storage-magazin.de

Eine Publikation von speicherguide.de

Bild: speicherguide.de via ChatGPT/DALL-E

Backup für den Mittelstand

Datenhoheit & Ausfallsicherheit durch resiliente Backup-Konzepte

2026
02

Editorial

DIGITALE SOUVERÄNITÄT VERÄNDERT DEN BACKUP-MARKT

Karl Fröhlich
Chefredakteur
speicherguide.de

Liebe Leserinnen und Leser,

die Diskussion über digitale Souveränität erreicht inzwischen auch den Markt für Backup-Software. Die Frage ist nicht mehr nur technischer Natur. Sie betrifft auch den Rechtsraum, in dem Software entsteht und betrieben wird.

Kurzfristig ist ein grundlegender Umbruch im Backup-Markt allerdings unwahrscheinlich. Zu dominant ist die Stellung der großen US-Anbieter und zu tief sind ihre Plattformen in vielen IT-Umgebungen verankert. Unternehmen haben über Jahre in Backup-Architekturen investiert, sie in Betriebsprozesse integriert und mit Monitoring-, Sicherheits- und Cloud-Systemen verzahnt. Ein kompletter Austausch dieser Infrastruktur wäre technisch aufwendig und wirtschaftlich kaum zu rechtfertigen.

Trotzdem dürfte die Debatte Folgen für den Markt haben. Digitale Souveränität entwickelt sich zu einem Entscheidungskriterium bei der Auswahl von IT-Infrastruktur. Vor einem Jahr wäre diese Perspektive noch schwer vorstellbar gewesen. Nach einem Jahr Trump-Regierung prüfen Unternehmen jedoch genauer, wo Software entwickelt wird, welchem Rechtsraum Anbieter unterliegen und wie Support- oder Cloud-Strukturen organisiert sind.

Für europäische Software-Anbieter eröffnet sich damit ein neues Marktfenster. Doch diese Chance entsteht nicht automatisch. Wer davon profitieren will, muss sichtbar werden, stärker kommunizieren und auch in Marketing investieren.

Die politische Entwicklung in den USA schafft dafür ein ungewöhnliches Umfeld. Ob beabsichtigt oder nicht: Die US-Regierung serviert europäischen Anbietern derzeit ein attraktives Marktfeld. Doch erobern müssen sie es selbst. Dazu gehört auch, die eigene Stimme zu erheben und sich zuzutrauen, gegen die etablierten Plattformen aus den USA anzutreten.

Der wahrscheinlichste Effekt ist daher keine abrupte Abkehr von US-Anbietern, sondern eine breitere Marktstruktur. Internationale Plattformen werden weiterhin eine zentrale Rolle spielen. Gleichzeitig könnten europäische Lösungen in einzelnen Segmenten an Bedeutung gewinnen.

Für IT-Verantwortliche bedeutet das vor allem eines: Die Auswahl von Backup-Software wird künftig nicht mehr nur über Funktionen, Performance oder Preis entschieden. Auch Aspekte wie Rechtsraum, Anbieterstruktur und die betriebliche Kontrolle über die eigene Datensicherung fließen stärker in die Bewertung ein.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Bild: speicherguide.de via DALL-E

Datensicherung, Recovery und Cyber-Resilienz

BACKUP IM MITTELSTAND: RECOVERY IST DER MASSSTAB

Backup im Mittelstand ist heute mehr als Datensicherung. Der Markt wächst, verschiebt sich aber in Richtung Services, Cloud und Cyber-Resilienz. Entscheidend ist nicht mehr die Kopie allein, sondern die belastbare Wiederherstellung. Air-Gap, Immutability, Archivierung und Datensouveränität rücken damit ins Zentrum.

Backup-Software im Überblick

BACKUP-PLATTFORMEN ZWISCHEN CYBERRESILIENZ UND DIGITALER SOUVERÄNITÄT

Backup-Software hat sich längst zu umfassenden Data-Protection-Plattformen entwickelt. Cyber-Resilienz, SaaS-Backup und Hybrid-Cloud-Schutz prägen heute den Markt. Gleichzeitig geraten rechtliche Rahmenbedingungen stärker in den Blick: Die dominierenden Anbieter stammen aus den USA – während europäische Unternehmen ihre Abhängigkeiten kritischer hinterfragen.

Bild: speicherguide.de via DALL-E

Backup, Disaster-Recovery und Ausfallsicherheit

WENN DER STANDORT AUSFÄLLT UND DIE IT WEITERLÄUFT

Bild: speicherguide.de/NCS via DALL-E

Übersicht
Storage-Anbieter


speicherguide.de
storage-magazin.de
Eine Publikation von speicherguide.de
Backup für den Mittelstand
Datenhoheit & Ausfallsicherheit durch resiliente Backup-Konzepte
2026
02
Daten schützen ist kein Projekt.
Strategien, Tools und Best Practices
für Backup, Security und Recovery.
Jetzt Newsletter abonnieren

Bild: speicherguide.de via DALL-E

Karl Fröhlich
speicherguide.de

Datensicherung, Recovery und Cyber-Resilienz

BACKUP IM MITTELSTAND: RECOVERY IST DER MASSSTAB

Backup im Mittelstand ist heute mehr als Datensicherung. Der Markt wächst, verschiebt sich aber in Richtung Services, Cloud und Cyber-Resilienz. Entscheidend ist nicht mehr die Kopie allein, sondern die belastbare Wiederherstellung. Air-Gap, Immutability, Archivierung und Datensouveränität rücken damit ins Zentrum.

Je nach Marktdefinition liegt der aktuelle Weltmarkt für klassische Enterprise-Backup- und Recovery-Software derzeit bei gut zehn bis knapp zwölf Milliarden US-Dollar. **Fortune Business Insights** taxiert ihn für 2025 auf 11,78 Milliarden US-Dollar und erwartet für 2026 bereits 13,06 Milliarden US-Dollar sowie 29,72 Milliarden US-Dollar bis 2034. **Mordor Intelligence** kommt für 2025 auf 10,63 Milliarden US-Dollar und auf 16,86 Milliarden US-Dollar bis 2030. Die Abweichung von gut einer Milliarde US-Dollar ist kein echter Widerspruch, sondern dürfte vor allem auf unterschiedliche Marktdefinitionen, Modellgrenzen und Prognosezeiträume zurückgehen. Als belastbare Klammer lässt sich daraus ableiten, dass das Kernsegment Backup und Recovery aktuell mit rund 10 Prozent pro Jahr wächst und damit ein reifer, aber weiterhin klar expandierender Software-Markt bleibt.

Service-Modelle wachsen schneller als der klassische Kernmarkt

Deutlich mehr Tempo zeigen die service-basierten Teilmärkte. **MarketsandMarkets** beziffert den weltweiten Data-Protection-as-a-Service-Markt auf 26,04 Milliarden US-Dollar im Jahr 2024 und erwartet 74,91 Milliarden US-Dollar bis 2030. Das entspräche einer jährlichen Wachstumsrate von 19,3 Prozent. **Grand View Research** liegt für denselben Grundtrend sogar noch höher und schätzt den DPaaS-Markt auf 28,07 Milliarden US-Dollar im Jahr 2025 sowie 179,06 Milliarden US-Dollar bis 2033 bei einer CAGR von 26,8 Prozent.

Auch im enger gefassten Backup-and-Restore-DRaaS-Markt sieht MarketsandMarkets viel Bewegung und projiziert ein Wachstum von 5,54 Milliarden US-Dollar im Jahr 2025 auf 17,52 Milliarden US-Dollar bis 2032 bei 17,9 Prozent CAGR. Für die Einordnung heißt das: Klassische Backup-Software wächst weiter, die eigentliche Investitionsdynamik verlagert sich aber in abonnierte und gemanagte Schutzmodelle wie Backup-as-a-Service, Disaster-Recovery-as-a-Service und allgemein Data-Protection-as-a-Service.

Bild: SEP

Lutz Preußners
SEP

»Datensicherung wird heute an Wiederherstellungsfähigkeit und Cyber-Resilienz gemessen.«

Cloud, Hybrid-Betrieb und Cyber-Resilienz treiben die Budgets

Innerhalb des Kernmarkts verschieben sich die Budgets klar in Richtung cloud-naher und hybrider Betriebsmodelle. Laut Mordor Intelligence kamen Hybrid- und Multi-Cloud-Modelle 2024 bereits auf 45,32 Prozent Marktanteil. Große Unternehmen hielten 63,39 Prozent Umsatzanteil, und Nordamerika lag mit 37,71 Prozent vorn. Grand View Research ergänzt dazu, dass der globale Cloud-Backup-Markt 2024 bereits 5,49 Milliarden US-Dollar erreicht haben soll und bis 2030 auf 20,34 Milliarden US-Dollar wachsen könnte. Für Europa beziffert Grand View Research den Cloud-Backup-Teilmarkt auf 1,33 Milliarden US-Dollar in 2024 und 4,86 Milliarden US-Dollar in 2030. Die Marktforscher sehen dies als Indiz, dass Cloud-basierte Schutzmodelle nicht länger nur eine Ergänzung sind, sondern zum eigentlichen Wachstumsmotor des Backup-Umfelds werden.

SaaS-Backups: Vom Sonderfall zur Pflichtdisziplin

Gartner erwartet, dass bis 2028 rund 75 Prozent der Unternehmen die Sicherung von SaaS-Anwendungen als kritische Anforderung priorisieren werden. 2024 lag dieser Wert noch bei 15 Prozent. Ebenfalls bis 2028 sollen 75 Prozent der Großunternehmen Backup-as-a-Service zusätzlich zu On-Premises-Werkzeugen einsetzen, um Cloud- und lokale Workloads gemeinsam abzusichern. Das passt zur Marktentwicklung der Analystenhäuser insgesamt: Der Backup-Markt verschiebt sich von punktueller Datensicherung hin zu umfassender Data-Protection und Cyber-Resilienz über hybride, cloud-basierte und service-orientierte Betriebsmodelle.

Bild: Quantum

Ines Wolf
Quantum

»Backup wird erst mit verlässlicher Wiederherstellung zur belastbaren Resilienz.«

Backup wird zur Resilienz-Disziplin

Diese Entwicklung zeigt sich auch im Mittelstand immer deutlicher. Entscheidend ist dort nicht mehr allein, ob Daten gesichert werden, sondern ob sich Systeme und Informationen nach einem Ausfall oder Angriff schnell, kontrolliert und vollständig wiederherstellen lassen. Backup entwickelt sich damit von einer klassischen IT-Pflichtaufgabe zu einem Baustein für Cyber-Resilienz, Verfügbarkeit und Compliance.

»Backup allein ist nicht genug, Geschwindigkeit und Garantie der Wiederherstellung sind entscheidend«, sagt **Ines Wolf**, Manager Presales Central Europe bei **Quantum**. Genau diese Verschiebung prägt derzeit viele Diskussionen im Markt. Denn mit jeder neuen Angriffswelle, mit strengeren regulatorischen Vorgaben und mit wachsendem Digitalisierungsgrad steigt der Druck auf Unternehmen, nicht nur Kopien ihrer Daten vorzuhalten, sondern den Wiederanlauf im Ernstfall belastbar sicherzustellen.

»Der Markt hat sich deutlich vom klassischen Datensicherungsmarkt hin zu einem Markt für Cyber-Resilienz und Wiederherstellungsfähigkeit entwickelt«, ergänzt **Lutz Preußners**, Chief Growth Officer bei **SEP**. Damit beschreibt er eine Entwicklung, die

auch andere Hersteller beobachten. Backup wird nicht mehr isoliert betrachtet, sondern als Teil einer übergeordneten Sicherheits- und Betriebsstrategie.

»Backup wird zunehmend als strategischer Bestandteil der Unternehmenssicherheit verstanden und nicht mehr nur als technische Grundversorgung«, erwartet **Stefan Utzinger**, CEO bei **Novastor**. Das trifft vor allem den Mittelstand, der in den vergangenen Jahren seine IT-Landschaften stark ausgebaut hat, häufig aber mit begrenzten personellen und finanziellen Ressourcen arbeiten muss. Die Datensicherung steht dadurch unter einem doppelten Druck. Sie soll zugleich robuster, schneller und einfacher beherrschbar werden.

»Die reine Cloud-Euphorie ist einer pragmatischeren Bewertung gewichen, bei der Wiederherstellungsgeschwindigkeit und Datensouveränität stärker gewichtet werden als bisher«, erklärt **Hannes Heckel**, Head of Marketing bei **Fast LTA**. Der Markt werde nüchterner. Nicht jede Auslagerung in die Cloud werde noch automatisch als Fortschritt verstanden. Vielmehr rücken Fragen in den Vordergrund, die im Alltag gern nach hinten geschoben werden: Wie schnell lassen sich Systeme wiederherstellen, wie gut sind Backups gegen Manipulation abgesichert und ob es eine letzte, wirklich getrennte Rückfallebene gibt.

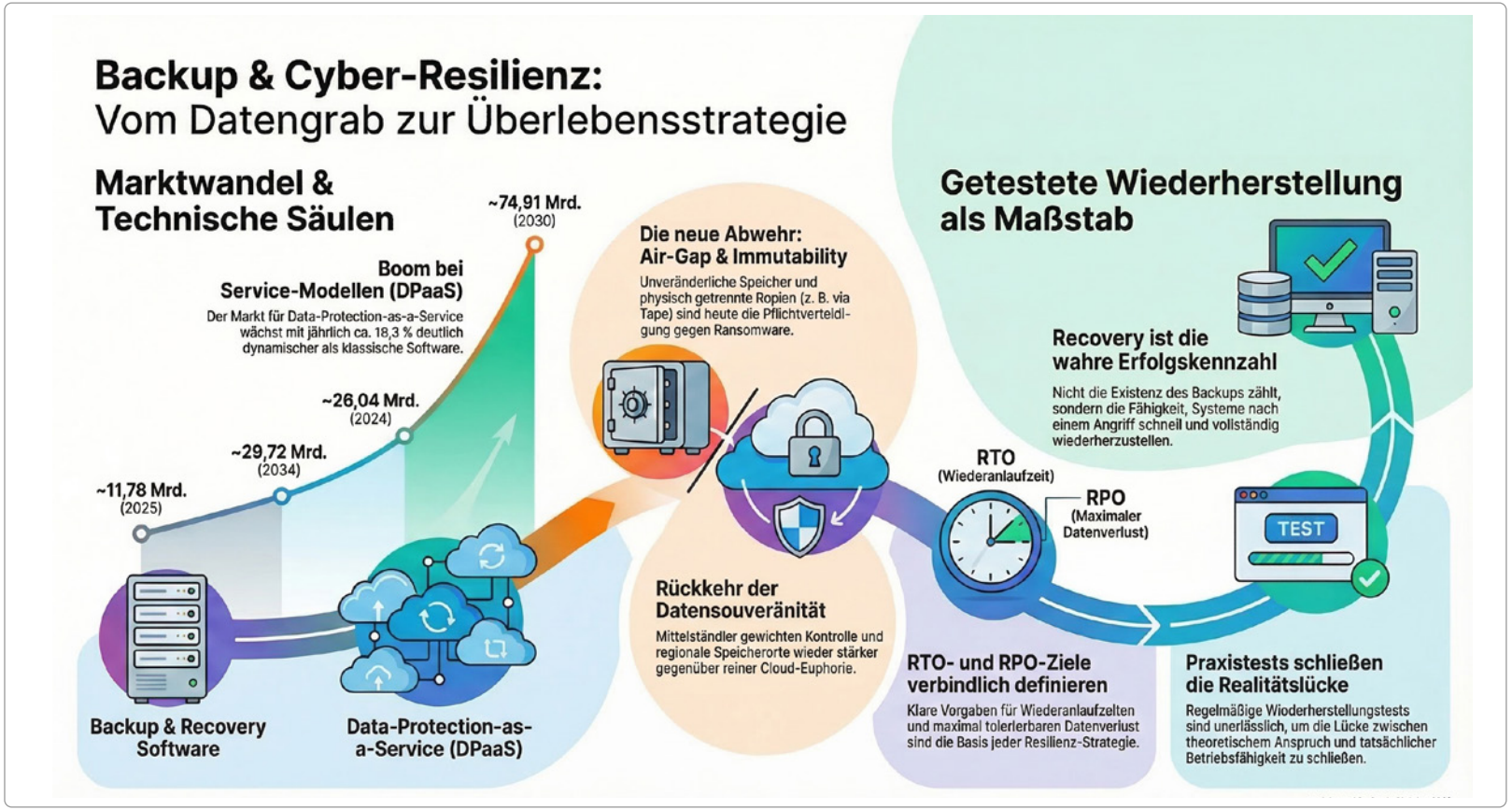


Bild: speicherguide.de via Notebook LM

Wiederherstellung wird zum eigentlichen Maßstab

Auffällig ist, dass nahezu alle Anbieter denselben wunden Punkt benennen. Viele Unternehmen sichern Daten, aber sie planen die Wiederherstellung noch immer nicht konsequent genug durch. »Die Lücke zwischen Anspruch und Realität ist groß, weil moderne IT-Umgebungen komplex, verteilt und hochgradig voneinander abhängig sind«, sagt Preußners. In vielen Fällen sei zwar ein Backup vorhanden, doch Wiederanlaufzeiten, Zuständigkeiten und Abläufe würden nicht sauber getestet.

Auch Quantum-Managerin Wolf beschreibt kein Erkenntnisproblem, sondern ein Umsetzungsproblem. Konzepte wie 3-2-1-1-0, unveränderliche Backups, Zero-Trust-Prinzipien und Automatisierung seien in vielen IT-Abteilungen durchaus bekannt. Im Alltag würden sie aber noch zu selten konsequent umgesetzt. Genau darin liegt derzeit eine der größten Schwächen vieler Backup-Strategien.

»Die entscheidende Frage, wie schnell ich nach einem Totalausfall wieder arbeitsfähig bin, bleibt häufig unbeantwortet«, mahnt Heckel. RPO- und RTO-Ziele seien vielerorts nicht

ausreichend definiert und noch seltener realistisch getestet. Ein vorhandenes Backup vermittle dann zwar Sicherheit, liefere im Ernstfall aber womöglich nicht die erwartete Betriebsfähigkeit zurück. Das ist unangenehm, aber eben genau der Punkt, an dem aus Datensicherung Resilienz werden müsste.

Auch Novastor-Manager Utzinger sieht hier Nachholbedarf. Unternehmen dächten Sicherungskonzepte oft noch zu stark von der Datenspeicherung her und zu wenig von der Betriebswiederherstellung. Entscheidend sei aber, ob sich Systeme und Daten in der geforderten Zeit tatsächlich wieder nutzbar machen lassen. Erst dann werde aus einer Datensicherung eine funktionierende Recovery-Strategie.

Bild: Fast LTA

Hannes Heckel
Fast LTA

»Wiederherstellungsgeschwindigkeit und Datensouveränität prägen Backup-Strategien im Mittelstand.«

Air-Gap und Immutability werden zum Pflichtprogramm

Technisch lässt sich aus den Stellungnahmen ein klarer Trend ablesen. Unternehmen setzen stärker auf mehrstufige Schutzkonzepte mit unveränderlichen Sicherungen, Off-Site-Backup, isolierten Recovery-Prozessen und physisch getrennten Kopien. »Wir sehen eine deutlich steigende Nachfrage nach Off-Site-Backup«, erklärt **Albrecht Hestermann**, Head of Sales bei **actidata**. Viele mittelständische Unternehmen würden ihre Backup-Umgebungen derzeit überarbeiten oder neu aufbauen, nachdem Investitionen zuvor eher in Firewalls und Sicherheits-Software geflossen seien.

Das ist eine nachvollziehbare Entwicklung. Ransomware greift längst nicht mehr nur Primärdaten an, sondern gezielt auch die Sicherungs-Infrastruktur. »Klassisches Backup schützt gegen Datenverlust durch technische Defekte oder menschliche Fehler«, erklärt Fast-LTA-Manager Heckel. »Gegen gezielte Cyberangriffe reicht es nicht.« Backup-Daten im selben Netzwerk und mit denselben Zugangsdaten wie die Produktiv-Daten vorzuhalten, sei ein erhebliches Risiko.

Wolf ergänzt, dass Unternehmen heute Restore-Geschwindigkeiten im Minutenbereich erwarteten, klassische Infrastrukturen dafür aber oft gar nicht ausgelegt seien. Daraus ergibt sich fast zwangsläufig ein mehrschichtiges Modell. Gefragt sind schnelle Primär-Ziele für tägliche Sicherungen, kapazitätsoptimierte zweite Ebenen und zusätzlich eine Air-Gap-Kopie als letzte Verteidigungslinie. SEP-Manager Preußners verweist in diesem Zusammenhang auf Immutable-Storage, belastbare Disaster-Recovery-Konzepte und regelmäßige Tests, damit der Wiederanlauf nicht nur auf dem Papier funktioniert.

Weniger Werkzeuge, mehr Automatisierung

Neben Resilienz und Wiederherstellbarkeit rückt auch die Vereinfachung der Backup-Landschaften in den Mittelpunkt. Der Mittelstand sucht nach Plattformen, die weniger Komplexität verursachen und knappe IT-Ressourcen entlasten. »Der Wunsch nach zentralisierten Plattformen und konsolidierten Werkzeugen nimmt deutlich zu«, sagt Utzinger. Unternehmen wollten die Zahl der Tools verringern, um Backup und Recovery einfacher steuern zu können.

Auch Wolf sieht hier eine klare Entwicklung. KI-gestützte Anomalie-Erkennung im Backup-Datenstrom, automatische Tiering-Konzepte sowie Deduplizierung und Kompression sollen Datensicherung nicht nur sicherer, sondern auch wirtschaftlicher machen. Dahinter steht kein technischer Selbstzweck. Der Mittelstand braucht Lösungen, die im Alltag beherrschbar bleiben. Gerade Fachkräftemangel, Zeitdruck und wachsende Datenmengen verschärfen die Anforderungen.

Bild: Novastor

Stefan Utzinger
Novastor

»Backup ist Teil der Unternehmenssicherheit und nicht mehr nur Grundversorgung.«

Dass Managed Services an Bedeutung gewinnen, passt in dieses Bild. Utzinger beobachtet, dass viele Unternehmen Partner suchten, die Backup und Recovery als Service übernehmen. Das sei weniger ein Kontrollverlust als vielmehr eine pragmatische Reaktion auf überlastete IT-Teams und steigende Anforderungen.

Archivierung darf nicht unter den Tisch fallen

Bedenken sollten IT-Manager die Abgrenzung zwischen Backup und Archivierung. »Aus unserer Sicht ist es wichtig, Daten beispielsweise zu vergangenen Quartalen oder Monaten regelmäßig zu archivieren«, fordert Actidata-Manager Hestermann. »Die Gefahr eines Datenverlustes durch ein Backup, welches Trojaner enthält, wird signifikant unterschätzt.« Damit spricht er einen Punkt an, der in vielen Backup-Diskussionen zu kurz kommt. Denn auch ältere Sicherungen können kompromittierte oder unerkannte Schad-Software enthalten.

Backup und Archivierung werden in der Praxis noch immer gern vermischt, obwohl sie unterschiedliche Aufgaben erfüllen. Backup dient der schnellen Wiederherstellung aktueller Daten und Systeme. Archivierung soll Informationen langfristig, unverändert und nachvollziehbar aufbewahren. Gerade bei Compliance, Langzeit-Aufbewahrung und forensischer Nach-

vollziehbarkeit reicht ein normales Backup daher oft nicht aus.

»Data-Protection ist mit einem einfachen Backup auf einem Online-System nicht hinreichend sichergestellt«, unterstreicht **Philipp Stevens**, Business Development Manager bei **Fujifilm**. Für eine nachhaltige Strategie empfiehlt er ein Offline-Archiv mit Magnetband-Technologie, »weil es einen echten Air-Gap« ermögliche. Damit rückt Tape wieder stärker in den Fokus, insbesondere dann, wenn es um Cyber-Resilienz, Langzeit-Aufbewahrung und eine wirklich getrennte Sicherheitskopie geht.

On-Premises und Hybrid-Modelle werden nüchterner bewertet

Mehrere Hersteller beobachten zudem, dass sich der Markt etwas von einer einseitigen Cloud-Orientierung entfernt. Das bedeutet nicht das Ende von Cloud-Backup oder Cloud-Services. Es zeigt vielmehr, dass Unternehmen Kosten, Kontrolle, Verfügbarkeit und rechtliche Rahmenbedingungen wieder differenzierter abwägen.

Stevens sieht dabei einen klaren Trend zu On-Premises-Lösungen und zugleich wachsendes Interesse an europäischen Cloud-Angeboten. Hintergrund seien globale Spannungen, regulatorische Unsicherheiten und Datenschutzbedenken gegenüber Anbietern aus anderen Rechtsräumen. Auch Utzinger beobachtet eine Wiederentdeckung von On-Premises-Komponenten, häufig in Kombination mit Cloud-Bausteinen. Verfügbarkeit, Kontrolle und Kostenbewusstsein spielten dabei eine zentrale Rolle.

Bild: Fujifilm

Philipp Stevens
Fujifilm

»Echter Air-Gap und Langzeit-Aufbewahrung rücken Tape wieder in den Fokus.«

Wolf ergänzt, dass steigende Speicherpreise und Engpässe bei HDDs und SSDs viele Unternehmen dazu zwingen, ihre Backup- und Recovery-Strategien neu zu bewerten. Hybride Architekturen und auch Tape als Storage-Tier könnten dadurch wieder relevanter werden. Datensicherung wird damit stärker zur Architekturfrage. Unternehmen entscheiden nicht mehr nur zwischen lokal und Cloud, sondern kombinieren unterschiedliche Ebenen gezielt nach Performance, Kosten, Souveränität und Schutzbedarf.

Datensouveränität rückt in den Vordergrund

Das Thema Datensouveränität gewinnt auch im Backup-Umfeld deutlich an Gewicht. Die Zusammenarbeit mit US-Anbietern wird zwar nicht grundsätzlich infrage gestellt, sie wird im Mittelstand aber nüchterner und kritischer bewertet als noch vor wenigen Jahren. Hintergrund sind geopolitische Unsicherheiten, Datenschutzfragen, Lizenz- und Preismodelle sowie die Sorge vor zu starken Abhängigkeiten von einzelnen Plattform-Anbietern. Parallel wächst das Interesse an europäischen Cloud-Angeboten, regionalen Providern und Open-Source-basierten Ansätzen.

Hinzu kommt ein strategischer Aspekt. Für viele Unternehmen geht es längst nicht mehr nur darum, wo Daten gespeichert werden, sondern wer im Ernstfall die tatsächliche Kontrolle über Backup-Bestände, Wiederherstellung und Zugriffswege behält. Gerade bei geschäftskritischen Informationen, Compliance-Anforderungen und geistigem Eigentum wird diese Frage wichtiger. Entsprechend werden Nutzungsmodelle überprüft und hybride Architekturen so gestaltet, dass sensible Daten gezielter im eigenen Einflussbereich bleiben.

Bild: actidata

Albrecht Hestermann
actidata

»Off-Site-Backup und Archivierung schließen kritische Lücken in Schutzkonzepten.«

»Datensouveränität ist im Mittelstand inzwischen mit Nachdruck angekommen«, sagt Fast-LTA-Manager Heckel. Besonders für Backup-Daten wiege dieser Punkt schwer, weil Unternehmen die letzte Verteidigungslinie gegen Datenverlust nicht ohne Weiteres in fremde Jurisdiktionen verlagern wollten.

»Entscheidend ist nicht nur, ob globale Plattformen genutzt werden, sondern wie Daten verwaltet, gesichert und kontrolliert werden«, ordnet Quantum-Managerin Wolf das Thema grundsätzlicher ein. Genau daraus entsteht derzeit ein spürbarer Trend zu Architekturen, die Kosten, Verfügbarkeit und Souveränität enger zusammen denken.

Recovery wird zur Pflichtdisziplin

Über alle Aussagen hinweg ergibt sich damit ein recht geschlossenes Bild. Der Mittelstand diskutiert Backup nicht mehr als reine Speicherfrage, sondern als Resilienz-, Architektur- und Governance-Thema. Klassische Sicherungskonzepte, die vor allem auf die Existenz einer Kopie setzen, reichen unter heutigen Bedingungen oft nicht mehr aus.

Entscheidend sind getestete Recovery-Prozesse, getrennte Sicherheitskopien, unveränderliche Speicherbereiche, klar definierte Zuständigkeiten und Architekturen, die Verfügbarkeit, Kosten und Datensouveränität zusammenbringen.

Oder etwas zugespitzter formuliert: Nicht das Backup an sich entscheidet im Krisenfall, sondern die Fähigkeit zur Wiederherstellung. Genau dort liegt im Mittelstand derzeit noch immer eine der größten Baustellen – und zugleich der größte Handlungsbedarf. ■

Ransomware, NIS-2 & das Ende der Tape-Ära – Datensicherung zukunftssicher aufstellen

BACKUP FÜR DEN MITTELSTAND: »HAT BISHER FUNKTIONIERT« REICHT NICHT MEHR

Backup-Konzepte gehören in vielen Unternehmen zum Inventar wie der Serverraum selbst: einmal eingerichtet, selten hinterfragt. Die Haltung »hat bisher immer funktioniert« ist weit verbreitet – und gefährlich. Denn die Bedrohungslandschaft hat sich fundamental verändert.

Hannes Heckel
FAST LTA

Moderne Ransomware verschlüsselt längst nicht mehr nur Produktivsysteme. Sie zielt gezielt auf Backup-Infrastrukturen, um jede Möglichkeit der Wiederherstellung zu zerstören. Gleichzeitig stellen Regularien wie NIS-2 und DORA neue Anforderungen: Nicht die Existenz eines Backups muss nachgewiesen werden, sondern die tatsächliche Restore-Fähigkeit unter Worst-Case-Bedingungen. Für den Mittelstand bedeutet das einen Paradigmenwechsel.

Der Restore entscheidet – nicht das Backup

Die entscheidende Frage lautet nicht »Wie sichern wir?«, sondern »Wie schnell können wir wiederherstellen?«. Wer nach einem Angriff tagelang auf Tape-Restores wartet, riskiert existenzbedrohende Produktionsausfälle. Laut *IBM Cost of Data Breach*-Report liegen die durchschnittlichen Kosten eines Datenvorfalls bei 4,45 Millionen Euro. Produktionsausfälle schlagen je nach Branche mit 50.000 bis 500.000 Euro – pro Tag.

Zeitgemäße Backup-Architekturen müssen deshalb vom Wiederherstellungsfall her gedacht werden. Kritische Systeme wie Domaincontroller oder Produktionssteuerungen verlangen Restore-Zeiten im Minutenbereich. Forensische Analysen nach Ransomware-Angriffen erfordern wahlfreien Zugriff auf historische Datenstände über Monate hinweg – ohne zeitraubende Bandwiederherstellungen.

Tape, Cloud, Disk – und ihre Grenzen

Klassische Backup-to-Disk-to-Tape-Konzepte (B2D2T) stoßen heute an ihre Grenzen. In der Theorie bieten sie über die physische Tape-Entnahme einen Air-Gap. In der Praxis scheitert das häufig am wachsenden Medienmanagement-Aufwand: Tapes werden nicht konsequent entnommen, einzelne Bänder bieten keine Redundanz, und die Wiederherstellung vom Band ist für forensische Analysen schlicht zu langsam.

Cloud-basierte Ansätze (B2D2D2C) lösen zwar das Problem der geografischen Trennung. Doch sie bringen neue Risiken: kein physischer Air-Gap, Bandbreitenlimitierungen bei großen On-Premises-Restores, schwer kalkulierbare Egress-Kosten und Compliance-Fragen rund um Datensouveränität und US-Cloud-Act.

Was fehlt, ist eine Backup- und Archiv-Lösung, die mehrschichtige Sicherheit bietet, ohne die Komplexität heterogener Tape-Disk-Cloud-Umgebungen mitzubringen.

Mehrschichtige Sicherheit: Der aktuelle Stand der Technik

Moderne Backup-Architekturen setzen auf drei aufeinander abgestimmte Sicherheitsebenen. Auf der ersten Ebene sorgt ein Performance Tier auf Flash-Basis für maximale Restore-Geschwindigkeit bei akuten Ausfällen – mit Wiederherstellungszeiten im Minutenbereich. Die zweite Ebene, ein Online Archive Tier mit Software-Immutability, ermöglicht forensische Analysen und historische Wiederherstellungen über Monate hinweg. Die dritte Ebene bildet ein Air-Gap-Tier mit physisch trennbaren Medien als letzte Verteidigungslinie gegen Advanced Persistent Threats und Zero-Day-Exploits.

Der Clou: Durch vorgelagerte Software-Immutability wird die Abhängigkeit vom Air-Gap reduziert. Der physische Air Gap dient nur noch als Worst-

Case-Absicherung – mit deutlich geringerer Frequenz und entsprechend weniger Aufwand.

Silent Bricks: Drei Sicherheitsebenen in einem System

Das *Silent Brick System* des Münchener Herstellers **FAST LTA** setzt genau dieses mehrschichtige Konzept in einer einzigen Plattform um. Das Prinzip: Controller und Speichermedien sind konsequent voneinander getrennt. Die sogenannten Silent Bricks sind kompakte, robuste Wechselmedien mit jeweils zwölf Datenträgern aus verschiedenen Produktionschargen und vierfachem Erasure-Coding. Das bedeutet konkret: Es entstehen keine Klumpenrisiken durch Seriendefekte, und bis zu vier Datenträger können gleichzeitig ausfallen, ohne dass ein einziges Byte verloren geht.

Je nach Anforderung deckt das System alle drei Sicherheitsebenen ab. Der neue NVMe-basierte *Silent Brick Pro* liefert als Performance-Tier Transferraten von bis zu 6 GByte/s – ideal für zeitkritische Restores. HDD-basierte Silent Bricks mit Software-Immutability durch Continuous-Snapshots und S3-Object-Locking bilden das Online-Archive-Tier. Und über den physischen Air-Gap – also die tatsächliche Entnahme der Medien aus dem System – entsteht eine letzte Verteidigungslinie, die kein Angreifer über das Netzwerk überwinden kann.

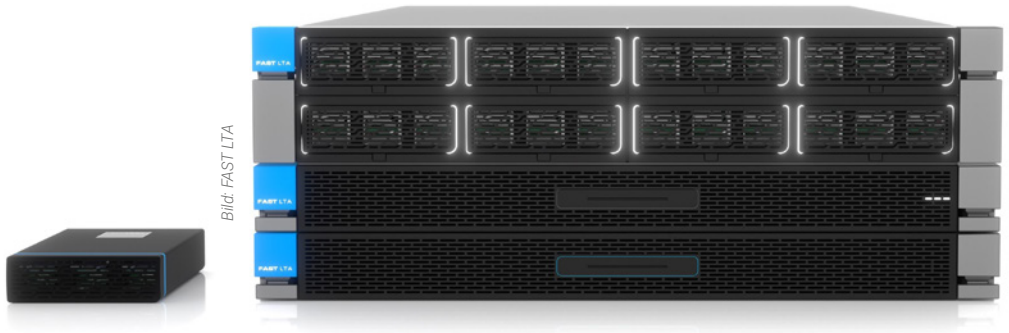


Bild: FAST LTA

Das Silent Brick System ist eine modulare Speicherlösung für Backup und Archivierung und basiert auf mobilen Datenträgern mit SSDs oder HDDs, die auch ein Air-Gap ermöglichen.

FAST LTA unterscheidet dabei vier Stufen der Unverfälschbarkeit: automatische Continuous-Snapshots, S3-Object-Locking, physischer Air-Gap und – für eine revisionssichere Archivierung – eine KPMG-zertifizierte Hardware-WORM-Versiegelung. Das gehärtete Linux-Betriebssystem bietet keine Angriffsfläche für Windows-Malware, und ein automatisches Digital Audit prüft die Datenintegrität auf Bit-Ebene.

Warum das für den Mittelstand relevant ist

Mittelständische Unternehmen stehen vor einem Dilemma: Die Anforderungen an Datensicherung steigen, die IT-Ressourcen bleiben knapp. Eine heterogene Landschaft aus Tape-Library, Disk-Storage und Cloud-Anbindung bindet Personal, erhöht die Fehleranfälligkeit und erschwert den Compliance-Nachweis.

Konkrete Alternative? Viele IT-Verantwortliche im Mittelstand verwalten heute drei parallele Systeme: eine Tape-Library, die eigentlich niemand mehr anfassen will; eine Cloud-Anbindung, deren Egress-Kosten beim letzten Restore für Überraschungen gesorgt haben; und eine Disk-Lösung, die irgendwann eingeführt wurde, weil die anderen beiden allein nicht mehr reichten. Das Ergebnis ist eine Infrastruktur, die komplex genug ist, um Fehler zu produzieren – aber nicht redundant genug, um sie zu tolerieren.

Das Silent Brick System konsolidiert Backup, Archivierung und Ransomware-Schutz in einer Plattform – mit einem Wartungsvertrag und einem Ansprechpartner. Das System lässt sich schrittweise einführen, ohne bestehende Infrastruktur sofort zu ersetzen. Der Einstieg beginnt bei wenigen Terabyte; die Skalierung reicht bis über sechs Petabyte. Langfristige Wartungsverträge mit bis zu zehn Jahren Laufzeit sorgen für planbare Kosten – ohne die Preisüberraschungen variabler Cloud-Modelle.

Die Kompatibilität mit gängigen Backup-Lösungen wie *Veeam*, *Commvault* oder *Acronis* stellt sicher, dass eine Migration ohne Bruch in der Backup-Kette möglich ist. Eine VTL-Emulation ermöglicht sogar den Ersatz bestehender Tape-Librarys, ohne die Backup-Software umkonfigurieren zu müssen.

Der erste Schritt: Ein ehrlicher Restore-Test

Die Modernisierung der Backup-Infrastruktur beginnt nicht mit einer Investitionsentscheidung, sondern mit einer ehrlichen Bestandsaufnahme. Wann wurde der letzte vollständige Restore-Test durchgeführt? Welche RPO- und RTO-Werte werden tatsächlich erreicht – nicht nur geplant? Existiert Software-seitige Immutability? Wird der Air Gap konsequent umgesetzt?

Erst wenn diese Fragen beantwortet sind, lässt sich eine fundierte Modernisierungsstrategie entwickeln. Die Investition in eine moderne Architektur amortisiert sich bei Umgebungen ab 20 TByte typischerweise innerhalb von 18 bis 24 Monaten – durch reduzierte Personalkosten, geringere Ausfallzeiten und die Vermeidung von Compliance-Verstößen.

Denn eines ist klar: Sicherheit beginnt beim Restore – nicht beim Backup. ■

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/de

Flexible Archivlösungen für jede Art von Datenbestand

LTO-10: 30 ODER 40 TBYTE FÜRS ARCHIV

Philipp Stevens
Fujifilm

Fujifilm präsentiert zwei LTO-10-Optionen, die gemeinsam durch modernste Hybrid-Partikeltechnologie überzeugen. Ob 30 TByte für Standardanwendungen oder 40 TByte mit erweiterten Umweltresistenzen – beide bieten hohe Sicherheit, schnelle Zugriffszeiten und nachhaltige Langzeitarchivierung für Ihre sensiblen Unternehmensdaten.

Die explosive Zunahme digitaler Daten stellt IT-Abteilungen vor neue Herausforderungen: Wie lassen sich große Datenmengen sicher, nachhaltig und bei kleinstmöglicher TCO langfristig archivieren? Fujifilm bietet mit den zwei Optionen der LTO-10 Generation flexible Antworten, die auf verschiedene Kundenbedürfnisse zugeschnitten sind – ohne Kompromisse bei Qualität und Zuverlässigkeit.

Gemeinsamkeiten beider LTO-10-Optionen

Beide Varianten – 30 TByte und 40 TByte native Kapazität – basieren auf der neuesten Generation feiner hybrider Magnetpartikel aus Strontium Ferrite und Barium Ferrite. Diese Materialkombination ermöglicht eine deutlich höhere Spurendichte von 15.104 Tracks pro Band, fast doppelt so viele wie bei LTO-9. Die dadurch erreichte Kapazitätssteigerung erlaubt mehr Daten auf gleicher Bandfläche zu speichern, ohne das Handling zu erschweren.

Beide LTO-10-Optionen setzen auf die »Tilted Head«-Technologie, wodurch die Initialisierung wie bei der Vorgängergeneration entfällt. Zusätzlich profitieren Sie von deutlich verkürzten Rewind-Zeiten, was die Effizienz bei Backup- und Restore-Prozessen steigert. Selbstverständlich garantieren beide Varianten eine physische Air-Gap-Isolation, die Ihre Daten sicher vor Cyberangriffen schützt, sowie eine Lebensdauer von über 30 Jahren.

LTO-10 30 TByte – Ihre robuste Standardlösung

Die 30-TByte-Variante erfüllt höchste Anforderungen an Performance und Zuverlässigkeit innerhalb typischer

Unterschied 1

Höhere Kapazität

LTO-10 40 TByte verwendet feine Hybrid-Magnetpartikel mit einem neuen Aramid-Basisträgerfilm, wodurch die Bandlänge verlängert werden konnte und sich die Kapazität von 30 TByte auf 40 TByte erhöht. Das bedeutet weniger Stellfläche und geringeren physischen Aufwand, was Kosten senkt und die Speicherung im großen Maßstab erleichtert.

Unterschied 2

Umweltbereiche

Der Einsatz von Aramid bei der 40-TByte-Cartridge führt zu verbesserter Temperatur- und Feuchtigkeitsbeständigkeit sowie zu optimierter Laufwerk-Kompensation. Dies erhöht die Zuverlässigkeit und Flexibilität in unterschiedlichen Umgebungen und senkt den Energieverbrauch sowie die Kosten.

Unterschied 3

Schnellere Datenzugriffe

Durch die Hinzunahme der hrRAO (High Resolution Recommended Access Order) Technologie verfeinert die 40TByte-Version den oRAO von LTO-9, indem das Band in 128 Segmente statt nur 2 unterteilt wird. Dies beschleunigt den Datenzugriff erheblich und verbessert die Effizienz bei der Datenwiederherstellung.

Unternehmensumgebungen. Mit nativen 30 TByte und einer nativen Transferrate von bis zu 400 MByte/s bietet sie ausgewogene Kapazität und Geschwindigkeit für Standardarchive. Dieses Modell eignet sich besonders für Unternehmen, die eine bewährte, gut integrierbare Lösung für langfristige Sicherung großer Datenvolumen suchen.

LTO-10 40 TByte – Für erweiterte Kapazitäten und anspruchsvollere Umweltbedingungen

Die 40-TByte-Version hebt die Kapazität noch weiter an – dank eines speziellen Aramid-Basefilms wird die Banddicke verringert und so eine erhöhte Bandlänge ermöglicht, sodass 40 TByte nativer Speicherplatz erreicht werden. Diese größere Kapazität reduziert nicht nur den Platzbedarf und physischen Handling-Aufwand, sondern spart auch Kosten bei umfangreichen Archivierungsprojekten.

Zudem erweitert der innovative Aramidfilm die zulässigen Umweltbedingungen deutlich: Die Kassetten sind resistenter gegenüber Temperaturschwankungen und niedriger Luftfeuchtigkeit, was besonders in herausfordernden Lager- oder Transportumgebungen entscheidend ist.

Gemeinsam schnell und effizient: hrRAO-Technologie

Exklusiv in der 40-TByte-Variante eingeführt, sorgt die High Resolution Recommended Access Order (hrRAO) Technologie für eine Revolution beim Dateizugriff. Im Vergleich zum bisherigen System mit nur zwei Bandsegmenten ermöglicht hrRAO eine Unterteilung des Bandes in 128 feine Segmente. Dieser feinere Zugriff reduziert die Such- und Zugriffszeiten drastisch, was für IT-Teams eine enorme Zeitersparnis und Effizienzsteigerung bei Backup und Restore bedeutet. Auch wenn die 30-TByte-Variante die bisherige oRAO-Technologie nutzt, ist mit hrRAO die Zukunft im Standard für schnellstmögliche Datenzugriffe gesetzt.

Fazit – Maßgeschneiderte Archivierung für jeden Bedarf

Mit den beiden LTO-10-Optionen bietet Fujifilm eine umfassende Lösungspalette für unterschiedliche Archivierungsanforderungen. Die 30-TByte-Variante überzeugt durch zuverlässige Performance und einfache Integration in bestehende Systeme, ideal für Standardarchive und häufigen Zugriff. Die 40-TByte-Version bietet darüber hinaus mehr Kapazität, erweiterte Umweltresistenz und modernste hrRAO-Technologie – perfekt für Anwender mit hohem Speicherbedarf und anspruchsvollen operativen Bedingungen.

Sicherheit und Nachhaltigkeit – unsere gemeinsamen Versprechen

Beide LTO-10-Optionen bieten Ihnen Infrastruktursicherheit durch physische Air-Gap-Isolation: Ihre archivierten Daten bleiben offline und damit geschützt vor Cyberangriffen und Ransomware. Die getestete Lebensdauer von über 30 Jahren sowie die Robustheit der Materialien garantieren eine langfristige Datenbewahrung ohne Qualitätseinbußen. Gleichzeitig ist Tape im Vergleich zu diskbasierten Systemen bis zu 80 Prozent kosteneffizienter und ressourcenschonender – ein nachhaltiger Beitrag zu Ihrem IT-Umweltmanagement.[1)]

Ein starker Partner an Ihrer Seite

Fujifilm steht seit Jahrzehnten für Innovation und Qualität in der Tape-Technologie. Neben erstklassigen Produkten bieten wir Ihnen umfassenden technischen Support und Beratung – von der Auswahl der passenden LTO-10 Lösung bis hin zur reibungslosen Integration in Ihre IT-Landschaft.

Jetzt auf die Zukunft setzen: Zwei starke LTO-10-Optionen, die sich Ihren Anforderungen anpassen.

Sichern Sie sich die Flexibilität, Kapazität und Sicherheit, die Ihr Unternehmen heute und morgen braucht. Ihre Daten haben es verdient.

Für weitere Informationen oder eine persönliche Beratung steht Ihnen Ihr Fujifilm-Ansprechpartner gerne zur Verfügung. ■

Weitere Informationen:

Fujifilm Germany GmbH

Fujistrasse 1
47533 Kleve
www.fujifilm.com

*1) Brad Johns Consulting LLC, Improving Data Center Sustainability with Modern Tape Storage, 2025

Tape-Archivierung für wachsende Backup-Umgebungen

DIE MITTELSTANDS-LIBRARY IST JETZT AUCH MIT LTO-10 VERFÜGBAR

Albrecht Hestermann
actidata

Mit der Unterstützung von LTO-10 erweitert actidata mit der »actiLib Kodiak 3416« sein Einsatzspektrum für Backup- und Archivierungsaufgaben im Mittelstand. Die modulare Tape-Library lässt sich von einem 3U-Basisgerät mit 40 Slots bis auf 640 Slots ausbauen und erreicht damit Kapazitäten von über 64 PByte. Gleichzeitig soll das System hohe Datentransferraten und eine flexible Nachrüstung neuer LTO-Generationen ermöglichen.

Die *actiLib Kodiak 3416* LTO-Tape-Library etabliert sich bereits seit mehreren Jahren in IT-Umgebungen des Mittelstandes. Als bewährtes System für die Speicherung großer Datenmengen für Backup und Archivierung auf auswechselbaren LTO-Tapes rangiert die 3U basierende Tape-Library als zentrales Datensicherungssystem im Rahmen unternehmensweiter Cyber-Security-Strategien. Unterstützt von allen gängigen Backup-Software-Herstellern werden die eingebauten LTO-Laufwerke entweder über das vorhandene Fibre-Channel-SAN oder die SAS-Schnittstelle des Backup-Servers angesprochen.

actiLib Kodiak 3416 – Basis-Modul

Bereits das Basis-Modul hält herausragende Leistungsmerkmale bereit. Ausgestattet mit aktuellen LTO-10-Tape-Drives werden auf 40 LTO-Slots eine Gesamtkapazität von bis zu 4 PByte* erreicht. Hierbei wird mit jeweils einem LTO-10-Laufwerk eine Datentransferrate von bis zu 2,5 TByte* pro Stunde erreicht.

actiLib Kodiak 3416 – Erweiterungsmodule

Bis zu 15 weitere Module lassen sich an einem Basis-Modul betreiben und stellen in der maximalen Ausbaustufe 640 LTO-Slots und mehr als 64

Bild: actidata

actiLib Kodiak 3416 – die mitwachsende Mittelstands-Library mit LTO-10

** komprimierte Daten mit 1:2,5*

PByte* Speicherkapazität zur Verfügung. Somit wächst die actiLib Kodiak 3416 LTO-Tape-Library mit und lässt sich den wachsenden Anforderungen flexibel anpassen.

Bereit für zukünftige LTO-Tape-Technologien

Neue LTO-Tape-Drive-Module lassen sich auch zu einem späteren Zeitpunkt problemlos in die actiLib Kodiak 3416 LTO-Tape-Library nachrüsten und sogar im Mixbetrieb mit unterschiedlichen LTO-Technologien betreiben.

Hohe Wirtschaftlichkeit

Mit 13 Slots pro Höheneinheit bietet die actiLib Kodiak 3416 höchste Kapazität bei bester Raumausnutzung. Durch optimale Skalierbarkeit mit netzteillosen Erweiterungsmodulen ist die LTO-Tape-Library wirtschaftlich im laufenden Betrieb und zukünftige Investitionen sind mitwachsend, bedarfsorientiert planbar.

Was heißt denn hier »skalierbar«?

Beginnend mit dem Basis-Modul (BTL) der actiLib Kodiak 3416 stehen bereits 40 Slots zur Aufnahme von LTO-Medien zur Verfügung. Die komplette Robotik für die Bestückung der eingebauten LTO-Tape-Drives sowie ein Barcode-Reader zur einfachen und schnellen Inventarisierung sind bereits eingebaut.

Technologie	LTO-8 HH Half Height	LTO-9 HH Half Height	LTO-9 FH Full Height	LTO-10 FH Full Height
Max. Kapazität per Medium native / DC*	12TB / 30TB (L8) 9TB / 22,5TB (M8)	18TB / 45TB	18TB / 45TB	30TB / 75TB 40TB / 100TB
Max. Datentransferrate native / DC*	300 MB/s / 750 MB/s Dynamische Anpassung	300 MB/s / 750 MB/s Dynamische Anpassung	400 MB/s / 700 MB/s Dynamische Anpassung	400 MB/s / 1000 MB/s Dynamische Anpassung
Schnittstelle per LTO Tape Drive	2x SAS 6Gb/s (SFF8088) / 2x FC 8Gb/s (LC-Type)	2x SAS 12Gb/s (SFF8644) / 2x FC 8Gb/s (LC-Type)	2x SAS 12Gb/s (SFF8644) 2x FC 8Gb/s (LC-Type)	2x SAS 12Gb/s (SFF8644) 2x FC 32Gb/s (LC-Type)

Verfügbare LTO Tape Drive Module für die actiLib Kodiak 3416

Leistungsdaten DC=Data Compression 2,5 : 1	actiLib Kodiak 3416 Basic Modul (BTL)	actiLib Kodiak 3416 Erweiterungsmodul (ETL)	actiLib Kodiak 3416 Volle Ausbaustufe
ca. Kapazität LTO-8 HH native / DC	480TB / 1200TB	480TB / 1200TB	7,68PB / 19,20PB
ca. Kapazität LTO-9 HH native / DC	720TB / 1800TB	720TB / 1800TB	11,52PB / 28,80PB
ca. Kapazität LTO-10 FH native / DC	1600TB / 4000TB	1600TB / 4000TB	25,6PB / 64,0PB

Leistungsdaten der actiLib Kodiak 3416 (Auszug)

Bild: actidata

Die actiLib Kodiak 3416 lässt sich vom 3U-Basisgerät mit 40 Slots auf bis zu 640 Slots ausbauen und unterstützt aktuelle LTO-10-Laufwerke für skalierbare Backup- und Archivierungsumgebungen im Mittelstand.

Die Erweiterung mit bis zu 15 actiLib Kodiak 3416 Erweiterungseinheiten (ETL) erfolgt durch Einbau ober- bzw. unterhalb des Basis-Moduls. Jede Erweiterungseinheit stellt weitere 40 Slots zur Verfügung und wird, soweit kein weiteres LTO-Tape-Drive eingesetzt wird, ohne Netzteile betrieben. Jedes Modul verfügt über zwei herausnehmbare Magazine mit je 20 Slots für LTO-Medien, wobei per Modul fünf Slots als Mail-Slots für den selektiven Zugriff genutzt werden können. Als hoch skalierbare LTO-Tape Library mit einem 3U-Basis-Modul und bis zu 15 3U-Erweiterungsmodulen empfiehlt sich die actiLib Kodiak 3416 als optimale mitwachsende LTO-Tape-Library für Mittelstandsanwendungen bis zu 640 LTO-Slots in der vollen 48U Ausbaustufe. Je nach den Anforderungen der IT-Umgebung können bei der actiLib Kodiak 3416 per Modul typischerweise zwei LTO-Laufwerke (jedoch max. 3x HH oder 1x FH plus 1x HH) eingesetzt werden.

Ist Service nicht das A und O?

actiCare-Service steht für 36 Monate Gewährleistung inkl. des bewährten Fast-Exchange-Service (Vorabaustausch defekter Komponenten) sowie die kostenfreie technische Unterstützung über Telefon, E-Mail und Internet in deutscher Sprache. Auf Wunsch sind actiCare Services bis zu 60 Monate – auch vor Ort – verfügbar.

actidata Kodiak 3416 mit LTO-10-Tape-Drive-Modulen ist ab sofort verfügbar.

LTO-10-Tape-Drive-Module sind ausschließlich in voller Einbauhöhe verfügbar, die mit einer Aufzeichnungsgeschwindigkeit von bis zu 400 MByte/s (native) aufwarten.

Per Medium lassen sich hier 30 TByte (native) bzw. 40 TByte (verfügbar voraussichtlich Q4/2026) aufzeichnen. Somit sind pro Modul 1,6 PByte (native) Kapazität möglich. Der empfohlene Endkundenpreis beginnt mit 20.442 Euro, netto. ■

Weitere Informationen:

actidata Storage Systems GmbH

Schlossstr. 32a
45711 Datteln-Horneburg
Tel. 023 63/56 775-0
E-Mail: info@actidata.com
www.actidata.com

Datensouveränität und Rechtssicherheit in Europa

STRATEGISCHE BACKUP-LÖSUNGEN FÜR MITTELSTAND & MSPS

Hybride IT, wachsende Datenmengen und hohe Compliance-Anforderungen fordern den Mittelstand, Systemhäuser und MSPs gleichermaßen. Backup ist mehr als Datensicherung – es geht um Performance, Automatisierung und rechtliche Rahmenbedingungen. Genau hier bieten deutsche Hersteller entscheidende technische und regulatorische Vorteile.

Stefan Utzinger
NovaStor

Moderne IT-Architekturen bestehen aus On-Premises-, Virtualisierungs- und Cloud-Umgebungen sowie verteilt arbeitenden Teams. Diese Vielfalt erhöht die Anforderungen an Backup- und Restore-Prozesse. Gefragt sind Lösungen, die technisch leistungsfähig sind – gleichzeitig Transparenz und Kontrolle gewährleisten sowie den Betrieb schnell wieder hochfahren lassen.

Ein zentraler Aspekt ist die Datensouveränität. Deutsche Backup-Hersteller unterliegen der DSGVO und EU-Regelwerken mit klaren Schutzstandards. Bei außereuropäischen Anbietern entstehen rechtliche Unsicherheiten, etwa durch den US Cloud Act oder mögliche Zugriffe durch Regierungen. Daher bedeuten für Mittelstand und Systemhäuser europäische Hersteller mehr Klarheit, Kontrolle und weniger rechtliche Grauzonen im täglichen Betrieb.

Neben regulatorischen Fragen zählen technische und kommerzielle Faktoren. Europäische Backup-Lösungen sind häufig auf die heterogenen Infrastrukturen des Mittelstands ausgerichtet: wie beispielsweise physische Server, moderne Hypervisor-Umgebungen, hybride Cloud-Szenarien und Einsatz von Tape. Entscheidend sind unter anderem effiziente Deduplizierung und Architekturen mit hoher Backup-Geschwindigkeit auch bei wachsendem Datenvolumen. Ebenso wichtig ist eine schnelle, verlässliche Wiederherstellung – denn im Ernstfall zählt die Zeit bis zur Betriebswiederaufnahme.

Administratoren brauchen ein zentrales Management, klar strukturierte Policies und detailliertem Monitoring. Gerade im Mittelstand zählt transparentes, reproduzierbares Backup-Verhalten sowie gesicherte Restore-Prozesse – inklusive Reporting – was mit NIS-2 für viele Unternehmen zur Pflicht wird.

Ein Vorteil deutscher Anbieter ist die geografische und organisatorische Nähe zum Kunden. Support und Professional Services werden häufig durch eigene Teams der Hersteller erbracht – ohne globale Call-Center-Strukturen. Das verkürzt Reaktions- & Ausfallzeiten, verbessert Fehleranalysen und sorgt für ein gemeinsames Verständnis der regulatorischen Rahmenbedingungen.

Auch für MSPs gewinnen europäische Backup-Plattformen an Bedeutung. Mandantenfähige Plattformen, automatisierte Bereitstellung sowie Reporting- und Abrechnungsfunktionen schaffen die Basis für skalierbare Backup-Services mit klaren Compliance-Anforderungen. Der Betrieb innerhalb Europas erleichtert zudem die Einhaltung branchenspezifischer Vorgaben – etwa im Gesundheitswesen, in der öffentlichen Verwaltung oder in der Industrie – und stärkt das Vertrauen in die Services.

Fazit: Digitale Souveränität beginnt nicht in der Cloud-Strategie – sie beginnt beim Backup. Wer auf deutsche oder europäische Technologien setzt, entscheidet sich für klare Rahmenbedingungen, Qualität und partnerschaftliche Zusammenarbeit. Für den Mittelstand sowie für Systemhäuser und MSPs ist europäische Software eine strategische Entscheidung für Stabilität, Sicherheit und Zukunftsfähigkeit. ■

Weitere Informationen:

NovaStor GmbH

Lübeckertordamm 1-3,
20099 Hamburg
Tel. +49 (0)40/63809 0
E-Mail: kontakt@novastor.de
www.novastor.de

Actidata

www.actidata.com

Sitz der Gesellschaft:
Dortmund

Jahr der Gründung:
2009

Zielgruppe:
Systemhäuser, VARs und Industriekunden

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

FAST LTA

www.fast-lta.de

Sitz der Gesellschaft:
München

Jahr der Gründung:
1999

Zielgruppe:
KMUs, VARs und Industriekunden

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

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

Fujifilm Recording Media

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

Sitz der Gesellschaft:
Kleve

Jahr der Gründung:
1987

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

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.

NovaStor GmbH

www.novastor.de

Sitz der Gesellschaft:
Hamburg

Jahr der Gründung:
1999

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

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.

Tape-Librarys 2026: Sicherheit schlägt Slot-Zahl

AUTOMATISCHE UND SKALIERBARE BACKUPS

Karl Fröhlich
speicherguide.de

Der Tape-Markt hat seit Frühjahr 2025 deutlich an Kontur gewonnen. LTO-10 ist verfügbar, bringt aber keine Rückwärts-Kompatibilität mit. Gleichzeitig rücken Vaulting, MFA und Verifizierungsfunktionen stärker in den Fokus. Für den Mittelstand geht es damit weniger um maximale Kapazität als um eine belastbare Backup- und Archiv-Architektur.

Im Segment für Bandspeicherlösungen haben sich die Rahmenbedingungen verändert: Seit rund einem Jahr bewegt sich die Diskussion weg von der reinen Kapazitätsfrage. Tape-Librarys ordnen sich heute stärker als Baustein für Cyber-Resilienz, Offline-Kopien und langfristige Datenhaltung ein. Der frühere Fokus auf Slots, Höheneinheiten und Preis pro Kassette reicht dafür allein nicht mehr aus.

Der wichtigste Technologiesprung ist nicht einmal die reine Kapazität, sondern der Bruch im Medienpfad. LTO-10 wurde im August 2025 offiziell vorgestellt und startet mit 30 TByte nativer Kapazität und bis zu 75 TByte komprimiert. Inzwischen existiert zusätzlich ein 40-TByte-Medium mit bis zu 100 TByte komprimierter Kapazität. Gleichzeitig können LTO-10-Laufwerke ausschließlich LTO-10-Medien lesen und schreiben. Genau das macht den Generationswechsel strategisch heikler als früher.

Wer migriert, muss Bestände, Restore-Prozesse und Mischbetrieb sauber planen, statt nur größere Kassetten zu bestellen und auf einen nahtlosen Übergang zu hoffen.

Für viele Mittelständler bleibt LTO-9 vorerst die vernünftigere Wahl

In mittelständischen Umgebungen dürfte LTO-9 deshalb noch einige Zeit der pragmatischere Standard bleiben. Die Technik ist im Markt etabliert, der Medienbestand ist vorhanden und typische Backup- sowie Auslagerungs-Szenarien lassen sich damit weiterhin solide abdecken. LTO-10 ist vor allem dort interessant, wo ohnehin ein größerer Plattformwechsel ansteht, wo neue Libraries aufgebaut werden oder wo stark wachsende Datenmengen die höhere Medienkapazität wirtschaftlich sinnvoll machen. Aus einem Routine-Upgrade ist damit eher ein Architekturprojekt geworden.

Cyber-Resilienz rückt von der Kassette in die Library

Auch funktional hat sich der Markt bewegt. **HPE** ergänzt seine MSL-Reihe um Funktionen wie *Vault Partition*, MFA und *Data Verification*. **Quantum** positioniert seine *Scalar*-Familie mit Active Vault und Logical Tape Blocking klar in Richtung Ransomware-Schutz und kontrollierten physischen Zugriff. **IBM** betont bei aktuellen Tape-Laufwerken neben AES-256-Verschlüsselung sogar Post-Quanten-Kryptographie-Zertifikate für den Schlüsselaustausch. Das ist ein Unterschied zur älteren Sicht auf Tape als bloßes Offline-Medium. Sicherheit entsteht heute nicht mehr nur durch den Medienbruch, sondern zunehmend auch durch Library-Logik, Management-Funktionen und nachprüfbare Restore-Fähigkeit.

Bild: Actidata

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

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 dauer-hafte Speicherung von Daten Verwendung.

Das Anbieterfeld bleibt in Bewegung

Das Marktbild bei Tape-Librarys hat sich seit Frühjahr 2025 verändert, aber nicht einfach nur ausgedünnt. Mit dem Aus von **Overland-Tandberg** ist zwar ein bekannter Hersteller weggefallen. Gleichzeitig ist **MagStor** neu hinzugekommen und bedient über **EDP** den deutschen Markt für Tape-Librarys. Für Käufer wird damit weniger die Zahl der Anbieter entscheidend, sondern die Frage, wie breit ein Portfolio vom kompakten Autoloader bis zur skalierbaren Library reicht und welche Management- und Sicherheitsfunktionen die Systeme im Betrieb mitbringen. LTO-10 gehört dabei zunehmend zum generellen Technik-Fortschritt des Marktes und taugt immer weniger als einzelnes Abgrenzungsmerkmal.

Tape profitiert von Archiv, Hybrid-Cloud und unstrukturierten Daten

Wer Tape noch immer nur als Restbestand aus alten Backup-Zeiten betrachtet, übersieht die aktuelle Marktdynamik. Das *LTO Consortium* weist für 2024 ein Rekordvolumen von 176,5 EByte ausgelieferter komprimierter Tape-Kapazität aus. Das entspricht einem Plus von 15,4 Prozent gegenüber 2023. Als Treiber nennt die Organisation vor allem das Wachstum unstrukturierter Daten und die stärkere Nutzung von Hybrid-Cloud-Architekturen.

Tape profitiert damit nicht nur vom Wunsch nach einer Offline-Kopie, sondern auch von Archiv-, Compliance- und Kostenfragen in längerfristigen Datenhaltungsmodellen. Das Band läuft also nicht aus Gewohnheit weiter, sondern weil es in bestimmten Schichten der Infrastruktur wirtschaftlich immer noch verdammt schwer zu schlagen ist.

Für Kaufentscheidungen zählt heute das Betriebsmodell

Für mittelständische Käufer ist deshalb weniger entscheidend, ob eine Tape-Library in der Basiseinheit 24, 40 oder 80 Slots bietet. Wichtiger ist, ob das System zum eigenen Betriebsmodell passt. Bleibt LTO-9 noch mehrere Jahre gesetzt oder lohnt sich der harte Schnitt auf LTO-10? Gibt es belastbare Prozesse für Offsite-Lagerung und Rückholung? Und welche Sicherheitsfunktionen werden im Alltag tatsächlich genutzt, statt nur im Datenblatt gut auszusehen?

Der passende Bandroboter ist 2026 kein isoliertes Gerät mehr, sondern die letzte, bewusst getrennte Stufe in einer Architektur aus Backup-Software, Primärspeicher, Offsite-Prozess und Band. Entscheidend ist damit weniger die reine Slot-Zahl als die Frage, welche Systeme Migration, Medienbruch, Cyber-Resilienz und Langzeit-Aufbewahrung schlüssig zusammenbringen.

Tape ist kein Technik-Fossil, sondern eine nüchterne Antwort auf ein sehr aktuelles Problem: wachsende Datenmengen, knappe Budgets und eine größere Angriffsfläche. ■

Air-Gap auch mit Disk-Speichern möglich

Tape gilt als klassisches Offline-Medium. Dass sich ein physischer Air-Gap auch mit Festplatten- und Flash-Speichern umsetzen lässt, zeigt **FAST LTA** mit seinem *Silent-Brick-System*. Die aktuelle Plattform basiert auf dem *Silent Brick Controller X*. Er bietet je nach Modell zwei, vier oder acht Slots für mobile *Silent Brick Pro*-Module und lässt sich über SAS um bis zu 26 stationäre *Silent Brick Max Air* erweitern. Damit sind brutto mehr als 6 PByte Gesamtkapazität möglich. *Silent Bricks* unterstützen *True Air Gap*, Continuous-Snapshots sowie S3-Object-Locking und eignen sich damit für Backup, VTL-Archive und unveränderbare Sekundärspeicher.

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.

Die mobilen Silent Brick Pro arbeiten mit NVMe-Medien und sind in Größen von 12, 24, 48 und 96 TByte brutto erhältlich. Die stationären *Silent Brick Max Air* sind mit zwölf 3,5-Zoll-Festplatten aus drei verschiedenen Chargen bestückt und stehen mit 48, 96, 144 oder 240 TByte brutto pro Höheneinheit zur Verfügung. Mehrere Module lassen sich zu größeren Volumes kombinieren. Als Schutzmechanismen nennt der Hersteller Triple-Parity in *SecureNAS 3p* sowie vierfache Redundanz per Erasure Coding in *SecureNAS ERC* bzw. im VTL-Betrieb.
Bei den Schnittstellen bietet der *Controller X* je nach Modell Dual 10GbE, Dual 10/25GbE oder Dual 100GbE. Das System zielt damit nicht nur auf klassische Backup-Ablagen, sondern auch auf performantere Restore- und VTL-Szenarien. Wartungsseitig stellt Fast LTA Service-Laufzeiten von bis zu zehn Jahren sowie optionale 24/7-Erreichbarkeit in Aussicht. 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 4.444
www.actidata.com	actiLib 1U LTO-Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 6.173
	actiLib 1U LTO-Autoloader	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 5.473
	actiLib 2U LTO Tape Library	LTO-7	24	1-2	144	2,2	SAS 6G/12G, FC 8Gb	2U	ab 4.798
	actiLib 2U LTO Tape Library	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 6.775
	actiLib 2U LTO Tape Library	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 8.530
	actiLib Kodiak 3416	LTO-7	40	1-2	240	3	SAS 6G/12G, FC 8Gb	3U	ab 10.860
	actiLib Kodiak 3416	LTO-8	40	1-2	480	3	SAS 6G/12G, FC 8Gb	3U	ab 11.639
	actiLib Kodiak 3416	LTO-9	40	1-2	720	3	SAS 6G/12G, FC 8Gb	3U	ab 13.858
	actiLib Kodiak 3416	LTO-10	40	1-2	1.660	4	SAS 6G/12G, FC 32Gb	3U	ab 20.442
	actiLib Kodiak 6807	LTO-7	80	1-6	480	6	SAS 6G/12G, FC 8Gb	6U	ab 12.058
	actiLib Kodiak 6807	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 15.735
	actiLib Kodiak 6807	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 19.281
Fsas Technologies	Eternus LT140	LTO-8	20	1-14	240	22,7	SAS 6G, FC 8Gb	3U	ab 9.830
eu.fsastech.com/de/	Eternus LT140	LTO-9	20	1-42	360	22,7	SAS 6G, FC 8Gb	3U	ab 11.994
	Eternus LT260	LTO-7	80	1-6	480	45,4	SAS 6G, FC 8Gb	6U	k.A.
	Eternus LT260	LTO-8	80	1-6	960	45,4	SAS 6G, FC 8Gb	6U	k.A.
	Eternus LT270 S2	LTO-7	138-713	2-20	828	2,7	FC 8Gb	42U	k.A.
	Eternus LT270 S2	LTO-8	138-713	2-20	1.536	2,7	FC 8Gb	42U	k.A.
HPE	StoreEver MSL 1/8 Tape Autoloader	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 7.470
www.hpe.com/de/de/	StoreEver MSL 1/8 Tape Autoloader	LTO-9	8	1	144	2,2	SAS 6G/12G, FC 8Gb	1U	ab 9.658
	StoreEver MSL2024	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 6.963
	StoreEver MSL2024	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 7.916
	StoreEver MSL3040	LTO-8	40	1-3	480	22,5	SAS 6G/12G, FC 8Gb	3U	k.A.
	StoreEver MSL3040	LTO-9	40	1-21	720	22,5	SAS 6G/12G, FC 8Gb	3U	ab 11.945
	StoreEver MSL6480	LTO-8	80	1-6	960	6,48	SAS 6G/12G, FC 8Gb	6U	k.A.
	StoreEver MSL6480	LTO-9	80	1-6	1.440	6,48	SAS 6G/12G, FC 8Gb	6U	ab 24.704
IBM	TS2900	LTO-8	9	1	108	1,6	SAS 6G	1U	ab 6.882
www.ibm.com	TS2900	LTO-9	9	1	162	3	SAS 6G	1U	ab 7.850
	TS4300	LTO-8	40	1-3	480	3	SAS 6G, FC 8Gb	3U	ab 7.650
	TS4300	LTO-9	40	1-3	720	3	SAS 6G, FC 8Gb	3U	ab 8.950
	TS4300	LTO-10	40	1-3	1.600	4	SAS 6G, FC 32Gb	3U	k.A.
Oracle	StorageTek SL4000	LTO-8	339	1-24	4.000	31,1	FC, Ficon	42U	ab 10.500
www.oracle.com/de/	StorageTek SL4000	LTO-9	339	1-24	6.100	34,5	FC, Ficon	42U	k.A.
	StorageTek SL8500	LTO-8	2.000	64	24.000	82,9	FC, FCoE, Ficon	42U	k.A.
	StorageTek SL8500	LTO-9	2.000	64	36.000	92.1	FC, FCoE, Ficon	42U	k.A.

Hersteller	Produktname	Bandformat	Max. Tape-Slots/ Basiseinheit	Tape-Drives	Max. Kapazität in TByte	Transferrate in TByte/h	Schnittstellen	Formfaktor (Rackmount)	Nettopreis (Euro)
Magstor	M1000	LTO-8	8	1	96	1,1	SAS 6G/12G, FC 8Gb	1U	ab 6.850
magstor.com	M1000	LTO-9	8	1	144	1,1	SAS 6G/12G, FC 8Gb	1U	ab 7.720
edp-shop.de	M2000	LTO-8	24	1-2	288	2,2	SAS 6G/12G, FC 8Gb	2U	ab 7.125
	M2000	LTO-9	24	1-2	432	2,2	SAS 6G/12G, FC 8Gb	2U	ab 7.990
	M3000	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 8.925
	M3000	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 9.790
	M3280	LTO-9	280	21	5.000	4	SAS 6G/12G, FC 8Gb	21U	ab 33.953
	M3640	LTO-9	640	48	11.500	4	SAS 6G/12G, FC 8Gb	48U	ab 70.313
Qualstar	Q8	LTO-8	8	1	96	1,1	SAS 6G, FC 8Gb	1U	ab 7.780
www.qualstar.com	Q8	LTO-9	8	1	144	1,1	SAS 6G, FC 8Gb	1U	ab 8.870
	Q24	LTO-8	24	1-2	288	2,2	SAS 6G, FC 8Gb	2U	ab 8.100
	Q24	LTO-9	24	1-2	432	2,2	SAS 6G, FC 8Gb	2U	ab 9.364
	Q40	LTO-8	40	1-3	480	3	SAS 6G/12G, FC 8Gb	3U	ab 10.400
	Q40	LTO-9	40	1-3	720	3	SAS 6G/12G, FC 8Gb	3U	ab 12.240
	Q40	LTO-10	40	1-3	1.200	3	SAS 6G/12G, FC 8Gb	3U	ab 20.193
	Q80	LTO-8	80	1-6	960	6	SAS 6G/12G, FC 8Gb	6U	ab 16.878
	Q80	LTO-9	80	1-6	1.440	6	SAS 6G/12G, FC 8Gb	6U	ab 18.275
	Q80	LTO-10	80	1-6	2.400	6	SAS 6G/12G, FC 8Gb	6U	ab 26.390
Quantum	Scalar i3	LTO-8	25-400	1-24	300	1,08	SAS 6G/12G, FC 8Gb	3U-24U	ab 7.543
www.quantum.com	Scalar i3	LTO-9	25-400	1-24	450	1,62	SAS 6G/12G, FC 8Gb	3U-24U	ab 8.400
	Scalar i6	LTO-8	50-800	1-24	600	1,3	SAS 6G/12G, FC 8Gb	6U-48U	ab 15.800
	Scalar i6	LTO-9	50-800	1-24	900	1,44	SAS 6G/12G, FC 8Gb	6U-48U	ab 16.800
	Scalar i6	LTO-10	50-800	1-24	2.000	5,4	SAS 6G/12G, FC 8Gb	6U-48U	k.A.
	Scalar i6000	LTO-7	100-12k	1-192	600	1,08	SAS 6G/12G, FC 8Gb	Full Rack	ab 75.000
	Scalar i6000	LTO-8	100-12k	1-192	1.200	1,3	SAS 6G/12G, FC 8Gb	Full Rack	k.A.
	Scalar i6000	LTO-9	100-12k	1-192	1.800	1,44	SAS 6G/12G, FC 8Gb	Full Rack	k.A.
	Scalar i6000	LTO-10	100-12k	1-192	4.000	1,44	SAS 6G/12G, FC 32Gb	Full Rack	k.A.
Spectra Logic	Spectra T950	LTO-7	920	24	8.280	25,92	FC 8Gb	Full Rack	ab 9.000
spectralogic.com	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.
	Spectra T950	LTO-10	920	24	36.800	172,8	FC 32Gb	Full Rack	k.A.

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


speicherguide.de
IT-Entscheidungen brauchen Substanz.
Analysen, Tests und Orientierung für IT-Verantwortliche.
speicherguide.de
Newsletter abonnieren

Bild: speicherguide.de via DALL-E

Karl Fröhlich
speicherguide.de

Backup-Software im Überblick

BACKUP-PLATTFORMEN ZWISCHEN CYBER-RESILIENZ UND DIGITALER SOUVERÄNITÄT

Backup-Software hat sich längst zu umfassenden Data-Protection-Plattformen entwickelt. Cyber-Resilienz, SaaS-Backup und Hybrid-Cloud-Schutz prägen heute den Markt. Gleichzeitig geraten rechtliche Rahmenbedingungen stärker in den Blick: Die dominierenden Anbieter stammen aus den USA – während europäische Unternehmen ihre Abhängigkeiten kritischer hinterfragen.

Backup gehört zu den wenigen IT-Disziplinen, die im Ernstfall über die Handlungsfähigkeit eines Unternehmens entscheiden. Für kleine und mittlere Unternehmen gilt das genauso wie für große Organisationen. Ransomware, Systemausfälle oder Fehlkonfigurationen können innerhalb weniger Stunden komplette IT-Umgebungen lahmlegen. Eine funktionierende Datensicherung ist deshalb weiterhin eine zentrale Voraussetzung für die Wiederherstellung kritischer Systeme und Daten.

Gleichzeitig haben sich die Anforderungen an Backup-Software deutlich verändert. Klassische Sicherungsjobs allein reichen längst nicht mehr aus. Unternehmen erwarten heute Lösungen, die Cyberangriffe erkennen, Datenintegrität prüfen, Cloud-Workloads schützen und eine schnelle Wiederherstellung ermöglichen. Backup entwickelt sich damit zu einem zentralen Baustein moderner Cyber-Resilienz.

Für IT-Abteilungen im Mittelstand kommt ein weiterer Aspekt hinzu: Die Frage nach der digitalen Souveränität. Neben technischen Funktionen rücken deshalb auch Anbieterstruktur, Support-Zugriffe und rechtliche Rahmenbedingungen stärker in den Fokus.

Backup-Software muss einfacher zu betreiben sein

Gerade kleinere IT-Abteilungen haben selten die Ressourcen, komplexe Backup-Infrastrukturen dauerhaft zu betreiben. Viele Unternehmen suchen deshalb nach Lösungen, die sich möglichst einfach installieren, verwalten und automatisieren lassen.

Moderne Backup-Software setzt deshalb zunehmend auf zentrale Management-Oberflächen, automatisierte Sicherungsprozesse und vorkonfigurierte Richtlinien. Auch Self-Service-Funktionen, automatische Recovery-Tests oder vereinfachte Disaster-Recovery-Szenarien gewinnen an Bedeutung.

Parallel dazu steigt der Druck durch Cyberangriffe. Backup-Lösungen müssen heute nicht nur Daten sichern, sondern auch Angriffe erkennen und eine sichere Wiederherstellung ermöglichen. Funktionen wie unveränderbare Backups, Malware-Scans oder isolierte Recovery-Umgebungen gehören deshalb immer häufiger zum Standard moderner Datensicherung.

Quelle: die jeweiligen Hersteller, fiktive Box-Collage: speicherguide.de

Backup entwickelt sich zu umfassenden Data-Protection-Plattformen

Der Markt für Backup-Software wird inzwischen breiter definiert als noch vor wenigen Jahren. Im jüngsten *Magic Quadrant* beschreibt **Gartner** das Segment nicht mehr als klassischen Markt für Enterprise-Backup- und Recovery-Software, sondern als Markt für »Backup and Data Protection Platforms«. In der Leader-Gruppe sieht Gartner **Cohesity**, **Commvault**, **Dell Technologies**, **Druva**, **Rubrik** und **Veeam**. Das zeigt, dass sich der Wettbewerb zunehmend um Plattform-Fähigkeiten dreht und nicht mehr nur um das reine Sichern und Wiederherstellen von Daten.

Treiber dieser Entwicklung sind vor allem Cyber-Resilienz, Hybrid-Cloud-Schutz und der Wunsch nach einfacheren Betriebsmodellen. Gartner erwartet, dass bis 2029 rund 95 Prozent der Backup- und Data-Protection-Plattformen integrierte Funktionen zur Erkennung von Cyberbedrohungen enthalten. Für 2025 liegt dieser Anteil nach Einschätzung der Analysten bei 55 Prozent. Auch generative KI spielt inzwischen eine deutlich größere Rolle als noch vor kurzem. Der Anteil entsprechender Funktionen in diesen Plattformen soll von heute unter 25 Prozent auf 90 Prozent bis 2029 steigen.

SaaS-Backup und Plattform-Konsolidierung treiben den Markt

Besonders stark wächst die Bedeutung von SaaS-Backup (Software-as-a-Service). Gartner geht davon aus, dass bis 2029 etwa 80 Prozent der Unternehmen die Sicherung von SaaS-Anwendungen als kritische Anforderung einstufen werden. 2025 sind es demnach 20 Prozent. Parallel dazu steigt der Bedarf an einheitlichen Plattformen für On-Premises- und Cloud-Daten. Aktuell nutzen laut Gartner 25 Prozent der Unternehmen eine gemeinsame Lösung für Backup und Recovery in beiden Welten. Bis 2029 soll dieser Anteil auf 75 Prozent zulegen.

Damit verschiebt sich der Markt klar in Richtung konsolidierter Plattformen, die unterschiedliche Workloads, Betriebsmodelle und Schutzanforderungen unter einem Dach zusammenführen.

Hinzu kommt ein wachsender Trend zu Backup-as-a-Service (BaaS). Nach Gartners Prognose werden bis 2029 rund 85 Prozent der großen Unternehmen solche Angebote zusätzlich zu selbst betriebenen Umgebungen einsetzen. 2025 liegt dieser Wert bei 25 Prozent. Backup wird damit stärker zu einem flexiblen Betriebsmodell, das je nach Workload, Standort und Risikoanforderung aus unterschiedlichen Bereitstellungsformen zusammengesetzt wird.

Datenresilienz ersetzt den klassischen Backup-Blick

Auch **Forrester** betrachtet den Markt inzwischen aus einer breiteren Perspektive. Die *Wave* zu »Data Resilience Solutions« von Ende 2024 soll zeigen, dass Unternehmen heute mehr erwarten als eine funktionierende Datensicherung. Im Vordergrund stehen Lösungen, die Backup, Wiederherstellung, Sicherheits-Funktionen, Governance und betriebliche Wiederanlauffähigkeit zusammenbringen. Der Fokus verschiebt sich damit vom klassischen Backup hin zur umfassenderen Datenresilienz.

Diese Verschiebung hat technische Gründe. Die stärkere Nutzung von IaaS, SaaS, Kubernetes und neuen Virtualisierungs-Plattformen erhöht die Komplexität der Datensicherung deutlich. Gleichzeitig wächst der Druck, im Fall von Ransomware oder anderen Cyberangriffen nicht nur Daten zurückzuspielen, sondern auch verlässlich zwischen kompromittierten und sauberen Datenbeständen unterscheiden zu können.

Gefragt sind deshalb Lösungen, die beschädigte Daten erkennen, vertrauenswürdige Wiederherstellungspunkte identifizieren und eine schnelle Recovery in produktiven Umgebungen unterstützen. Backup-Strategien müssen heute also über das reine Erstellen von Sicherungskopien hinausgehen.

Dominanz der US-Anbieter wird zum Souveränitätsproblem

Neben technischen Kriterien spielt inzwischen auch der rechtliche Rahmen eine größere Rolle. Dabei geht es vor allem um Anbieter mit Sitz in den USA.

Vor rund einem Jahr erschien es plausibel, dass das *EU-US Data Privacy Framework* juristisch erneut scheitern könnte. Dieses Szenario ist bislang nicht eingetreten. Das Abkommen gilt weiterhin und ermöglicht Datentransfers an zertifizierte US-Unternehmen.

Die grundlegenden Konfliktpunkte bleiben jedoch bestehen. Dazu gehören insbesondere mögliche staatliche Zugriffe auf Daten sowie rechtliche Verpflichtungen für US-Unternehmen, Daten an Behörden herauszugeben. Für europäische Unternehmen stellt sich deshalb weiterhin die Frage, wie stark sie sich bei kritischen Infrastrukturen von Anbietern außerhalb des europäischen Rechtsraums abhängig machen wollen.

Der globale Backup-Markt wird von US-Anbietern geprägt

Gleichzeitig zeigt ein Blick auf die Marktanalysen der großen Analystenhäuser ein klares Bild. Die führenden Anbieter im Bereich Backup- und Data-Protection-Plattformen stammen fast ausschließlich aus den USA. Diese prägen den Markt seit Jahren und bestimmen maßgeblich die technologische Entwicklung.

Für europäische Unternehmen ergibt sich daraus ein offensichtliches Spannungsfeld. Wenn rechtliche Risiken und digitale Souveränität stärker berücksichtigt werden sollen, stellt sich zwangsläufig die Frage, ob sich kritische Infrastruktur langfristig auf Software aus einem anderen Rechtsraum stützen sollte.

Vollständiger Wechsel auf europäische Software unrealistisch

Ein radikaler Wechsel auf ausschließlich europäische Backup-Lösungen wäre allerdings für viele Unternehmen kaum realistisch. In zahlreichen Rechenzentren sind Backup-Plattformen seit Jahren tief in die Infrastruktur integriert. Ein Austausch würde erhebliche technische, organisatorische und wirtschaftliche Auswirkungen haben.

Hinzu kommt, dass viele der technologischen Innovationen im Backup-Markt weiterhin von US-Anbietern ausgehen. Funktionen für Cyber-Resilienz, Cloud-Integration, SaaS-Backup oder automatisierte Recovery-Verfahren werden häufig zuerst von den großen internationalen Herstellern umgesetzt.

Wahrscheinlicher ist eine schrittweise Neujustierung

Statt eines abrupten Marktwechsels zeichnet sich daher eher eine andere Entwicklung ab. Europäische Unternehmen prüfen Anbieterstruktur, Support-Zugriffe und Datenflüsse genauer als früher. Gleichzeitig gewinnen europäische Hersteller stärker an Aufmerksamkeit, insbesondere in sensiblen Branchen oder in öffentlichen Einrichtungen.

Ein vollständiger Rückzug europäischer Unternehmen aus US-Software ist derzeit jedoch nicht zu erwarten. Zu stark ist die Marktstellung der etablierten Anbieter, und zu groß sind die Investitionen, die Unternehmen bereits in bestehende Plattformen getätigt haben.

Für den Backup-Markt bedeutet das vermutlich eher eine schrittweise Verschiebung als eine abrupte Abkehr. Digitale Souveränität wird zu einem zusätzlichen Entscheidungskriterium – neben Funktionen, Integrationsfähigkeit und Betriebskosten.

Europäische Anbieter gewinnen an Aufmerksamkeit

Vor diesem Hintergrund prüfen viele Unternehmen verstärkt Alternativen zu großen US-Herstellern. Europäische Anbieter können hier vor allem mit lokalen Support-Strukturen, kürzeren Entscheidungswegen und einem vertrauten Rechtsrahmen punkten.

Gerade im Mittelstand kann das ein wichtiger Faktor sein. Kleinere IT-Abteilungen profitieren häufig davon, wenn Ansprechpartner, Support-

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

Teams und Entwicklung nicht über mehrere Kontinente verteilt sind.

Die Herkunft eines Herstellers allein sollte jedoch nicht das einzige Entscheidungskriterium sein. Ebenso wichtig bleiben technische Funktionen, Integrationsmöglichkeiten, Skalierbarkeit und die Unterstützung moderner Workloads.

Wann ein Wechsel der Backup-Plattform sinnvoll sein kann

Auch wenn die Diskussion über digitale Souveränität an Bedeutung gewinnt, ist ein kurzfristiger Austausch bestehender Backup-Infrastrukturen in vielen Unternehmen unrealistisch. Backup-Plattformen sind häufig tief in Betriebsprozesse, Monitoring, Automatisierung und Recovery-Szenarien integriert. Ein Wechsel bedeutet daher immer auch organisatorischen Aufwand.

In der Praxis prüfen viele Unternehmen Alternativen deshalb vor allem zu bestimmten Zeitpunkten im Lebenszyklus ihrer Infrastruktur. Dazu gehören etwa das Ende von Lizenzlaufzeiten oder Wartungsverträgen. Gerade wenn Software-Abonnements verlängert werden müssen oder Hersteller neue Lizenzmodelle einführen, entsteht häufig ein natürlicher Entscheidungszeitpunkt.

Auch größere Infrastrukturänderungen können einen solchen Moment darstellen. Dazu zählen beispielsweise der Austausch von Virtualisierungs-Plattformen, die Einführung neuer Cloud-Strategien oder eine umfassende Modernisierung der Storage- und Serverlandschaft. In solchen Situationen wird die Backup-Architektur ohnehin überprüft und angepasst.

Ein weiterer Auslöser kann die Konsolidierung von IT-Landschaften sein. Wenn Unternehmen mehrere Backup-Lösungen parallel betreiben oder neue Workloads wie SaaS-Anwendungen und Container-Plattformen absichern müssen, stellt sich häufig die Frage nach einer einheitlichen Plattform.

Für IT-Verantwortliche bietet sich deshalb eine pragmatische Vorgehensweise an: Bestehende Lösungen müssen nicht überstürzt ersetzt werden. Sinnvoller ist es, strategische Veränderungen im Infrastruktur- oder Lizenzzyklus zu nutzen, um Alternativen zu bewerten und gegebenenfalls schrittweise umzusteigen.

Backup bleibt ein zentraler Bestandteil der Cyber-Resilienz

Unabhängig vom Anbieter bleibt Backup eine der wichtigsten Verteidigungslinien gegen Datenverlust und Cyberangriffe. Gerade im Mittelstand entscheidet eine funktionierende Wiederherstellung häufig darüber, ob ein Unternehmen nach einem Angriff schnell wieder arbeitsfähig wird.

Die Anforderungen an Backup-Software werden dabei weiter steigen. Neben klassischen Sicherungsfunktionen gewinnen Cyber-Resilienz, Plattform-Integration, SaaS-Backup und flexible Betriebsmodelle an Bedeutung. Gleichzeitig rückt auch die Frage der digitalen Souveränität stärker in den Fokus.

Für IT-Manager bedeutet das, dass die Auswahl einer Backup-Lösung heute mehr umfasst als einen reinen Funktionsvergleich. Technische Fähigkeiten, Betriebsmodell, Sicherheitsfunktionen und rechtliche Rahmenbedingungen müssen gemeinsam betrachtet werden.

Erst aus dieser Gesamtsicht ergibt sich, welche Lösung langfristig zur eigenen Infrastruktur und zum jeweiligen Risikoprofil passt.

Entwicklungen bei Backup-Lösungen für den Mittelstand

Der Markt für Backup-Software hat sich in den vergangenen Monaten weiter konsolidiert und funktional ausgebaut. Viele Anbieter erweitern ihre Lösungen inzwischen gezielt in Richtung Cyber-Resilienz, Cloud-Integration und Plattformunterstützung.

Ein Beispiel für diese Entwicklung ist die zunehmende Unterstützung alternativer Virtualisierungs-Plattformen. Neben *VMware* und **Microsoft** *Hyper-V* rücken inzwischen auch Plattformen wie *Proxmox VE* stärker in den Fokus vieler Hersteller. Gerade im Mittelstand wächst das Interesse an solchen Lösungen, weil sie häufig kostengünstigere Alternativen darstellen.

Parallel dazu investieren Hersteller verstärkt in Funktionen zur Ransomware-Abwehr. Dazu gehören etwa unveränderbare Backups, automatische Integritätsprüfungen, Malware-Scans sowie Mechanismen zur Identifikation vertrauenswürdiger Wiederherstellungspunkte.

Auch SaaS-Backup gewinnt deutlich an Bedeutung. Die Sicherung von *Microsoft 365*-Daten gehört inzwischen bei vielen Lösungen zum Standard. Dazu zählen vor allem *Exchange Online*, *SharePoint*, *OneDrive* und *Microsoft Teams*.

Konsolidierung und Plattformstrategien verändern den Markt

Der Backup-Markt hat in den vergangenen Monaten zudem eine wichtige Konsolidierungsbewegung erlebt. Besonders sichtbar wurde dies durch die Kombination des Enterprise-Data-Protection-Geschäfts von Veritas mit Cohesity. Das Unternehmen positioniert sich damit als einer der größten Anbieter im Bereich Datenmanagement und Backup-Plattformen.

Diese Entwicklung unterstreicht den Trend zu umfassenderen Data-Protection-Plattformen, die Backup, Archivierung, Datenmanagement und Sicherheitsfunktionen stärker zusammenführen.

Gleichzeitig setzen viele Hersteller stärker auf Cloud-basierte Betriebsmodelle. Neben klassischer Software für lokale Installationen gewinnen Backup-as-a-Service-Angebote an Bedeutung. Gerade für mittelständische Unternehmen kann dies eine Möglichkeit sein, Backup-Infrastrukturen mit geringerem Betriebsaufwand umzusetzen.

Acronis Cyber Protect

Der ursprünglich 2003 in Singapur gegründete Anbieter **Acronis** ist heute ein global agierendes Unternehmen mit Hauptsitz in Schaffhausen in der Schweiz. Der Hersteller positioniert sich längst nicht mehr nur als Anbieter klassischer Backup-Software, sondern als Plattform für Cyber-Protection.

Während *Acronis Cyber Protect Cloud* als cloud-basierter Backup- und Sicherheitsdienst insbesondere für Managed-Service-Provider und mittelständische Unternehmen konzipiert ist, lässt sich *Acronis Cyber Protect* auch lokal betreiben. Die Lösung kombiniert Backup, Disaster Recovery, Anti-Malware, Endpoint-Security sowie Management-Funktionen in einer gemeinsamen Plattform.

Die Software schützt Daten, Anwendungen und Systeme und adressiert physische Server, virtuelle Ma-

schinen (VMs), Cloud-Workloads sowie Endgeräte. Unterstützt werden unter anderem Virtualisierungs-Plattformen wie *Citrix Xen*, Microsoft Hyper-V, *KVM*, *Nutanix*, *Oracle VM*, Proxmox, *Red Hat Virtualization* sowie Vmware.

In neueren Versionen hat Acronis vor allem Funktionen zur Cyber-Resilienz erweitert. Dazu gehören verbesserte Ransomware-Erkennung, automatisierte Malware-Scans in Backups sowie erweiterte Sicherheitsfunktionen für SaaS-Workloads. Zudem integriert der Hersteller stärker Endpoint-Detection- und Response-Funktionen (XDR) in seine Plattform.

Acronis bietet verschiedene Lizenzmodelle für Unternehmen und Managed-Service-Provider. Neben abonnementbasierten Lizenzen gibt es auch nutzungsbasierte Modelle für Service-Provider. Acronis Cyber Protect Advanced kostet beispielsweise im Jahresabo für drei Server rund 1.845 Euro, bei einer dreijährigen Laufzeit etwa 1.303 Euro pro Jahr.

Mehr zu Acronis Cyber Protect ⊙

Archiware P5

Der Münchner Hersteller **Archiware** entwickelt seit mehr als zwei Jahrzehnten Software für Datenmanagement und Archivierung. Die Plattform Archiware P5 kombiniert Backup, Archivierung und Datenreplikation in einer modular aufgebauten Lösung. Die Software richtet sich sowohl an mittelständische Unternehmen als auch an Organisationen mit komplexeren Speicherumgebungen.

Die Plattform besteht aus mehreren Modulen für Backup, Archivierung, Synchronisation und Cloning. Damit lassen sich klassische Datensicherungsaufgaben ebenso abdecken wie langfristige Archivierungsstrategien oder Disaster-Recovery-Szenarien.

Aktuelle Versionen der Plattform haben vor allem das zentrale Management und Monitoring erweitert. Auch Funktionen zur Integritätsprüfung sowie zur Verwaltung verteilter Speicherumgebungen wurden ausgebaut. P5 unterstützt unterschiedliche Speicherziele wie Disk, Tape und Cloud-Speicher und eignet sich daher für hybride Backup-Architekturen.

Ein Schwerpunkt der Lösung liegt weiterhin auf Medien- und Kreativumgebungen sowie heterogenen Speicherlandschaften.

Die Preisgestaltung hängt von der gewählten Edition sowie der Anzahl von Agenten und Speicherressourcen ab. Die *P5 Professional Edition* kostet beispielsweise rund 5.950 Euro und umfasst alle P5-Module für fünf Server-Agenten und zehn Workstation-Agenten.

Mehr zu Archiware P5 ⊙

Bacula Enterprise

Die Backup-Plattform *Bacula Enterprise* wird von **Bacula Systems** mit Sitz im schweizerischen Yverdon-les-Bains entwickelt und basiert ursprünglich auf einem Open-Source-Projekt. Neben der frei verfügbaren Community-Version bietet der Hersteller eine kommerzielle Enterprise-Variante mit erweiterten Funktionen, Zusatzmodulen und professionellem Support.

Die Software adressiert physische Systeme, virtuelle Maschinen, Container-Umgebungen sowie Hybrid-Cloud-Infrastrukturen. Bacula Enterprise unterstützt eine Vielzahl von Betriebssystemen, Datenbanken und Virtualisierungs-Plattformen und gilt als besonders flexibel für komplexe IT-Landschaften.

Neuere Versionen der Plattform erweitern insbesondere die Unterstützung moderner Infrastrukturumgebungen wie *Kubernetes* und containerbasierter Workloads. Darüber hinaus wurden Funktionen für Cyber-Resilienz und automatisierte Wiederherstellung erweitert.

Die Architektur ist modular aufgebaut und erlaubt eine Anpassung an unterschiedliche Anforderungen und Skalierungsstufen. Bacula Enterprise unterstützt dabei Backup-Ziele auf Disk, Tape sowie Cloud-Speicher wie *Amazon S3*, *Microsoft Azure*, *Google Cloud*, *Backblaze B2* oder *Wasabi*.

Die Preisgestaltung richtet sich nach der Anzahl von Clients, Modulen und Speicherressourcen. Konkrete Preise veröffentlicht der Hersteller in der Regel nur projektbezogen.

Mehr zu Bacula Enterprise ⊙

Bareos

Die Backup-Lösung *Bareos* (Backup Archiving Recovery Open Sourced) stammt ursprünglich aus Deutschland und wird heute von **Bareos GmbH & Co. KG** mit Sitz in Köln entwickelt. Die Software entstand als Abspaltung des Bacula-Projekts und ist vollständig Open-Source. Neben der frei verfügbaren Community-Version bietet der Hersteller auch kommerzielle Subskriptionen mit Enterprise-Support an.

Bareos richtet sich vor allem an Unternehmen mit heterogenen IT-Umgebungen sowie an Organisationen mit hohen Anforderungen an Transparenz und Anpassungsfähigkeit. Die Plattform unterstützt physische Server, virtuelle Maschinen, Container-Workloads und Cloud-Infrastrukturen. Zu den unterstützten Systemen zählen unter anderem Linux, Windows, Unix sowie Virtualisierungs-Plattformen wie Vmware, Hyper-V und KVM.

Worauf es bei Backup-Software ankommt

Bei der Auswahl einer Backup-Plattform geht es längst nicht mehr nur um klassische Sicherungsfunktionen. IT-Verantwortliche sollten mehrere Aspekte gleichzeitig bewerten:

Cyber-Resilienz:
Moderne Backup-Lösungen müssen Schutzmechanismen gegen Ransomware bieten, etwa unveränderbare Backups, Integritätsprüfungen oder Malware-Scans.

Plattformunterstützung:
Neben klassischen Servern und virtuellen Maschinen sollten sich auch Cloud-Workloads, SaaS-Anwendungen und Container-Plattformen absichern lassen.

Betriebsmodell:
Viele Unternehmen kombinieren heute lokale Backup-Systeme mit Cloud-Speicher oder Backup-as-a-Service-Angeboten.

Recovery-Fähigkeit:
Entscheidend ist nicht nur die Sicherung der Daten, sondern vor allem eine schnelle und zuverlässige Wiederherstellung.

Rechtsraum und Anbieterstruktur:
Bei internationalen Herstellern ist entscheidend, welchem Rechtsraum Anbieter unterliegen und wie Support- oder Cloud-Strukturen organisiert sind.

Integration in bestehende IT-Infrastruktur:
Backup-Plattformen sollten sich möglichst nahtlos in Monitoring-, Sicherheits- und Storage-Umgebungen integrieren lassen.

Die Architektur ist modular aufgebaut und erlaubt eine flexible Integration in bestehende IT-Landschaften. Als Backup-Ziele lassen sich Disk-, Tape- und Cloud-Speicher einsetzen, darunter auch S3-kompatible Objektspeicher. Funktionen wie Deduplizierung, Verschlüsselung und automatisierte Wiederherstellung unterstützen Unternehmen bei der Umsetzung moderner Backup-Strategien.

Ein Vorteil von Bareos ist die Offenheit der Plattform. Gerade in Umgebungen, in denen digitale Souveränität eine Rolle spielt, kann eine Open-Source-Lösung zusätzliche Transparenz und Kontrolle über die eingesetzte Software bieten.

Bareos kann als Community-Version kostenlos eingesetzt werden. Für den professionellen Betrieb bietet der Hersteller kommerzielle Subskriptionen mit Support und zertifizierten Paketen an, deren Preis projektabhängig kalkuliert wird.

Mehr zu Bareos
Produkt-Review
auf speicherguide.de

Hornetsecurity VM Backup

Die Backup-Lösung *Hornetsecurity VM Backup* richtet sich vor allem an kleine und mittlere Unternehmen sowie Managed-Service-Provider. Der Sicherheitsanbieter **Hornetsecurity** mit Sitz in Hannover hatte 2021 die Backup-Software des Herstellers **Altaro** übernommen und seitdem weiterentwickelt.

Die Lösung konzentriert sich auf die Sicherung virtueller Umgebungen und unterstützt aktuell vor allem Vmware und Microsoft Hyper-V. Neuere Versionen erweitern die Unterstützung für Proxmox-VE-Umgebungen, die insbesondere im Mittelstand zunehmend eingesetzt werden.

Backups können sowohl lokal als auch in Cloud-Speicher wie Microsoft Azure, AWS, Backblaze oder Wasabi abgelegt werden. Zudem unterstützt die Plattform Immutable-Storage-Funktionen zum Schutz vor Ransomware. Weitere Funktionen umfassen blockbasierte Backups, Continuous-Data-Protection-Mechanismen sowie Replikation für Disaster-Recovery-Szenarien. Die Sicherung virtueller Maschinen erfolgt agentenlos.

Im Jahr 2024 wurde Hornetsecurity vom US-Sicherheitsanbieter **Proofpoint** übernommen. Damit gehört auch die Backup-Plattform VM Backup zu einem US-Unternehmen. Mit Blick auf digitale Souveränität müssen IT-Manager die Software eventuell neu bewerten. Während Entwicklung und Teile des Betriebs weiterhin in Europa stattfinden, unterliegt der Konzern nun dem US-Rechtsraum – ein Aspekt, der insbesondere im Zusammenhang mit Themen wie Cloud-Act oder internationalen Support-Strukturen zunehmend diskutiert wird.

Die Lizenzierung erfolgt pro virtueller Maschine oder Host. Die *Unlimited-Plus-Edition* ist beispielsweise im Abonnement ab rund sechs Euro pro VM und Monat erhältlich.

Mehr zu Hornetsecurity
VM Backup

Novastor Datacenter

Der Hamburger Hersteller **NovaStor** ist seit Ende der 1990er-Jahre im Markt für Backup- und Recovery-Software aktiv. Die Plattform *NovaStor DataCenter* richtet sich vor allem an mittelständische Unternehmen sowie IT-Dienstleister.

Die Lösung unterstützt heterogene IT-Umgebungen mit unterschiedlichen Betriebssystemen, Hypervisoren und Datenbanken. Dazu gehören unter anderem Windows, Linux, Unix sowie Virtualisierungs-Plattformen wie VMware, Hyper-V, Nutanix und Proxmox. Auch gängige Datenbanken wie Microsoft SQL, MySQL/MariaDB, PostgreSQL oder Oracle lassen sich integrieren.

Zu den Sicherheitsfunktionen gehören Ende-zu-Ende-Verschlüsselung mit TLS 1.2/1.3 sowie AES-256-Verschlüsselung für Backups. Backups können sowohl lokal als auch in Cloud-Speichern abgelegt werden.

Aktuelle Versionen haben insbesondere zentrale Management- und Monitoring-Funktionen ausgebaut. Eine webbasierte Benutzeroberfläche ermöglicht die Steuerung komplexer Backup-Umgebungen mit vielen Systemen und Workloads.

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

Die Backup-Software *SEP sesam* wird von der **SEP** aus Holzkirchen bei München entwickelt. Die Plattform richtet sich sowohl an mittelständische Unternehmen als auch an größere IT-Umgebungen mit heterogenen Systemlandschaften.

Die Lösung unterstützt eine große Bandbreite an Betriebssystemen, Anwendungen und Virtualisierungs-Plattformen. Dazu zählen unter anderem Vmware, Hyper-V, Nutanix sowie zunehmend auch Proxmox-VE-Umgebungen. Die Unterstützung für *ZFS, LVM-thin* und *Ceph RBD* besteht bereits seit den frühen 5.x-Versionen und wurde in späteren Releases vor allem funktional erweitert und stabilisiert.

Für den Schutz gegen Ransomware setzt SEP Sesam auf mehrere Sicherheitsmechanismen. Dazu gehören Immutable-Storage, S3-Object-Lock sowie zusätzliche Integritäts- und Virenprüfungen beim Restore.

Die Plattform unterstützt parallele VM-Backups und eignet sich damit auch für größere Umgebungen. Funktionen wie Inline-Deduplizierung und Replikation sollen zudem den Speicherbedarf reduzieren.

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

Weiterführende Links:

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

Backup-Strategie und Infrastruktur-Lebenszyklus

WANN SICH EIN WECHSEL DER BACKUP-PLATTFORM ANBIETET

Karl Fröhlich
speicherguide.de

Backup-Systeme gehören zu den langlebigsten Komponenten einer IT-Infrastruktur. Entsprechend selten werden sie vollständig ausgetauscht. Dennoch entstehen im Lebenszyklus von Infrastruktur, Lizenzmodellen oder Betriebsanforderungen immer wieder Zeitpunkte, an denen Unternehmen ihre Backup-Plattform neu bewerten.

Auch wenn Diskussionen über digitale Souveränität oder Herstellerabhängigkeiten an Bedeutung gewinnen, ist ein kurzfristiger Austausch bestehender Backup-Infrastrukturen in vielen Unternehmen unrealistisch. Backup-Plattformen sind häufig tief in Betriebsprozesse, Monitoring, Automatisierung und Recovery-Szenarien integriert. Ein Wechsel betrifft daher nicht nur die Software selbst, sondern auch organisatorische Abläufe, Schulungen und etablierte Betriebsmodelle.

In der Praxis prüfen Unternehmen Alternativen deshalb meist zu bestimmten Zeitpunkten im Lebenszyklus ihrer Infrastruktur. Dazu gehört etwa das Ende von Lizenzlaufzeiten oder Wartungsverträgen. Wenn Software-Abonnements verlängert werden müssen oder Hersteller neue Lizenzmodelle einführen, entsteht häufig ein natürlicher Entscheidungszeitpunkt.

Checkliste:

Wann IT-Verantwortliche ihre Backup-Plattform prüfen sollten

Lizenzverlängerung steht an
Wartungsverträge oder Software-Abonnements laufen aus und neue Lizenzmodelle verändern Kosten oder Nutzungsbedingungen.

Neue Workloads müssen abgesichert werden
Container-Plattformen, SaaS-Anwendungen oder hybride Cloud-Umgebungen kommen hinzu.

Kosten steigen überproportional mit Datenvolumen
Lizenzmodelle reagieren empfindlich auf wachsende Datenmengen oder zusätzliche Workloads.

Mehrere Backup-Lösungen parallel im Einsatz
Historisch gewachsene Umgebungen führen zu höherem Betriebsaufwand und komplexeren Prozessen.

Neue Anforderungen an Cyber-Resilienz
Funktionen wie unveränderliche Backups, isolierte Recovery-Umgebungen oder automatisierte Wiederherstellung fehlen oder sind nur eingeschränkt verfügbar.

Steigender Betriebs- und Managementaufwand
Backup-Prozesse lassen sich nur noch mit zusätzlichem Aufwand automatisieren oder integrieren.

Neue Infrastruktur wird eingeführt
Wechsel der Virtualisierungs-Plattform, neue Cloud-Strategien oder Modernisierung von Server- und Storage-Systemen.

Grafik: speicherguide.de via DALL-E

Backup-Plattformen entscheiden darüber, wie unabhängig, sicher und handlungsfähig Unternehmen im Krisenfall bleiben.

Infrastrukturänderungen als Auslöser

Auch größere Infrastrukturprojekte können einen solchen Moment darstellen. Dazu zählen etwa der Austausch von Virtualisierungs-Plattformen, die Einführung neuer Cloud-Strategien oder eine umfassende Modernisierung der Storage- und Server-Landschaft. In solchen Situationen wird die Backup-Architektur ohnehin überprüft und angepasst.

SaaS-Anwendungen, Container-Plattformen oder hybride Cloud-Umgebungen stellen häufig Anforderungen, die klassische Backup-Konzepte nur teilweise abdecken. Unternehmen prüfen daher zunehmend, ob bestehende Lösungen diese Szenarien ausreichend unterstützen.

Typische Indikatoren für eine Neubewertung

Für IT-Leiter ergeben sich in der Praxis mehrere konkrete Signale, die eine Überprüfung der bestehenden Backup-Plattform sinnvoll machen können. Ein häufiger Auslöser sind steigende Lizenz- oder Betriebskosten, etwa wenn neue Preismodelle eingeführt werden oder zusätzliche Workloads abgesichert werden müssen.

Auch der Betriebsaufwand spielt eine Rolle. Wenn Backup-Umgebungen zunehmend komplex werden, mehrere Tools parallel betrieben werden oder wichtige Funktionen nur mit Zusatzlösungen realisierbar sind, wächst der Druck zur Konsolidierung.

Ein weiterer Indikator kann die eingeschränkte Unterstützung neuer Plattformen sein. Moderne IT-Umgebungen integrieren zunehmend Container-Plattformen, SaaS-Anwendungen oder hybride Cloud-Strukturen. Wenn vorhandene Backup-Lösungen diese Szenarien nur eingeschränkt unterstützen, geraten bestehende Architekturen schnell an ihre Grenzen. Nicht zuletzt gewinnen Sicherheitsanforderungen an Bedeutung. Funktionen wie unveränderliche Backups, isolierte Recovery-Umgebungen oder automatisierte Wiederherstellungsprozesse sind heute zentrale Bausteine einer Cyber-Resilienz-Strategie. Wenn diese Funktionen fehlen oder nur eingeschränkt verfügbar sind, kann eine Neubewertung der Plattform sinnvoll sein.

Schrittweise Modernisierung statt Komplettumstellung

Für IT-Verantwortliche bietet sich deshalb eine pragmatische Vorgehensweise an. Bestehende Lösungen müssen nicht überstürzt ersetzt werden. Sinnvoller ist es, strategische Veränderungen im Infrastruktur- oder Lizenzzyklus zu nutzen, um Alternativen zu bewerten.

In vielen Fällen erfolgt der Wechsel schrittweise. Neue Plattformen sichern zunächst zusätzliche Workloads oder modernisierte Infrastrukturkomponenten ab, während bestehende Backup-Systeme parallel weiterlaufen. Erst mit der Zeit wird die Umgebung konsolidiert. Dieser Ansatz reduziert Risiken und erleichtert die Migration bestehender Datenbestände.

Gleichzeitig kann eine solche Neubewertung auch einen Beitrag zur digitalen Souveränität leisten. Wer Backup-Plattformen regelmäßig im Kontext von Infrastruktur, Lizenzmodellen und Sicherheitsanforderungen überprüft, behält mehr Handlungsspielraum gegenüber Herstellern und Technologien. Entscheidungen entstehen dann nicht aus kurzfristigem Druck, sondern aus einer strategischen Bewertung der eigenen IT-Architektur. ■

Bild: speicherguide.de/NCS via DALL·E

Karl Fröhlich
speicherguide.de

Backup, Disaster-Recovery und Ausfallsicherheit

WENN DER STANDORT AUSFÄLLT UND DIE IT WEITERLÄUFT

Ein Brand, Wasserschaden oder technischer Defekt trifft nicht nur Räume und Inventar, sondern oft auch Zugänge, Prozesse und Zuständigkeiten. Für mittelständische Unternehmen reicht ein Backup deshalb allein nicht aus. Erst wenn Daten, Systeme und Arbeitsfähigkeit voneinander entkoppelt sind, bleibt der Betrieb im Ernstfall handlungsfähig, wie beim Friedberger Integrator NCS.

Wenn über Backup gesprochen wird, geht es im Mittelstand oft zuerst um Datensicherung, Aufbewahrungsfristen und Wiederherstellungspunkte. Das ist wichtig, greift aber zu kurz. Ein echter Notfall betrifft nicht nur Daten. Er betrifft Gebäude, Arbeitsplätze, Kommunikationswege, Zuständigkeiten und den Zugang zu den Systemen. Genau deshalb beschreibt das **BSI** (Bundesamt für Sicherheit in der Informationstechnik) Notfallmanagement als geplantes und organisiertes Vorgehen, um die Widerstandsfähigkeit zeitkritischer Geschäftsprozesse zu sichern. Im BSI-Umfeld gehören dazu ausdrücklich Business-Impact-Analyse und die Frage, wie lange ein Ausfall maximal tolerierbar ist.

Backup schützt Daten, aber nicht automatisch den Betrieb

Ein funktionierendes Backup ist unverzichtbar. Es beantwortet aber noch nicht die Frage, ob ein Unternehmen nach einem Gebäudeschaden arbeitsfähig bleibt. Die *NIST*-Leitlinie *SP 800-34* trennt deshalb klar zwischen Datensicherung, alternativem Speicherort und alternativem Verarbeitungsstandort. Gefordert sind nicht nur Backups, sondern auch getrennte Speicherorte, Ausweich-Möglichkeiten für den Betrieb und eine Wiederherstellung im Rahmen der definierten Recovery-Ziele. Mit anderen Worten: Die Sicherungskopie allein ist noch keine Betriebsfortführung. Sie ist nur ein Baustein davon.

Backup schafft Sicherungskopien der Daten. Disaster-Recovery zielt darauf, IT-Services nach einem Ausfall wieder bereitzustellen. Business-Continuity beschreibt Maßnahmen, mit denen kritische Prozesse auch bei Störungen weiterlaufen oder schnell fortgesetzt werden.

Architektur entscheidet über die Handlungsfähigkeit

Für mittelständische IT-Umgebungen wird damit eine Frage zentral, die in vielen Backup-Konzepten zu wenig Beachtung findet: Hängt der Betrieb noch am Gebäude oder nicht mehr? Wer Server, Backup-Infrastruktur, Management-Systeme und Kommunikationswege an einen einzelnen Standort koppelt, trägt ein Gebäuderisiko in der Architektur. Wer diese Komponenten trennt, etwa über Colocation, Managed-Services, Cloud-Dienste, ein zweites Rechenzentrum oder klar definierte Ausweich-Arbeitsplätze, reduziert dieses Risiko deutlich. Auch CISA verweist darauf, dass Ausweich-Standorte, alternative Nutzung bestehender Flächen und Remote-Arbeit die Resilienz und Business-Continuity verbessern.

Standort-Trennung als Resilienz-Prinzip

Wie relevant dieses Szenario ist, zeigt ein aktueller Vorfall in Friedberg bei Augsburg. Beim Systemintegrator **NCS** kam es Mitte Januar 2026 zu einem Brand im Heizungsraum. Rauch und Schadstoffe verteilten sich über die Lüftungsanlage im Gebäude. Die




Augsburger Allgemeine bezifferte den Schaden auf 150.000 Euro.

Das Gebäude wurde geräumt und blieb auch nach den Löscharbeiten zunächst unbenutzbar. Trotzdem konnte das Unternehmen weiterarbeiten, weil die zentralen IT-Systeme nicht im Bürogebäude, sondern in einem Rechenzentrum außerhalb betrieben wurden. »Der Vorfall hat gezeigt, dass ein Backup-Konzept allein nicht genügt«, erklärt NCS-Geschäftsführer **Stefan Schneider** gegenüber *speicherguide.de*. »Entscheidend war für uns, dass Systeme, Daten und Arbeitsplätze so voneinander entkoppelt waren, dass der Betrieb auch ohne Gebäude weiterlaufen kann.«

Ein zweiter Brandabschnitt ist in vielen Rechenzentren Standard, aber er löst nur einen Teil des Problems. Er reduziert das Risiko, dass sich ein Feuer oder Rauch im Gebäude unkontrolliert ausbreitet, und schützt damit Infrastruktur innerhalb eines Standorts. Im NCS-Beispiel ist der entscheidende Punkt jedoch ein anderer: Die zentralen Systeme waren nicht nur »besser getrennt«, sondern räumlich ausgelagert und damit vom Bürogebäude entkoppelt. Das ist mehr als Brandschutz, es ist eine Architektur-Entscheidung. Denn sobald ein Gebäude evakuiert wird oder nach einem Schaden nicht mehr betreten werden darf, scheitert der Betrieb häufig nicht an fehlenden Backups, sondern an alltäglichen Abhängigkeiten wie Zugängen, Management-Werkzeugen, Identitäten oder Kommunikationswegen. Genau hier zeigt die Standort-Trennung ihren Wert: Sie verlagert das Risiko weg vom Gebäude und hin zu planbaren Betriebsprozessen.

Im Ernstfall geht es um die Handlungsfähigkeit

Der Vorfall legt einen blinden Fleck vieler Backup-Strategien offen: In zahlreichen mittelständischen Umgebungen werden Daten inzwischen ordentlich gesichert, aber die Betriebsfähigkeit im Fall eines Standort-Ausfalls bleibt unzureichend durchdacht. Fällt das Gebäude weg, fehlen mitunter nicht nur Server oder Speichersysteme, sondern auch Telefonie, Netzwerk-Zugänge, Management-Werkzeuge, Schlüsselpersonen und definierte Ausweich-Prozesse.

Der Friedberger Fall zeigt deshalb weniger die Qualität eines einzelnen Anbieters als vielmehr ein Grundprinzip moderner IT-Architekturen: Kritische Services sollten nicht an denselben physischen Ort gebunden sein, an dem auch der reguläre Büro-Alltag stattfindet. »Im Ernstfall geht es nicht zuerst um Technik, sondern um Handlungsfähigkeit«, ergänzt Schneider. »Wer auf Systeme zugreifen, Support leisten und Kundenanfragen weiterbearbeiten kann, hat die wichtigste Hürde bereits genommen.«

Konsequenzen für Backup- und Notfallplanung im Mittelstand

Für den Mittelstand ergibt sich daraus keine Einheitslösung, aber eine klare Reihenfolge. Zuerst steht die Business-Impact-Analyse. Welche Systeme müssen nach einem Vorfall in Stunden wieder laufen, welche erst später, und welche lassen sich vorübergehend auch manuell überbrücken? Danach folgt die Architektur-Frage. Wo liegen produktive Systeme, wo die Backups, wo die Management-Ebene und von wo aus kann im Notfall gearbeitet werden?

Ebenso wichtig sind Abhängigkeiten wie Identitäts- und Zugriffs-Management, Remote-Zugänge, Telefonie, Monitoring, Dokumentation und die Verfügbarkeit von Schlüsselrollen. Erst im dritten Schritt geht es um die konkrete Technik, also etwa Backup-Software, Immutable-Speicherziele, Tape, Cloud-Repository, Ausweich-Standort oder Managed-Service-Modell. Das BSI verknüpft diese Planung mit der maximal tolerierbaren Ausfallzeit. NIST fordert ergänzend, Backups und Restore-Verfahren regelmäßig zu testen, statt sich auf das bloße Vorhandensein von Sicherungskopien zu verlassen.

Backup muss den Ernstfall abbilden

Die Qualität eines Backup-Konzepts entscheidet sich nicht nur daran, ob Daten gesichert werden, sondern daran, ob sich aus diesen Daten unter realen Bedingungen wieder arbeitsfähige IT-Services herstellen lassen. Ein Brand, ein Wasserschaden oder eine länger andauernde Gebäudesperrung sind keine theoretischen Randereignisse. Sie sind plausible Ausfalltypen. Wer sie im Backup- und Recovery-Konzept mitdenkt, plant nicht pessimistischer, sondern realistischer. Und genau das dürfte für viele mittelständische Unternehmen die eigentliche Reifeprüfung ihrer Backup-Strategie sein. ■

Interview mit Stefan Schneider, Geschäftsführer, NCS

STANDORT-AUSFALL: SYSTEMINTEGRATOR ALS EIGENER RESILIENZ-PROOF

Ein Brand am Bürostandort kann Abläufe, Arbeitsplätze und Kommunikation wochenlang blockieren. Beim Systemintegrator NCS verursachten Rauch, Ruß und Schadstoffe den größten Schaden. Der IT-Betrieb blieb dennoch stabil, weil systemkritische Anwendungen im externen Rechenzentrum liefen und das Team binnen zwei Stunden auf Ausweich-Arbeitsplätze wechselte. Wir sprachen mit NCS-Geschäftsführer Stefan Schneider über die Folgen des Brandes am Standort und warum das Unternehmen nun sein eigener bester Proof ist.

Karl Fröhlich
speicherguide.de

Im Firmengebäude von NCS hat es gebrannt, was genau ist passiert?

Schneider: Im Bereich der Heizungsanlage kam es zu einem Kurzschluss. Zunächst entwickelte sich ein Schwelbrand mit starker Rauchbildung. Als die Tür geöffnet wurde und Zugluft entstand, ist daraus ein Feuer geworden. Die wesentlichen Schäden in den Räumlichkeiten wurden jedoch nicht durch das Feuer verursacht, sondern durch Rauch, Ruß und den daraus entstandenen Schadstoffen.

Im Grunde hatten wir Glück, weil das Feuer sehr früh am Morgen ausgebrochen und entdeckt wurde. Es war erst ein Mitarbeiter im Haus, der mich wegen eines Alarmsignals informiert hat und auf meine Anweisung zum Heizungskeller gegangen ist. Der Kollege hat sich direkt in Sicherheit gebracht und dafür gesorgt, dass niemand mehr das Gebäude betritt. Ich habe währenddessen die Feuerwehr alarmiert.

Wie sah das Schadenbild nach dem Einsatz aus?

Schneider: Wir mussten das komplette Gebäude im Grunde auf »Null drehen«. Böden, Einrichtung, es musste alles raus. Ruß ist giftig und kann über Zeit offenbar auch Materialien wie Kupferleitungen angreifen. Wir haben alle Möbel entsorgt und beispielsweise rund 60 Monitore und praktisch die komplette Inneneinrichtung. Es ist so gut wie nichts übrig geblieben.

Wir gehen inzwischen von einer Schadenssumme von über einer Million Euro aus. Das zeigt auch, dass ein solcher Vorfall nicht nur ein »Büroproblem« ist, sondern schnell eine existenzielle Dimension bekommen kann.

Stefan Schneider
NCS-Geschäftsführer

Das Büroproblem konntet Ihr aber sehr schnell lösen.

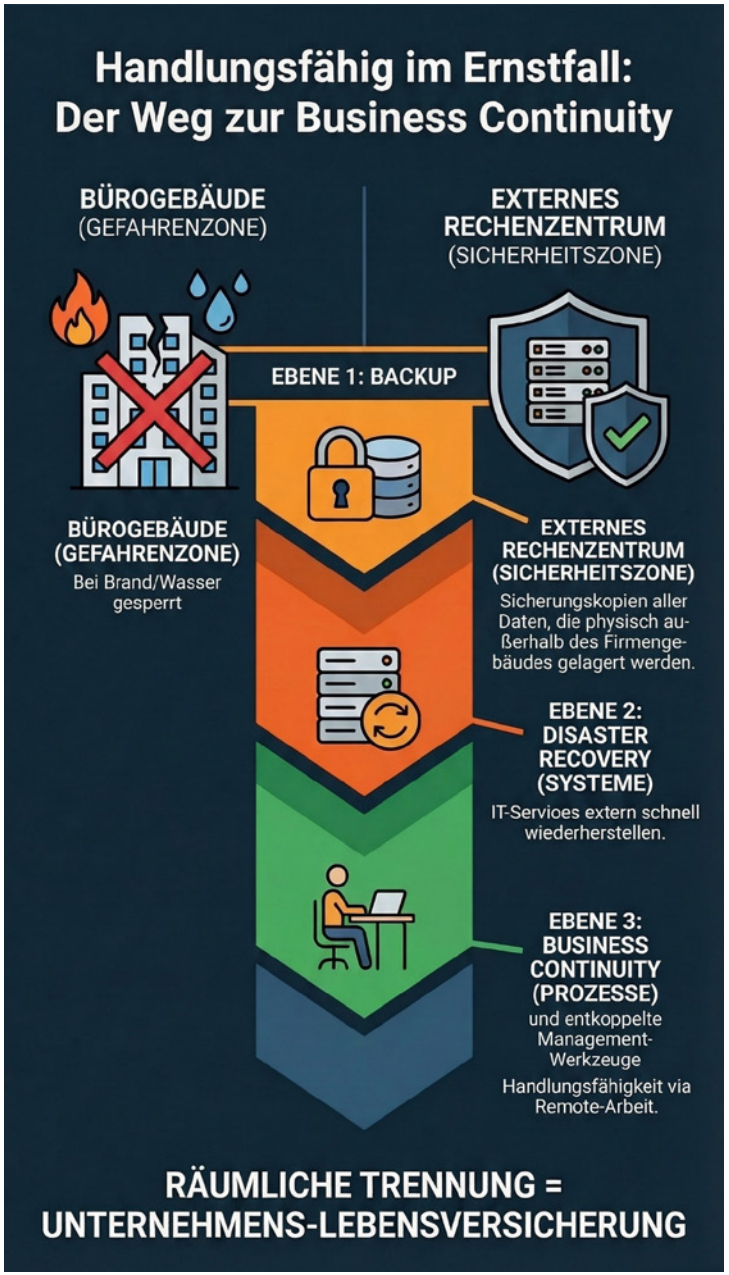
Schneider: Der Brand wurde gegen 7:00 Uhr morgens festgestellt. Ab da ging es um zwei Dinge. Erstens Sicherheit und Abstimmung mit Einsatzkräften. Zweitens so schnell wie möglich Arbeitsfähigkeit herstellen. Bereits um 9:00 Uhr konnten wir bei einem benachbarten Unternehmen Büroräume anmieten. Zufällig waren dort Räume frei. Das war ein echter Glücksfall.

Wie konnten Eure Mitarbeiterinnen und Mitarbeiter so schnell weiterarbeiten?

Schneider: Weil fast alle mit Notebooks arbeiten und die meisten ihre Geräte ohnehin dabeihatten. Dadurch konnten viele sofort im Ausweichbüro oder aus dem Home-Office weiterarbeiten. Das war sehr effektiv.

Das heißt, es gab keinen IT-Ausfall oder Beeinträchtigungen für Mitarbeitende wie auch für Kunden?

Schneider: Einen spürbaren IT-Ausfall gab es nicht. Kunden und Lieferanten haben im Normalbetrieb praktisch nichts bemerkt. Der Grund ist, dass alle systemkritischen Anwendungen im Colocation-Rechenzentrum LEW Green Data Center in Augsburg laufen. Damit waren wir nicht vom Bürogebäude abhängig und konnten einfach weiterarbeiten – und wurden dabei aber unfreiwillig zum



Grafik: speicherguide.de via NotebookLM

eigenen Praxistest. Die Architektur-Entscheidung für ausgelagerte, systemkritische Anwendungen hat sich im realen Vorfall bewährt – nicht auf dem Papier, sondern unter Zeitdruck und mit gesperrtem Gebäude.

Was ist aus Eurer Sicht die wichtigste Lehre aus dem Vorfall?

Schneider: Der Vorfall hat gezeigt, dass ein Backup-Konzept allein nicht genügt. Entscheidend ist, dass Systeme, Daten und Arbeitsplätze so voneinander entkoppelt sind, dass der Betrieb auch ohne Gebäude weiterlaufen kann.

Und ja, es war am Ende auch Glück dabei, etwa weil wir so schnell Ausweichräume gefunden haben. Auch unserem Versicherungsvertreter muss ich ein Kompliment machen, der kam direkt vorbei und hat die Schadensregulierung übernommen. Wie sich herausstellte, waren wir sehr gut beraten, bis hin zu einer Neuwertversicherung. Beispielsweise war auch eine Palette mit Kunden-Servern voll versichert. Was sich als sehr wichtig erwiesen hat: Wir hatten alles dokumentiert und belegbar vorliegen. Diese Vorarbeit entscheidet im Ernstfall mit darüber, wie schnell man wieder handlungsfähig wird.

Was uns hier ebenfalls rettete, war eine absolut saubere Anlagenbuchhaltung. Wir konnten auf Knopfdruck unseren Bestand und die zugehörigen Werte abrufen. Das läuft bei uns über DATEV und ist ebenfalls nicht an die lokale IT gebunden. Diese Transparenz hilft enorm, um Schäden sauber zu beziffern und später auch geltend zu machen. Die Dokumentation wird gerne unterschätzt, im Ernstfall ist sie überlebenswichtig.

Welche Empfehlungen leitet Ihr daraus für mittelständische Unternehmen ab?

Schneider: Ich empfehle, einmal im Jahr eine Katastrophenübung durchzuspielen. Außerdem sollte immer eine aktuelle Datensicherung außerhalb der Geschäftsräume gelagert werden. Und ein Notfallplan ist nur dann brauchbar, wenn er auch im Notfall zugreifbar ist, inklusive Zuständigkeiten, Passwörtern und der Frage, wer was wann entscheidet.

Was ist der aktuelle Stand, und wie geht es weiter?

Schneider: Aktuell planen wir, bereits zum 1. Mai wieder einzuziehen. Das ist ambitioniert, aber das ganze Team packt mit an. Und inhaltlich würden wir gar nicht sagen, dass wir jetzt alles umwerfen müssen. Durch die Auslagerung haben wir in diesem Punkt vieles richtig gemacht. Wichtig ist, konsequent weiterzumachen, Dokumentation aktuell zu halten und die Notfallplanung regelmäßig zu prüfen. ■

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

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

Schlussredaktion:
Bettina Röber

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