **Gartner**. Laut der neuesten Prognose erhöht sich die weltweite Endnutzerausgaben für SaaS bis 2024 um 20 Prozent auf insgesamt 247,2 Milliarden US-Dollar und erreicht voraussichtlich bis 2025 fast 300 Milliarden US-Dollar.

Das Risiko von IT-Ausfällen unterstreicht laut Hoeck die dringende Notwendigkeit für regelmäßige Sicherung und Wiederherstellung kritischer Unternehmensdaten: »Da Unternehmen zunehmend von SaaS-Technologien abhängig sind, ist es entscheidend, sicherzustellen, dass SaaS-Daten sowohl geschützt als auch wiederherstellbar sind. Angesichts der Anfälligkeit von SaaS-Daten für Fehler, Cyberangriffe und Anbieterpannen sind robuste Backup-Lösungen ebenfalls unverzichtbar.«

Einer Kaseya-Umfrage zufolge haben 87 Prozent der befragten IT-Experten 2024 Datenverluste bei SaaS-Anwendungen erlebt. Böswillige Löschungen stellten dabei die Hauptursache dar. »Obwohl erwartet wird, dass in den nächsten zwei Jahren 61 Prozent der Anwendungen und Workloads auf öffentlichen Cloud-Plattformen laufen«, erklärt **Frank DeBenedetto**, GTM General Manager, MSP Suite bei Kaseya, »fühlen sich nur 14 Prozent der IT-Leiter in der Lage, kritische SaaS-Daten binnen Minuten nach einem Vorfall wiederherzustellen. Diese Ergebnisse unterstreichen die dringende Notwendigkeit für Unternehmen, ihre Strategien zur Datenresilienz zu verstärken.«

BaaS als Teil des Datenschutzes

Gartner sieht BaaS (Backup-as-a-Service) als wesentlichen Bestandteil, um Informationen vor Datenverletzungen

oder Sicherheitslücken innerhalb von Cloud-Workloads zu schützen. Derzeit erwarten die Marktforscher, dass 75 Prozent der großen Unternehmen bis 2028 BaaS neben On-Premises-Tools adoptieren werden.

Das bedeutet auch, dass Unternehmen im Jahr 2025 mehr Aufmerksamkeit auf die Spezifikationen des Shared-Responsibility-Models legen müssen. Das Beibehalten und Sichern von Datensätzen erfordert, dass Firmen ihre Maßnahmen zum Datenschutz überprüfen, einschließlich verschiedener Dienstanbieter in diesem Bereich. Der Kunde ist verantwortlich für die Implementierung und Aufrechterhaltung von Datenschutz- und Sicherheitsmaßnahmen für die Komponenten, die der Kunde bereitstellt und kontrolliert. Und das ist ein entscheidender Grund für die Diversifizierung von Backup-Anbietern.

Es wird geschätzt, dass 60 Prozent der Unternehmen fälschlicherweise annehmen, dass ihre SaaS-Anbieter allein für den Datenschutz verantwortlich sind. Das ist einer der Gründe, warum Drittanbieter-Software wie *GitProtect.io* als umfassende Sicherheitswerkzeuge in Betracht gezogen werden könnte, wenn die Sicherheitsmaßnahmen unzureichend sind. Dies könnte sich auf begrenzten API-basierten Datenzugriff und Wiederherstellungsoptionen beziehen. Dies wird auch Fragen zum angemessenen Datenschutz aufwerfen und die Unterstützung für Drittanbieterlösungen für Backups stören. Darüber hinaus werden Unternehmen im Jahr 2025 immer noch mit einem Mangel an Branchenstandardisierung in diesem Bereich konfrontiert sein.

»Die Integration von BaaS ist entscheidend, um Cloud-Workloads zu schützen und die betriebliche Kontinuität zu gewährleisten«, mahnt Hoeck. »Außerdem müssen Unternehmen das Modell der geteilten Datenverantwortung bei SaaS-Anwendungen verstehen und die Datenschutzmaßnahmen ihrer Anbieter bewerten. Sind diese Maßnahmen unzureichend, sollten Drittanbieterlösungen in Betracht gezogen werden, um einen umfassenden Datenschutz zu garantieren.«

SaaS-Kunden müssen selbst auf ihre Daten aufpassen

»Der Schutz und die Wiederherstellung von SaaS-Anwendungen waren für viele Unternehmen oft eine niedrigere Priorität«, sagte Hoeck. »Dies liegt an der Verwirrung über die Verantwortung des nativen SaaS-Anbieters für den Datenschutz und dem Mangel an branchenweiter Standardisierung. Begrenzter API-basierter Datenzugang zum Schutz und zur Wiederherstellung durch native SaaS-Anbieter kompliziert den effektiven Datenschutz und verlangsamt die Unterstützung für Drittanbieter-Backup-Lösungen.«

Dennoch wächst der Markt für SaaS-Anwendungs-Backups rapide, anfangs angeführt von spezialisierten Start-ups, jetzt aber auch von umfassend etablierten Unternehmen für Backup- und Wiederherstellungs-Software.

Um SaaS-basierte Anwendungsdaten effektiv zu schützen, schlägt Gartner vor, dass Organisationen sich auf Folgendes konzentrieren:

- **Governance-Bewertung:** Datenschutz- und Wiederherstellungsfähigkeiten in die Governance-Bewertung von SaaS-Anwendungen mit einschließen.
- **Fähigkeiten des Anbieters:** Überprüfung der Fähigkeit des SaaS-Anbieters, Daten vor allen möglichen Verlustszenarien zu schützen und wiederherzustellen.
- **Drittanbieterlösungen:** Verwendung von Drittanbieter-SaaS-Backup-Lösungen, um die nativen Fähigkeiten von SaaS-Anbietern zu ergänzen. Diese Lösungen können die Verwaltung verbessern, den Schutz mehrerer SaaS-Anwendungen zentralisieren und orchestrieren, Prozesse vereinfachen und verbesserte granulare Wiederherstellungsfähigkeiten bieten.

»Da der Markt reift, ist es für Unternehmen unerlässlich, gründliche Governance-Bewertungen durchzuführen und die Fähigkeiten ihrer SaaS-Anbieter zu überprüfen«, meint Hoeck. »Die Nutzung von Drittanbieter-Backup-Lösungen kann den Datenschutz und die Wiederherstellung erheblich verbessern und sicherstellen, dass Unternehmensdaten sicher und zugänglich bleiben.«

Herausforderungen im Backup-Management

Das Management von Backups für SaaS-Anwendungen stellt eine Herausforderung dar, die je nach Plattform und Nutzergruppe variieren. Die Kaseya-Umfrage zeigt deutliche Schmerzpunkte für Nutzer von Microsoft 365, Google Workspace und Salesforce:

- **Datenwiederherstellungsprobleme:** Nutzer von Google Workspace (23%) und Salesforce (23%) berichten von Problemen bei der Datenwiederherstellung, verglichen mit 20 Prozent der Microsoft-365-Nutzer.
- **Alarmierung und Berichterstattung:** Nutzer von Google Workspace (11%) haben die größten Herausforderungen beim Einrichten und Verwalten von Alarmen. Microsoft 365 (8%) und Salesforce (8%) liegen nicht weit dahinter.
- **Einhaltung von Compliance:** Salesforce-Nutzer (24%) kämpfen am meisten mit der Aufrechterhaltung der Compliance, gefolgt von Google Workspace (23%) und Microsoft 365 (21%).
- **Zunehmende zeitliche Belastung durch Backup-Management:** Das Management von Backups ist für IT-Teams zunehmend zeitintensiv geworden:
  - Über 50 Prozent der Befragten verbringen täglich mehr als zwei Stunden – was mehr als 10 Stunden pro Woche entspricht – mit der Überwachung, Verwaltung und Fehlerbehebung von Backups.
  - Der Anteil derjenigen, die täglich weniger als eine Stunde verbringen, ist von 39 Prozent in 2022 auf 23 Prozent in 2024 stark gesunken, während diejenigen, die täglich drei oder mehr Stunden widmen, von fünf Prozent in 2022 auf 14 Prozent in 2024 gestiegen sind.

Backup-Infrastruktur: Ein Viertel noch ohne Richtlinien & Kontrolle

Die Mehrheit der Organisationen berichtet, dass sie Richtlinien und Kontrollen zur Sicherung des Zugriffs auf ihre Backups in Schlüsselbereichen implementiert haben, einschließlich öffentlicher Cloud (77%), Servern oder virtuellen Maschinen (76%), SaaS-Anwendungen (74%) und Endpunkten/PCs (73%).

»Obwohl diese Zahlen einen proaktiven Ansatz widerspiegeln, fehlen immer noch rund 25 Prozent der Organisationen Richtlinien und Kontrollen für die Sicherheit von Backups«, sagt Kaseya-General-Manager DeBenedetto. Dies stelle in zunehmend hybriden und Multicloud-Umgebung eine Verwundbarkeit dar. ■

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, S3 Object-Lock und Cloud-basierte Lösungen.

Karl Fröhlich
speicherguide.de

Kerstin Mende-Stief
speicherguide.de

Für Unternehmen und ihre digital gespeicherten Daten ist Cyberkriminalität eine ernste Bedrohung: Schätzungen von **Statistas 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**
- **Signaturen und Hashes**

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 **Amazon**s *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-Ma-

nager 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.

Bild: via Dall-E

S3 Object-Lock ist eine Funktion in AWS S3, die es ermöglicht, Objekte in einem unveränderlichen Zustand zu speichern, um sie vor Löschung oder Modifikation zu schützen.

Planung und Beschaffung

Bei der Auswahl von Immutable-Storage-Lösungen für Unternehmen müssen viele Faktoren berücksichtigt werden. Zu den wichtigsten Kriterien zählen:

1. Datenretention: Die Lösung sollte langfristige Datenretention ermöglichen, um sicherzustellen, dass Daten für die erforderliche Zeit verfügbar bleiben.

2. Skalierbarkeit: Die Lösung sollte skalierbar sein, um den wachsenden Datenbedarf zu befriedigen.

3. Sicherheit: Die Lösung sollte eine hohe Sicherheit bieten, um Daten vor unbefugten Zugriff, Verlust oder Zerstörung zu schützen.

4. Kompatibilität und Integration: Die Lösung sollte kompatibel sein mit den bestehenden Systemen und Anwendungen des Unternehmens sowie sich leicht (z. B. über Standard-Schnittstellen und -Protokolle) integrieren lassen.

5. Verwaltung: Die Lösung sollte einfach zu verwalten und zu warten sein. Idealerweise lässt sich die Plattform in bestehende Automatisierungslösungen wie Ansible integrieren.

6. Compliance: Die Lösung sollte die Anforderungen von Gesetzen und Vorschriften wie GDPR, HIPAA erfüllen.

7. Datenzugriff: Die Lösung sollte sicherstellen, dass nur autorisierte Benutzer auf die Daten zugreifen können.

8. Support: Die Lösung sollte einen guten Support bieten, um Fragen und Probleme zu beantworten und möglichst schnell zu lösen.

Im Rahmen der Planung ist die Beantwortung der folgenden Fragen hilfreich:

- Welche Art von Daten wird gespeichert?
- Wie lange müssen die Daten gespeichert werden?
- Welche Sicherheitsanforderungen müssen erfüllt werden?
- Wie skalierbar muss die Lösung sein?
- Welche Kosten sind für die Lösung die Anschaffung sowie Betrieb zu erwarten?
-

Indem Unternehmen diese Fragen beantworten und die oben genannten Faktoren berücksichtigen, können sie eine Immutable-Storage-Lösung auswählen, die ihre spezifischen Bedürfnisse erfüllt und Daten zuverlässig speichert.

Immutability: Ein Risiko bleibt

Bei allen Vorteilen sind IT-Anwender trotzdem gut beraten Immutable-Systeme skeptisch zu betrachten: »Auch ihnen liegt immer irgendein Betriebssystem zugrunde«, mahnt **Jörg Riether**, Leiter IT-Verbund 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 würden viele Backup-System auch im operativen Betrieb genutzt – und dafür seien eben Online-Datenspeicher ideal. ■

Lesen Sie auch auf speicherguide.de auch:

➔ **Immutable-Storage: Was es ist und wie es funktioniert**

➔ **Doc Storage: Immutable-Backups: Sicherungen müssen unveränderlich sein**

Ihre Backups sind nur sicher, wenn Ihre Backups sicher sind!

DATACORE

storage-magazin.de
Eine Publikation von 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.

Unser Team

Karl Fröhlich
Chefredakteur
speicherguide.de

Michael Baumann
Redaktion
speicherguide.de

Peter Marwan
Redaktion
speicherguide.de

Jens Leischner
Redaktion
speicherguide.de

Bettina Röber
Mediaberatung
speicherguide.de

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:
Karl Fröhlich, Peter Marwan, Kerstin Mende-Stief

Schlussredaktion:
Brigitte Scholz

Titelbild:
ChatGPT/Dall-E

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
Tel. +49 177 8487001
E-Mail: broeber@speicherguide.de