



Backup für den Mittelstand

Trend: Datensicherung wird zum Datenmanagement

Backup/Recovery: KMUs lassen nötige Ernsthaftigkeit vermissen

Liebe Leserinnen und Leser,

auch auf die Gefahr mich zu wiederholen, Backup & Recovery reicht bei weitem nicht mehr aus. Firmen müssen ihre Datensicherungsstrategien auf den Prüfstand stellen und Data-Protection als umfassenden Datenschutz erkennen und einführen. Grundsätzlich lassen sich vier (bekannte) Problemherde definieren: ein ungebremses Datenwachstum, Bedrohungen von außen, unterschiedliche Datenquellen und das Erfüllen rechtlicher Bestimmungen und Vorschriften. Diese sind alle nicht neu, verschärfen sich aber zusehend.

Ransomware ist eine ernstzunehmende Bedrohung. Mit jedem Cloud-Dienst und neuem Mitarbeiter kommen zusätzliche Datenquellen hinzu. Die Datenschutz-Grundverordnung (DSGVO) hat letztes Jahr massiven Einfluss auf die Datensicherheit genommen. Konzerne und große Mittelständler müssen schon aus Compliance-Gründen – und natürlich aus eigenem Interesse – die DSGVO korrekt umsetzen. Je kleiner die Unternehmen der Sparte KMUs werden, desto weniger bis gar nicht setzen sich die Verantwortlichen mit dieser Problematik auseinander.



Karl Fröhlich,
Chefredakteur
speicherguide.de

Die Verantwortlichen müssen sich schon die Fragen gefallen lassen, wie kann das sein? Letztes Jahr wunderten wir uns an dieser Stelle auch, dass es immer noch eine große Anzahl an Backup-Verweigerer gibt. Eine Umfrage zum »World Backup Day« ergab, dass ein Drittel der Befragten Unternehmen und Verbraucher kein aktuelles Backup von ihren wichtigen Daten besitzen. Als Grund wird angeführt, es fehle an Zeit, um eine geeignete Backup-Lösung zu finden und diese regelmäßig zu administrieren. Auch ein Datenverlust wird von vielen in Kauf genommen. Die ordnungsgemäße Funktion der Backup-Lösung wird nur selten geprüft.

Leider hat sich die Lage wenig verändert, zumindest nicht zum Positiven. Dies bestätigen mir meine Gespräche auf den letzten Veranstaltungen. Oft genug fehlt es nicht nur an einer Strategie, sondern schon an den Grundlagen und von der nötigen Ernsthaftigkeit will ich gar nicht sprechen.

Wir nehmen dies zum Anlass, uns wieder mehr den Basics zu widmen und unsere Grundlagenbeiträge aufzufrischen. Daher wird es in Kürze noch einmal ein Update zu dieser Ausgabe geben.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Inhalt

Editorial Seite **2**

Datensicherungstrends

Datensicherung im Wandel Seite **4**

Datensicherungsstrategie

Backup-Service: Von der Strategie bis zur Implementierung Seite **8**

Advertorial

Datensichere Zukunft an zwei Bierbrauer-Standorten Seite **10**

Warum nicht einfach Nearline-Storage und Backup-Server kombinieren? Seite **12**

Datensicherung

Backup muss auch Datenmanagement-Anforderungen erfüllen Seite **14**

Data-Protection-Markt

Backup und Daten-Resilienz Seite **17**

Backup-Hardware

LTO-8: Doppelte Kapazität und etwas mehr Speed Seite **20**

Datensicherungsstrategie

Unersetzlich: Die 3-2-1-Backup-Regel Seite **21**

Impressum Seite **22**

Storage-Forum 2019

28. + 29. November

Eventpalast Leipzig

Das Storage-Forum 2019 ist eine Plattform zum fachlichen Austausch für Nutzer und Anbieter von Enterprise-Storage-Systemen und -Lösungen.

In Keynotes, Anwenderberichten und Vorträgen sowie der Begleitausstellung informieren wir Sie über Technologien und Trends in den Bereichen Data Management, Data Storage, Archivierung, Backup u.v.a.m.

Early-Bird-Tickets gibt es noch bis 13.10.2019. Bitte [registrieren](#) Sie sich rechtzeitig.

Keynote-Speaker

Michael M. Beeck – Unternehmer, Querdenker, Strategie-Consultant und Referent

Peter Buschman – Product Owner Storage, booking.com

Frank Karlitschek – Gründer und Geschäftsführer, Nextcloud GmbH

Wolfgang Stief – Unternehmer, Übergeek, Storagenerd

Die vollständige Agenda wird am 30.09.2019 veröffentlicht.

www.storage-forum.de

Sponsoren

BOSTON
Servers | Storage | Solutions

 **DATACORE**

FAST LTA

FUJIFILM

 **LucidLink**

 **ScaleFlux**

 **SCALITY**

Backup für den Mittelstand

Datensicherung im Wandel

Die Grundanforderungen bleiben zwar unverändert, trotzdem wird die Datensicherung immer komplexer und schwieriger. Damit steigt die Verantwortung, die auf den IT-Verantwortlichen lastet. Künftig gilt es nicht nur das Datenwachstum zu handhaben, sondern auch die vielen unterschiedlichen Quellen. Flash wird fester Bestandteil kommender Backup-Strategien, aber auch Tape bleibt gesetzt.

Karl Fröhlich

Das Datenwachstum fordert nicht nur die Datenspeicherung, sondern auch die Datensicherung – und dies natürlich auch schon seit Jahren. Auch die Verkürzung der Zeitfenster für Backup-Prozesse sowie der Einhaltung festgelegter Recovery-Ziele sind keine neuen Anforderungen. Trotzdem wird Data-Protection im Unternehmen gefühlt immer schwieriger. Wir haben uns in der Branche umgehört und dieser Eindruck täuscht keineswegs. Die Gründe sind vielfältig.

Viele unterschiedliche Workloads sowie Daten und Compliance-Anforderungen unterschiedlichster Art erhöhen den Schwierigkeitsgrad. »Hinzukommt die Sicherheitsfrage und die Tatsache, wo und wie die



Foto: speicherguide.de

Stefan Roth
Fujitsu

»In den kommenden Jahren werden in den Bereich Backup/Recovery und Data-Protection im Kontext der Digitalisierung deutlich mehr Investitionen fließen.«

einzelnen Daten erzeugt werden, zum Beispiel Edge-Core-Cloud«, erklärt **Stefan Roth**, Category Manager Datacenter Central Europe bei **Fujitsu**. »Das alles erfordert nicht nur unterschiedliche Technologien, sondern auch verschiedene Formen der Integration, um die Daten je nach SLA abzusichern zu können. Absichern heißt dabei natürlich nicht einfach Wegschließen: Die Datenverfügbarkeit muss ebenso gewährleistet sein wie eine schnelle Wiederherstellung und auch eine effiziente Archivierung.«

Für **Albrecht Hestermann** sind die Probleme aber auch oft hausgemacht: »Oft genug wissen die Leute nicht was sie tun sollen«, sagt der Leiter Vertrieb & Marketing bei **actidata**, gegenüber *speicherguide.de*. »Dass mag provokativ klingen trifft aber in ganz, ganz vielen Fällen zu. Vorgaben aus



Foto: Actidata

Albrecht Hestermann
Actidata

»Viel zu sehr verlässt sich die Geschäftsleitung auf den IT-Admin und seine vorgehaltenen Backups und ist damit der »natürliche Feind aller Unternehmensbereiche«, wenn es zum Datencrash kommt.«

den Führungsetagen werden hinsichtlich Datensicherheit, Datensicherung und Betriebssicherheit aus Unwissenheit vermischt und sind oft auf Grund populärer Stichworte seitens der Schwerpunkte falsch gesetzt. Beispiel: Wir müssen in die Cloud – koste es, was es wolle! Das die Cloud für das Backup und das Restore oftmals ungeeignet ist, sollte bekannt sein. Admins werden somit zu ausführenden Organen, wo-

bei diese doch eigentlich eher federführend sein sollten.«

Hauptanforderungen in den IT-Abteilungen 2019

Die IT-Abteilungen in den Unternehmen waren schon immer gefordert, aber das Datenwachstum und die akute Abhängigkeit von der IT, erschweren die Aufgaben zusehend. Letztendlich steigt auch die Verantwortung, ohne dass dies monetär oder in den Budgets Berücksichtigung findet.



Foto: speicherguide.de

Hannes Heckel
Fast LTA

»Als größte Herausforderungen sehen wir das immense Datenwachstum, dem herkömmliche Speichersysteme oft nicht gewachsen sind«

»Manche mögen sich angesichts des enormen Arbeitspensums sogar partiell überfordert fühlen«, sagt Roth. »Zumal viele Unternehmen immer noch keine dedizierten Backup-Experten haben. Tatsächlich gibt es viel zu tun. Das Spektrum reicht von einer umfänglichen Erfassung, wo die Daten überhaupt erzeugt und gespeichert werden, über die Suche nach optimalen Orten zur Informationsablage bis hin zur Verfügbarkeit entsprechender Budgets.« Ebenfalls hochrelevant sei die Sicherstellung der Compliance, auch im Hinblick auf die DSGVO.

Kompetenz, Know-how, Objektivität und eine fehlende Notfallplanung gehören für Actidata-Manager Hestermann zu den aktuellen »Pain-Points« der IT-Abteilungen: »Bezogen auf Hardware (also Tape und Disk) im Rahmen der Datensicherung stellen wir immer wieder fest, dass Admins sich auf Anwendung und Software konzentrieren, aber die Hardware-Aspekte und damit die Definition deren Leistungsanforderungen nicht überblicken.«

Auch die Cloud rückt bei der Frage nach der richtigen Ablage und Sicherheit für Backups in den Fokus. Dabei gelte es die Recovery-Time ebenso zu berücksichtigen, wie die Möglichkeit eines individuellen Zugschnitts des jeweiligen Backup-, Restore- und Archivierungskonzepts.

Folgen Sie
speicherguide.de
auch auf
unseren
Social-Media-
Kanälen

speicherguide.de



»Als größte Herausforderungen sehen wir das immense Datenwachstum, dem herkömmliche Speichersysteme oft nicht gewachsen sind«, ergänzt **Hannes Heckel**, Marketing Manager bei **FAST LTA**. »Dazu kommen die erwähnte Absicherung gegen Ransomware, und die steigende Gesamtkomplexität der IT. Deswegen kann man in *Silent Brick* Systemen Archiv und Backup im selben System realisieren und voneinander unabhängig skalieren.«

Flash als Backup-Medium

Disk-Backup-Systeme haben die Sicherung deutlich beschleunigt, trotzdem wird noch mehr Leistung benötigt. Viele Anbieter sehen Flash-basierte Backup-Systeme als den nächsten logischen Schritt. Bei **Pure Storage** waren die Verantwortlichen durchaus überrascht, weil viele Kunden die gekauften All-Flash-Systeme für Backups einsetzen. Aufgrund der anhaltenden Nachfrage brachte der Hersteller mit der *ObjectEngine* sogar ein eigenes Produkt auf den Markt.

Laut Pure wechseln rund 57 Prozent der Unternehmen innerhalb der nächsten zwei Jahre ihre bestehende Datenschutzlösung und sieht hier durchaus Potenzial für ein Flash-Konzept: »Veraltete Ansätze der Datensicherung wurden für eine Welt entwickelt, in der Daten eine Last darstellten und nicht als strategischer Mehrwert erachtet

wurden«, meint **Markus Grau**, Principal Systems Engineering bei Pure. »Mit herkömmlichen Lösungen kann es Stunden oder Tage dauern, um geschäftskritische Daten in einer Umgebung wiederherzustellen, in der Echtzeitzugriff zur Erwartung der Verbraucher geworden ist.«

»Der Trend hin zu Flash-Speichern ist natürlich auch im Backup angekommen, zumindest für die täglichen Snapshots, um im Notfall möglichst schnell wieder betriebsbereit sein zu können«, ergänzt Fast-LTA-Manager Heckel hervor. »Funktionen wie Veeam InstantRecovery, die das Starten von VMs während der Wiederherstellung erlauben, werden durch Flash-Backups erheblich beschleunigt. Für die großen Datenmengen von wöchentlichen und monatlichen Backups werden Festplatten weiterhin die Hauptrolle spielen. Gerade haben wir mit dem *Silent Brick DS* eine nicht-transportable Erweiterung für unser *Silent Brick*-System vorgestellt, auf der sich pro Höheneinheit bis zu 192 TByte (brutto) speichern lassen – entstanden aus klaren Kundenanforderungen.«

Wobei Flash nicht immer eine höhere Backup-/Recovery-Geschwindigkeit bedeuten muss. »Das ist von der E2E-Lösung abhängig«, meint Roth. »Schon jetzt setzen viele Unternehmen Flash als Caching und für schnelle Snapshots beispielsweise oder



Foto: speicherguide.de

Ines Wolf
Quantum

»Firmen sollten in eine flexible, zukunftsstaugliche Strategie investieren, weg von Insellösungen und hohem manuellem Aufwand.«

für Schattenlösungen ein. Auch in Backup-Appliances hat Flash schon Einzuges erhalten. Hier bringen die entsprechenden Lösungen je nach geforderten SLA konkrete Vorteile. Insgesamt kann eine Kombination von Flash und Non-Flash ratsam sein.«

Ines Wolf, Manager Presales CE bei **Quantum**, sieht Flash nicht unbedingt als den besten Weg: »Kann man machen: Hardware mit Hardware erschlagen. Sinnvoller wäre es allerdings, die Daten auf dem Primär-Storage zu klassifizieren, statische vs. nicht-statische Daten. Statische Daten müssen nicht in das

tägliche Backup fließen, von diesen Daten kann auf anderen Wegen eine Sicherheitskopie erstellt werden.« Unternehmen sollten die Relevanz ihrer Daten kennen. Quantum empfiehlt unter anderem die Definition von BU-Schedules nach Datengruppen.

Bekannte Backup-Strategien immer noch gültig

Bei vielen Verantwortlichen kommt die Frage auf, ob die bislang gängigen Backup-Strategien endgültig passé sind. Quantum-Managerin Wolf antwortet mit einem klaren »Nein«: »Diese Strategien sind nicht passé, aber die Anforderungen an die Umgebungen haben sich verändert bzw. erschwert. Hinzukommen eine zunehmende Virtualisierung in Verbindung mit einer sinkenden Zahl an physischen Systemen mit dem Ziel, den administrativen Aufwand zu reduzieren.« Auch rücke die Bewertung der Relevanz der einzelnen Datengruppen für den Geschäftsprozess in den Vordergrund, um die passende Strategie für die Datensicherheit zu implementieren.

Fujitsu-Manager Roth sieht es ähnlich: »Ganz im Gegenteil bietet die schon oft totgesagte Backup-Kopie auf Band eine einzigartige Versicherung gegenüber Ransomware-Angriffen. Was bisher funktionierte, muss keineswegs ungesehen auf den Müll, sondern kann in Kombination mit den neu-

Folgen Sie dem
speicherguide.de-
Team auf
Social-Media

speicherguide.de

Karl Fröhlich



Kerstin Mende-Stief



Wolfgang Stief



en Möglichkeiten durchaus auch weiterhin eine Rolle spielen.« Wichtig sei, externe Anforderungen und eigene Kapazitäten miteinander abzugleichen. Im Endeffekt gehe es darum, Lösungen einzusetzen, die viele unterschiedliche Backup/Recovery-Applikationen und Umgebungen vereinen, um dort die SLAs sicherstellen zu können.

Recovery größerer Datenmengen

»Aus der Recovery-Perspektive stellt eine Kombination aus Plattenspeicher und Tape die beste Option für die Wiederherstellung größerer Datenmengen dar«, erklärt Fujitsu-Manager Roth. »Eine reine Dedup-Plattenspeicherlösung mag Vorteile beim Wiederherstellen einzelner Dokumente haben, für die komplette Wiederherstellung großer Datenmengen hingegen bieten Tapes eindeutig die bessere Leistung.« Mit Fujitsus *ETERNUS CS8000* sei zum Beispiel True-Tape-Virtualisierung möglich. Dabei dienen Platten oder Flash als primärer Speicherplatz für sämtliche Backup-Daten, ohne dass durch Deduplizierung die Leistung gemindert werde. Je nach Vorgabe schreibt das System diese Daten im Hintergrund in einem Stream auf Tape. Für die Wiederherstellung werden die vorhandenen Daten aus dem Platten- bzw. Flash-Speicher gelesen bzw. läuft die Datenwiederherstellung parallel im Hintergrund.

»Aus Recovery-Aspekten besteht ein möglichst perfekter Mix, um größere Datenmengen wiederherzustellen, heute aus Backup-to-Disk-to-Tape (B2D2T)«, meint Hestermann. »Morgen aus B2F2D2T und dies immer zusammen mit einer intelligenten Backup- und Recovery-Software.«

Backup/Recovery: Markt & Entwicklung

Die Zukunft sieht die Branche durchgängig positiv. Es wird erwartet, dass in den kommenden Jahren in den Bereich Backup/Recovery und Data-Protection im Kontext der Digitalisierung deutlich mehr Investitionen fließen werden. Unternehmen bietet sich dabei ein breit gefächertes Spektrum welches von Tapes als Medienbruch über Appliances und die Integration in HCI-Lösungen reicht, aber auch Cloud-Connectivity einschließt, Backup von und zur Cloud sowie Datensicherung speziell »on the Edge«. Speziell bei letztgenannten soll ein extremes Wachstum stattfinden.

»Datensicherung wird oft nicht mehr nur alleine fürs Backup genutzt, sondern immer mehr zum Datenmanagement – auch in Richtung Langzeitspeicher und Archivierung, zum Beispiel für Data Analytics, KI-, Deep-Learning- und Machine-Learning-Anwendungen«, argumentiert Roth von Fujitsu. »Wichtig für den potenziellen Anwender

ist angesichts der vielen Möglichkeiten in jedem Fall, den individuellen Bedarf wie auch die eigenen Potenziale genau zu kennen und bei der Lösungssuche konsequent zu beachten.«

»Generell werden die Datenmengen weiter steigen – und zwar deutlich mehr, als man noch vor Jahren gedacht hat«, erwartet Heckel. »Da die Trennung von wichtigen und unwichtigen Daten faktisch nur vom Datenerzeuger – und nicht vom IT-Verantwortlichen – erfolgen könnte, werden in den meisten Fällen auch weiterhin alle Daten gesichert, die irgendwie anfallen. Man weiß ja nie, wozu man die Version »final-final-2.2a« noch irgendwann brauchen kann.«

Neue Technologien und Strategie-Ansätze, die sicherlich entwickelt werden, gehen laut Hestermann nicht zu Lasten von Magnetbändern: »Seitens Tape ist mit Stand heute keine Alternativ-Technologie zu sehen, die hinsichtlich der Kosten für Archivierung und Datensicherung mithalten kann. Dass Disk/Flash-basierende Speicher sich ergänzen und vielleicht ersetzen ist bereits erkennbar. Cloud-Lösungen für Backup werden an Daseinsberechtigung gewinnen, jedoch das klassische Backup nicht ersetzen. Warum? Witzig aber wahr: Kunden beginnen Daten ihrer Cloud-Applikationen aus der Cloud zusätzlich lokal zu sichern. Und auf was? Auf Tape.«



Storage-Forum 2019

28. + 29. November

Eventpalast Leipzig



Das Storage-Forum 2019 ist eine Plattform zum fachlichen Austausch für Nutzer und Anbieter von Enterprise-Storage-Systemen und -Lösungen.

In Keynotes, Anwenderberichten und Vorträgen sowie der Begleitausstellung informieren wir Sie über Technologien und Trends in den Bereichen Data Management, Data Storage, Archivierung, Backup u.v.a.m.

www.Storage-Forum.de

**PROGRAMM
&
REGISTRIERUNG**

Expertengespräch mit Stefan Utzinger, CEO, Novastor

Backup-Service: Von der Strategie bis zur Implementierung

Der Bereich Backup/Recovery unterliegt von jeher einem steten Wandel. Dieser beschleunigt sich aber gerade signifikant, mit der Etablierung von Cloud-Services, der Digitalisierung und der zunehmenden Bedeutung von Daten. Wir sprachen mit Novastor-CEO Stefan Utzinger über die sich verändernden Anforderungen an die Datensicherung, Managed-Services und die sich wandelnde Rolle eines Herstellers zum Lösungsanbieter.

Woran sollten Firmen aktuell arbeiten, wenn es um Datensicherung geht?

Utzinger: Daten bestimmen zunehmend die Geschäftsprozesse bzw. beeinflussen diese zumindest. Das Datenwachstum und die zunehmende Relevanz von Daten für Kerngeschäftsprozesse betreffen wirklich jedes Unternehmen.

Hinzukommt die Digitalisierung: Die bekommt man nicht »for free«, darum müssen sich IT-Leute aktiv kümmern, und die müssen meist aus anderen Bereichen abgezogen werden. Zusätzliche IT-Mitarbeiter zu finden ist in der Regel sehr, sehr schwierig und bedeutet auch zusätzliche Investitionen. Das heißt, es gibt eine generelle

Knappheit in den Firmen, diese Prozesse zu begleiten. Das hat Auswirkungen auf die Infrastruktur, wo auch Backup angesiedelt ist. Hier sehen wir den Trend, diesen Prozess an Spezialisten auszulagern und sich weniger selbst darum zu kümmern.

Viele Unternehmen stellen fest, die Daten wachsen schneller als geplant. Gleichzeitig wachsen die Infrastrukturen nicht in dem gleichen Maße mit. Nun gilt es diese Infrastrukturen neu zu überdenken – meist bei gleichbleibendem Budget und vermindernden Ressourcen.

Hinzukommt das Thema Ransomware: Hier setzt sich die Erkenntnis durch, dass diese Verschlüsselung eine echte Bedro-

hung ist. Aktuell haben wir hier in Hamburg mit *Juwelier Wempe* ein sehr prominentes Beispiel.

Unsere Gesprächspartner bemerken zunehmend, wenn es um Backup geht, dann wird kein Tool mehr gesucht, sondern eine Lösung. Das heißt, eine Lösung und auch eine Beratung, die ganzheitlicher ist. Das einzelne Feature reicht am Ende nicht, um den Herausforderungen gewachsen zu sein.

Haben die meisten denn eine Strategie?

Utzinger: Nein, das stellen wir ganz klar fest. Ein Backup-Konzept besteht ganz oft noch aus einer reinen Auflistung von IT-Systemen, ohne die geschäftsrelevanten Prozes-



Foto: speicherguide.de

Stefan Utzinger, CEO, Novastor:

»Die Vernetzung von Prozessen führt mit einer ganzheitlichen Betrachtung zu einer – wie wir es nennen – Datensicherung 4.0«

se und Prioritäten zu berücksichtigen. Damit ist keine Transparenz vorhanden. Das heißt, sehr oft kann die IT-Abteilung Fragen nach der Wiederherstellung einzelner Systeme oder dem Wiederanlauf nach einem Disaster nicht beantworten. Hier ist mittlerweile tatsächlich ein Sinneswandel da. Wir

haben mit einer Umfrage gerade festgestellt, dass fast 90 Prozent der Befragten geantwortet haben, »Ja, wir haben so etwas ähnliches wie ein Backup-Konzept, aber nein, wir wissen eigentlich nicht was unsere Backup-Software macht.«

Das heißt, Sie müssen hier als Hersteller mehr Unterstützung leisten? Wie sieht diese aus?

Utzing: Mit der Vernetzung von Geschäftsprozessen und der immer weiteren Digitalisierung von Geschäftsprozessen hat die Verfügbarkeit von Daten eine extrem kritische Bedeutung. In der Zeit von Industrie 4.0 bedeutet dies, ohne die relevanten Daten lassen sich Maschinen nicht betreiben und Geschäftsprozesse nicht aufrechterhalten. Da unsere Wirtschaft extrem vernetzt ist, betrifft dies nicht nur die eigene Firma, sondern die Produktion steht plötzlich auch in verbundenen Unternehmen still. Das heißt, Daten sind ein extrem sensibler Bestandteil der gesamten Produktions- und Wertschöpfungskette. Im Schadensfall geht es schnell um sehr große Summen. Deshalb greift hier plötzlich die Haftung der Geschäftsführung und das wird den Beteiligten mehr und mehr bewusst.

Neben den strategischen Komponenten haben wir konkrete Angebote zur Unterstützung. Beispielsweise kommen immer mehr

Kunden auf uns zu und interessieren sich für unseren Health-Check. Das heißt, wir schauen uns die Implementierung der Datensicherung an und führen testweise Restores durch. Dies ist extrem wichtig, da wir aus Erfahrung feststellen, dass im Tagesgeschäft nur wenige Restores auch wirklich ausprobiert werden. Wenn es hochkommt führen nur zehn Prozent der Unternehmen überhaupt einen Restore über alle Daten aus. 80 Prozent der Daten werden eigentlich nur gesichert, aber nie wiederhergestellt.

Ob die SAP-Datenbanken wirklich gesichert wird oder ob das Medium im Schadensfall funktioniert, das weiß oft keiner.

Diese Vernetzung von Prozessen, die Digitalisierung, diese ganzheitliche Betrachtung, das verstehen wir unter Datensicherung 4.0. Und genau hier darf sich der Hersteller nicht aus der Pflicht stellen, da darf man nicht nur einfach nur ein Tool verkaufen und den Kunden damit »glücklich« werden lassen.

Sie prägen den Begriff Datensicherung 4.0. Können Sie dies nochmal zusammenfassen?

Utzing: Die zunehmende Digitalisierung, Business-Intelligence oder Machine-Learning erzeugen wachsende Datenmengen und steigern die Relevanz der IT für sämtli-

che Unternehmensbereiche. Die IT muss zusätzlich Herausforderungen wie steigende gesetzlichen Anforderungen oder kurzfristige Veränderungen der IT-Infrastrukturen bewältigen.

Datensicherung 4.0 muss eine Gesamtlösung sein: wirtschaftlich, technisch, rechtlich, organisatorisch. Backup-Software allein wird in Zukunft den Anforderungen nicht gerecht werden.

Euer Konzept und Managed-Services-Angebot ist anders als marktüblich?

Utzing: Wir sind erstmal per sé kein Managed-Service-Provider (MSP) der in Konkurrenz zu einem Systemhaus steht. Wir sind Spezialisten für Datensicherung und unterstützten Kunden und Systemhäuser mit unserem spezifischen Know-how. Was wir für Partner und Kunden übernehmen, ist das Management unserer Backup-Lösung: Software, Service-Leistungen wie Implementierung oder Health-Checks und ein deutschsprachiger, technischer Support. Wir können im Prinzip für alles zuständig sein, vom Backup-Konzept bis hin zur Implementierung.

Das heißt, die Daten der Kunden werden nicht bei Novastor gespeichert?

Utzing: Die Daten verbleiben beim Kunden bzw. werden im RZ des Kunden oder der Systemhäuser gespeichert. Wir haben

auch kein eigenes Rechenzentrum, sondern sind »nur« ein Lösungsanbieter und Spezialisten für Datensicherung. Wir sagen auch ganz bewusst, der Kunde/das Systemhaus wählt das Rechenzentrum oder den Cloud-Speicherplatz aus, den er benötigt, wir supporten die Schnittstellen. Hier wollen wir uns ganz unabhängig aufstellen.

Die meisten Systemhäuser sehen beim Cloud-Backup, die Cloud als eine zweite Location, als eine Art Offsite-Backup des sowieso schon vorhandenen lokalen Backups. Fast 90 Prozent sichern mittlerweile tatsächlich in ein kleines RZ in ihren eigenen Geschäftsräumen. Wir reden hier von Systemhäusern mit mindestens 30 bis 40 Mitarbeitern, die verfügen über genügend Hardware und Know-how. Die Backups sind sowieso verschlüsselt und gerade mittelständischen Kunden ist es wichtiger, eine transparente und möglichst günstige Absicherung zu haben und hier nicht zu viel Geld investieren zu müssen. Bei Bedarf hat der Systemhauspartner die Daten bei sich vor Ort und kann sofort eingreifen und Maßnahmen einleiten. Hier muss man aber entsprechende Analysen machen, bevor eine Entscheidung gefällt wird. ■

Weitere Informationen

Lesen Sie eine ausführliche Fassung dieses Interviews auf speicherguide.de

Anwenderbericht: Kölner Hofbräu setzt auf Silent Bricks von FAST LTA

Datensichere Zukunft an zwei Bierbrauer-Standorten

»Wer zu Früh kommt, bleibt«, »Fließend Kölsch« und »Kein bisschen Alt«. Mit ihren Werbesprüchen für ihr FRÜH Kölsch provoziert die Traditionsbrauerei Kölner Hofbräu gerne – bei der Datensicherung werden aber keine Kompromisse gemacht. Mit Silent Bricks von FAST LTA sichert der Kölner Brauer Daten aus EASY ECM und Veeam Backup. Die Speicher stellen in einer SSD-, NAS- und WORM-Konfiguration eine Nettokapazität von 51 TByte zur Verfügung.

Hannes Heckel, FAST LTA

Wer an Köln denkt, dem fällt der Dom ein und dann gleich das Kölsch. Das obergärige helle, hopfenbetonte Bier gilt heute als regionale Spezialität und darf nur in Köln und der näheren Umgebung hergestellt und nur in der so genannten Stange serviert werden. Eine der traditionsreichsten Brauereien dafür ist **Kölner Hofbräu P. Josef Früh**. Das »FRÜH Kölsch« gehört mit einer Jahresproduktion von mehr als 400.000 Hektolitern zu den am meisten getrunkenen Kölsch. Gegründet 1904, ist das Stammhaus direkt am Kölner Dom zu finden. Dort wurde bis in die 1980er Jahre gebraut. Durch den steigenden Bedarf kam eine neue Braustätte in Köln-Feldkassel dazu. Diese beiden Standorte sind auch heute noch Dreh- und Angelpunkt für den Erfolg des Unternehmens.

Neben der Brauerei werden auch mehrere Kultkneipen und das »Eden Hotel Früh am Dom« mit dem dazugehörigen Restaurant »Hof 18« neben dem traditionellen Brau-

haus betrieben. Die Verwaltung war und ist stets auf Höhe der Zeit und so entschloss sich die IT-Abteilung bei der Umstellung des Dokumentenmanagement-Systems auch zur Anpassung der Datensicherungs- und Archivierungs-Infrastruktur. Gerade auch im Hinblick auf die seit 2018 geltenden DSGVO-Regeln. Zusammen mit **GID**, einem Systemhaus, mit dem man schon lange zusammenarbeitet, fand man **FAST LTA** und das Silent Brick System. Dies ist eine zukunftssichere Lösung, die modern, schnell und wachstumssicher mit den steigenden Datenmengen mithält.

Die IT-Umgebung der Brauerei und Gastronomie stützt sich auf zwei Rechenzentren. Sie ist zum Großteil virtualisiert und umfasst aktuell 14 TByte Datenvolumen am Standort Köln-Feldkassel und 8 TByte im Stammhaus am Dom. Effiziente Abläufe und moderne Abrechnungssysteme produzieren täglich eine große Menge an Daten. Für den zuverlässigen Betrieb und Ausbau sind IT-Leiter **Julian Kamp** und der Leiter Systemadmins, **Thomas Coßmann**, sowie weitere Kollegen zuständig.

DSGVO-konformer Archivspeicher musste revisions- und zukunftsicher sein

Um die Abläufe im Unternehmen immer digitaler abzubilden, entschloss man sich zur Umstellung des Dokumentenmanagement-Systems auf Easy DMS. Hier sollen Prozesse wie Rechnungsstellung, Belegerfassung, HR- und Verwaltungsdaten der Brauerei zusammengefasst werden. Dazu musste die Archiv-Lösung von der bisherigen Tape-basierten Lösung auf eine zukunftsfähige und revisionssichere Datenarchivierung umgestellt werden. »Unsere Haupt-Herausforderung war es, dass die Implementierung

Foto: Kölner Hofbräu



Kölner Hofbräu plant seine Backup- und Archivsysteme weiter auf das FAST LTA Silent Brick System umzurüsten.

und der Betrieb so einfach wie möglich erfolgen sollte. Zudem haben wir großen Wert auf eine sichere Langzeitarchivierung gelegt, die den DSGVO-Anforderungen genügen mussten«, sagt IT-Leiter Julian Kamp.

Die Primärspeicher sichert man nach klassischen Backup-Plänen. Belege und sonstige Daten mit Aufbewahrungsverpflichtung wurden auf ebenfalls Tape-basierte WORM-Lösungen gesichert. »Hier stießen wir bei unserer Planung für das

Herausforderung

Um die Abläufe im Unternehmen immer digitaler abzubilden, entschloss man sich zur Einführung des neuen Dokumentenmanagement-Systems Easy DMS. Hier sollen Prozesse wie Rechnungsstellung, Belegerfassung, HR- und Verwaltungsdaten der Brauerei zusammengefasst werden. Dabei musste die Archiv-Lösung von der bisherigen Tape-basierten Lösung auf eine zukunftsfähige und revisionssichere Datenarchivierung umgestellt werden. Außerdem sollte eine sichere Langzeitarchivierung möglich sein, die den DSGVO-Anforderungen entspricht. Bei der Umstellung sollte das gesamte Backup- und Archivierungssystem modernisiert werden.

neue DMS-System an Grenzen, die gerade in Zukunft unserem Wachstum im Weg gestanden hätten«, erläutert Thomas Coßmann, der als Leiter Systemadmins für die Datensicherung zuständig ist. Da man sich softwareseitig auf die Backup-Lösung von Veeam konzentrierte, untersuchte man zusammen mit dem Systemhaus **GID** in Köln, welche Sekundärspeicher optimal zur neuen IT-Infrastruktur passen. »Wir haben uns bei diesem wichtigen Projekt wieder für unseren Partner GID entschieden, da wir schon sehr vielen Jahren zusammenarbeiten«, blickt Kamp zurück.

Das Beste aus beiden Welten – HDD und Tape

Nach einer Analyse des Marktes, bei der vor allem WORM-Tape-Anbieter und Software-Lösungen betrachtet wurden, stellte sich das *Silent Brick*-System von FAST LTA als die optimalste Lösung heraus. »An sich verbindet FAST LTA mit den Silent Bricks das Beste aus beiden Welten – HDD und Tape – und war somit unsere erste Wahl für unsere zukünftige Datensicherung«, freuen sich Kamp und Coßmann. Im Vergleich zu anderen Systemen ist das Silent Brick System preislich attraktiv und flexibel skalierbar. Besonders das Prinzip der herausnehmbaren Bricks bietet ein hohes Maß an Sicherheit. »Durch die Mobilität der Bricks

können wir die Backups und Archive an unterschiedlichen Standorten nutzen und auch offline lagern. Zusammen mit dem attraktiven Lizenzmodell und den intelligenten Funktionen, macht das Silent Brick System das Handling der Systeme sehr einfach«, erläutert Coßmann.

Zügige Einführung und problemloser Betrieb

Da das neu eingeführte Easy DMS ab Januar 2019 produktiv eingesetzt werden sollte, musste die Einführung des neuen Backup- und Archivierungssystems zeitnah erfolgen. Gemeinsam mit den Experten von FAST LTA konzipierte man die Umgebung und entschied sich für Silent Bricks in SSD-, NAS- und WORM-Konfiguration. Insgesamt steht nun eine Nettokapazität von 51 TByte in mehreren Silent Brick Drives zur Verfügung. Auf den WORM-Bricks werden die revisionssicher aufzubewahrenden Dokumente wie Rechnungen und Verträge, sowie die geschäftlichen E-Mails DSGVO-konform archiviert. Die Backups erfolgen auf die SSD- und HDD-Bricks. Repliziert werden die Datensicherungen in den beiden RZs an den Haupt-Standorten am Dom und in Feldkassel.

Die Umstellung fand im Dezember 2018 statt und die finale Installation kurz vor Weihnachten. »Wir standen mit dem Projekt vor großen Herausforderungen. Dafür,



Foto: Fast LTA

Cölner Hofbräu setzt auf **Silent Bricks** in SSD- (3 TByte), NAS- (24 TByte) und WORM-Konfiguration (24 TByte) mit einer Nettokapazität von 51 TByte.

dass wir das bestens geschafft haben, möchten wir uns nochmals bei den Experten von Fast LTA bedanken«, lobt IT-Leiter Kamp. Die versprochenen Features funktionieren wie geplant und einwandfrei. Ältere Sicherungen, die noch auf dem Tape-System abliegen, werden nun sukzessive durch das Silent Brick System abgelöst. Durch die flexible Erweiterbarkeit können die IT-Verantwortlichen der Cölner Hofbräu P. Josef Früh KG dem kommenden Wachstum der Datenmengen gelassen entgegensehen. »Wir werden in den nächsten Jahren unsere Backup- und Archivsysteme weiter auf das FAST LTA Silent Brick System umrüsten und vorhandene Lösungen weiter ausbauen«, blickt Kamp in die Zukunft. ■

Weitere Informationen

FAST LTA AG

Rüdesheimer Str. 11, 80686 München

Tel. 089/89 047-0

E-Mail: info@fast-lta.de

www.fast-lta.de

Ein Lösungsansatz zur Effizienzsteigerung und Kostensenkung durch optimierte Nutzung von Speicherplattformen

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

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

Albrecht Hestermann,
actidata Storage Systems

Es versteht sich von selbst, dass jeder Administrator in die Luft geht, wenn die Marketing-Abteilung die 27. Vorversion des neuen Produktkataloges auf dem zentralen Fibre-Channel-Speichersystem ablegt. Letztlich muss jedoch den Mitarbeitern der Marketing-Abteilung zugutegehalten werden, dass diese in aller Regel ja gar nicht wissen, wo sie etwas abspeichern. Was zählt ist vielmehr, dass es morgen noch da ist – ein Dilemma, dem sich auch heute noch viele Administratoren ausgesetzt sehen, obwohl genau das der Ursprung der so genannten unstrukturierten Daten ist. Wurden nicht bereits im Vorfeld Maßnahmen ergrif-

fen, sind die 27 Versionen wohl auch noch in zehn Jahren auf dem zentralen Storage-System vorhanden. Genau hier setzt das Konzept des Nearline-Storage an, denn oftmals reicht für die sichere Speicherung von Benutzerdaten ein einfacher File-Service aus, der über einen Server oder ein NAS-System realisiert wird.

Nachts Backup und tagsüber aktive NAS-Nutzung

Die Ausnutzung der vollen Leistungsfähigkeit einer IT ist als Ziel zur Erreichung einer optimalen Systemeffizienz unumgänglich. Bekannterweise laufen die Datensicherungsaufträge in aller Regel in den Nachtstunden ab, da hier eben die geringste Belastung der Server und Infrastruktur besteht.

Backup-Server, sei es beim Datentransfer auf Disks oder bei der Sicherung auf Tapes, laufen in dieser Zeit mit der höchsten Last. Tagsüber dagegen ist die Auslastung eher gering. Genau hier können durch Änderungen im IT-Konzept freie Ressourcen für andere Services genutzt werden.

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

Datensicherung sehr performant direkt im Backup-Server abläuft und somit eine Belastung des LANs entfällt.

System der Einstiegsklasse vs. skalierbare Lösung

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

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

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

Datenauslagerung – ist das heute noch wichtig?

Ein klares Ja! Auch wenn die Auslagerung unternehmenskritischer Daten in die Wolke als verlockend zu bezeichnen ist, sprechen doch nach wie vor fehlende Bandbreiten und/oder offene Fragen rund um Datenverschlüsselung und RZ-Standorte dagegen. Oft wird vergessen, dass ein Download-Stream in aller Regel eine deutlich geringere Bitrate liefert – was besonders in der Datenrekonstruktion ein großes Manko darstellt. Deshalb vertrauen viele mittelständische Anwender nach wie vor auf Lösungen, die im direkten und damit schnellen Zugriff liegen. Das hier für ein schnelles Restore die letzte Disk-basierende Datensicherung online zur Verfügung stehen sollte, versteht sich von selbst. Aber was nützt ein Disk-basierendes Backup, wenn ein Verschlüsse-

lungstrojaner die Daten der NAS-Freigaben unwiederbringbar verschlüsselt hat oder gar ein Feuer- oder Wasserschaden die gesamte IT lahmlegte? Die Wichtigkeit unternehmenskritischer Daten sollte Vorständen und Geschäftsführern bekannt sein, die zur Sicherung des Fortbestandes eines Unternehmens die verantwortlichen Administratoren unterstützen müssen und die regelmäßige Auslagerung der Daten an einen sicheren Ort anweisen sollten.

Erweiterbarkeit von Nearline- & Backup-Storage ist wichtig

Heutige Systeme, beispielsweise der NAS- und Backup-Server *actiNAS WIN*, lassen sich

über die externe SAS-Schnittstelle mit professionellen JBODs (Just a Bunch of Disks) erweitern. Besonders wichtig ist hier, dass die Erweiterungseinheiten auch in das so genannte Enclosure-Management des Kopf-Systems eingebunden werden müssen. Hierdurch ist dann die Gehäuse-Überwachung und -Alarmierung sichergestellt.

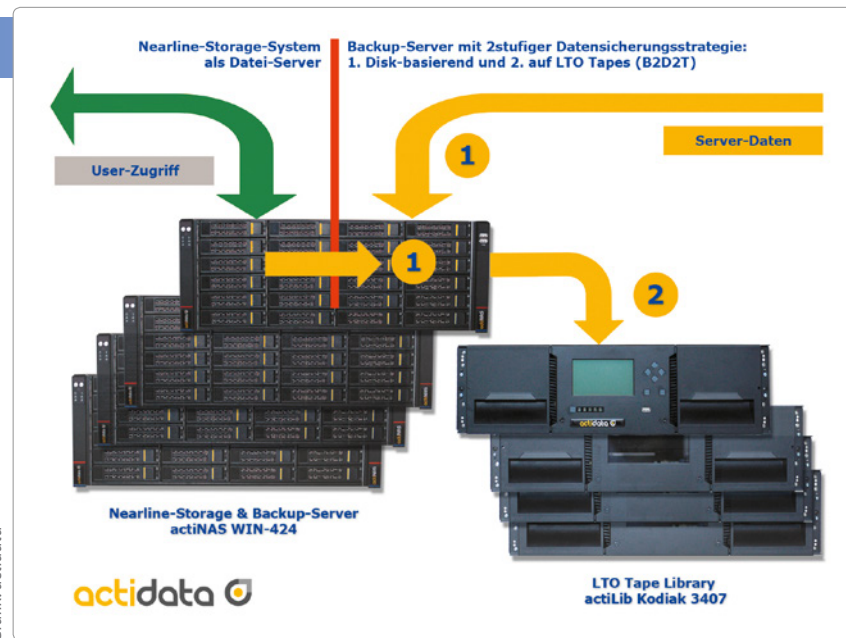
Gleiches gilt auch für die LTO-Tape-Library, wobei z.B. die *actLib Kodiak 3407* als 3U-Basis-Modul mit weiteren 3U-Erweiterungsmodulen individuell und je nach Bedarf skaliert werden kann. Skalierbarkeit schützt zum einen die Investitionen, denn Erweiterungen sind günstiger in der Anschaffung, als Neu-Systeme. Auch ab-

schreibungstechnisch spricht vieles für die Erweiterungsoptionen, denn Nearline-Storage- und Backup-Systeme werden in aller Regel auf fünf Jahre, im Gegensatz zu drei Jahren bei der zentralen IT, geplant.

Fazit – Versuch einer Empfehlung

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

Grafik: actidata



actidata »actiLib Kodiak 3407«: mehr als 8 PByte in 40 bis 280 Media-Slots.

Weitere Informationen

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

Backup-Gesamtlösung: technisch, wirtschaftlich, rechtlich und organisatorisch

Backup muss auch Datenmanagement-Anforderungen erfüllen

Eine moderne Datensicherungs-Lösung muss immer mehr können und leisten. Das automatisierte sichern und bedarfsgerechte wiederherstellen ist längst nicht mehr genug. Mussten früher verschiedene Netzwerkbetriebssysteme unterstützt werden, sind es nun diverse Hypervisoren, zuzüglich Cloud-Anwendungen und -Plattformen. Die Zukunft gehört Ansätzen, die technisch, wirtschaftlich, rechtlich und organisatorisch ein Gesamtlösung ergeben.

Karl Fröhlich

Die Data-Protection-Herausforderungen besteht für IT-Abteilungen vor allem in der schier Masse der Daten. Die überwiegende Mehrheit der in KMUs Verantwortlichen für Datenmanagement geht davon aus, dass das Datenvolumen in den nächsten fünf Jahren um das Zehnfache oder mehr zunehmen wird. 80 Prozent davon äußerten Besorgnis über das Risiko und die geschäftlichen Auswirkungen, die es auf ihr Unternehmen haben wird.

»Auch die Tatsache, dass Unternehmen sowohl On-Premise- als auch Off-Premise-Lösungen im Einsatz haben und nicht wissen, wo ihre Daten liegen macht es kom-

pliziert«, meint **Florian Malecki**, International Product Marketing Director bei **StorageCraft**. »Hinzukommt das Thema Compliance, beispielsweise die DSGVO oder branchenspezifische Anforderungen wie HIPAA (Health Insurance Portability and Accountability Act).« Es gehe darum zu verstehen, wer Zugang zu den Daten hat und welche Daten besonders wichtig sind und wie diese bereitgestellt werden müssen, um alle Richtlinien zu erfüllen.

»Datenschutz und Datensicherung sind komplexer geworden, weil es mehr Daten gibt, weil die Cyberkriminalität steigt und die Infrastrukturen mit Multi-Cloud und IoT komplexer werden«, ergänzt **Thomas Sandner**, Senior Regional Presales Mana-

ger CEMEA bei **Veeam**. »Umso wichtiger ist die Absicherung von Daten, also Backup/Recovery sowie Disaster-Recovery (DR), damit keine Daten verloren gehen, man nicht erpressbar ist und jederzeit die Verfügbarkeit wiederherstellen kann.«

Das Thema Cyber-Protection darf daher auch als einer der Trends in der Backup-Software-Branche gesehen werden. **Acronis** vermarktet beispielsweise seine »SAPAS«-Strategie nun über die gesamte Produktpalette. Das Akronym steht für Safety (Verlässlichkeit), Accessibility (Verfügbarkeit), Privacy (Vertraulichkeit), Authenticity (Authentizität) und Security (Sicherheit). Veeam bietet seinen Kunden einen optionalen Virencheck direkt bei der Wiederher-



Foto: speicherguide.de

Andreas Mayer
SEP

»Die Realisierung von, Industrie 4.0, KI und Big-Data spüren wir immer stärker und dies wirkt sich auf die Datenhaltung und auch die Datensicherheit maßgeblich aus.«

stellung. **arcserve** kooperiert mit Sicherheitsspezialisten **Sophos**.

»IT-Manager sollten Backup und IT-Sicherheit nicht mehr isoliert voneinander betrachte«, mahnt **Andreas Mayer**, Senior Marketing Managers bei **SEP**.

Data-Protection benötigt noch mehr Fokus

Obwohl Daten als das neue Gold gelten, berichten Branchenvertreter, dass viele Unternehmen die Datensicherung immer noch

zu geringerschätzen. Gängige Argumente sind Kosten für Zeit und Ressourcen. Geschäftsführer sehen die Datensicherung teilweise immer noch als totes Kapital. »Das ist erschütternd, weil Backup/Recovery und DR die Zukunftsversicherung einer Organisation und damit überlebenswichtig sind«, sagt Sander von Veeam. »Es wird noch viel zu viel manuell gemacht. Das kostet dann wirklich Zeit und Ressourcen. Dabei können Firmen mit moderner Backup-Software fast alles automatisieren, orchestrieren, testen und dokumentieren.«

Als schwierig bewerten Experten auch, dass viele Organisationen ihre Daten gar nicht genau kennen würden. Das heißt, wo entstehen diese, wer nutzt sie und wie sind sie abgesichert. »Was ich nicht kenne, kann ich nicht absichern«, stellt Veeam-Manager Sander klar.

Dass es oft genug an einer Strategie fehlt, bestätigte **Novastor-CEO Stefan Utzinger** im Interview gegenüber *speicherguide.de*: »Ein Backup-Konzept besteht ganz oft noch aus einer reinen Auflistung von IT-Systemen, ohne die geschäftsrelevanten Prozesse und Prioritäten zu berücksichtigen. Damit ist keine Transparenz vorhanden. Das heißt, sehr oft kann die IT-Abteilung Fragen nach der Wiederherstellung einzelner Systeme oder dem Wiederanlauf nach einem Disaster nicht beantworten.« Hier erwartet



Foto: speicherguide.de

Stefan Utzinger

Novastor

»Ein Backup-Konzept besteht ganz oft noch aus einer reinen Auflistung von IT-Systemen, ohne die geschäftsrelevanten Prozesse und Prioritäten zu berücksichtigen.«

Utzinger aber ein Umdenken, nicht zuletzt wegen der DSGVO werden IT-Manager immer häufiger nach der Datensicherheit gefragt. Dafür müssen sie letztendlich auch Verantwortung tragen.

Nicht in Silos denken

Wovon sich Unternehmen unbedingt trennen sollten, ist das Silo-Denken: »Oft versuchen Organisationen, bestehende Backup-Verfahren ›zu retten‹, weil sie ja noch funktionieren – so entstehen Silos«, mahnt

Veeam-Manager Sander. »Oder sie meinen, wenn sie einen Dienstleister beauftragen, also beispielsweise Software-as-a-Service einkaufen, dass dieser sich um die Absicherung der Daten kümmert, was ein Trugschluss ist.«

Die Datenspeicherung in separaten Silos führt in der Regel zu einer unzureichenden Verknüpfung untereinander. »Das bereitet mehr Probleme als man meint«, sagt Storagecraft-Manager Malecki. »Kleine und mittelständische Unternehmen kämpfen zudem damit, dass sie zu wenig Personal haben und dieses nicht immer über die erforderlichen Qualifikationen verfügt. So etwas kann leicht zu einer Herausforderung werden, wenn es um eine zuverlässige Verfügbarkeit der Daten geht. Helfen kann hier eine 360-Grad-Perspektive über alle Daten. Denn damit würden sich auch zuverlässige Prognosen erstellen lassen. Aber auch das ist für viele Unternehmen derzeit noch eher ein `Pain Point` als vorhandene Realität.«

Backup-Software wird zur zentralen Plattform

Die Antworten auf die Frage, was eine moderne Backup-Software auszeichnet, ähneln sich. Gleichzeitig setzen die einzelnen Hersteller natürlich unterschiedliche Schwerpunkte:

»Wer der Menge an verschiedenen Daten und Anwendungen Herr werden will, muss

die Sicherungen in zentrale Bahnen lenken«, rät **Sven Haubold**, Territory Account Director bei Arcserve. »Am effektivsten, aber auch am sichersten ist daher eine einzige Software-Lösung, die die Sicherung aller Anwendungen und IT-Umgebungen verarbeitet und verwaltet.«

Für Acronis ist Backup lediglich ein wichtiger Punkt einer Cyber-Protection-Strategie, welche Unternehmen verfolgen sollten: »Die Integration von Security-Workloads, erhöhte die Sicherheit beispielsweise gegen Ransomware-Angriffe mit automati-



Foto: Arcserve

Sven Haubold

Arcserve

»Neben dem Zwang zu mehr Flexibilität sehen wir auch die Tendenz zu Near-Zero-Toleranz bei Datenverlusten.«

sierter Rücksicherung«, sagt **Daniel Model**, Director Sales Engineering bei Acronis. »Zudem gilt es moderne Cloud-Services und deren Systeme (AWS, Azure) mit direkter Integration in die zentrale Backup-/Cyber-Protection-Plattform zu unterstützen. Außerdem sehen wir Disaster-Recovery-as-a-Service auf dem Vormarsch, wie auch die Sicherung mobiler Endgeräte.«

»Um Business-Continuity zu gewährleisten, ist es auch wichtig, dass neben granularen RPOs (Recovery-Point-Objectives) auf



Foto: Veeam

Thomas Sandner
Veeam

»Durch das enorme Datenwachstum aus immer mehr Quellen sind einer traditionellen, regelbasierten Datenverwaltung schnell Grenzen gesetzt.«

die RTOs (Recovery-Time-Objectives) zu achten ist, das heißt, dass im Disaster-Fall die Daten und Systeme schnell wiederhergestellt werden können«, argumentiert SEP-Manager Mayer. »Optimal ist es dabei, wenn die Backup-Lösung für die entsprechenden Applikationen und Systeme zertifiziert ist und die Backups nach den Vorgaben der diversen Hersteller erfolgt. So bleibt auch der originale Hersteller-Support erhalten. Hinzu kommt, dass eine zeitgemäße Backup-Software heterogene Systeme abdecken kann, physische und virtuelle Umgebungen – und nicht nur die Mainstream-Hypervisoren unterstützt. Hybrid-, Public- und Private-Cloud sowie auch Cloud-Applikationen wie *Office 365*, *GSuite* und *Salesforce* sollten supportet werden.« Gerade diese Cloud-Anwendungen gelte es zu unterstützen, da vom Anbieter nur die Verfügbarkeit angeboten werde – ohne Datensicherung.«

»Eine Backup-Software muss flexibel, einfach und zuverlässig sein«, beschreibt Veeams Sandner die wesentlichsten Anforderungen. »Flexibel, um unterschiedliche Betriebsplattformen, auch zukünftige, zu integrieren. Einfach und intuitiv zu bedienen, möglichst weitgehend automatisierbare Sicherungs- und Validierungsprozesse, enge Integration mit allen gängigen Plattformen – von On-Premises bis Public-Cloud – und Storage-Angeboten. Stichworte sind einmal



Foto: Storagecraft

Florian Malecki
Storagecraft

»Die Geschwindigkeit, in der eine Datenwiederherstellung zu erfolgen hat, wird immer wichtiger werden – egal ob physisch oder virtuell.«

mehr Automatisierung sowie Speichereffizienz und Datensicherheit.«

Backup als Gesamtlösung mit Datenmanagement

Novastor prägt den Begriff Datensicherung 4.0: »Unternehmen müssen es als Gesamtlösung betrachten: wirtschaftlich, technisch, rechtlich, organisatorisch«, fordert Utzinger. »Backup-Software allein wird in Zukunft den Anforderungen nicht gerecht werden, ganzheitliche Datensicherungslösungen müssen her und wir sehen hier die Hersteller in der

Pflicht, ihre Partner und Kunden hierbei zu unterstützen. Wir setzen hier mit dem *No-vastor DataCenter* an – als ganzheitliche Lösung zur Visualisierung und automatischen Dokumentation von Compliance-gerechten Datensicherungskonzepten.«

»Organisatorische Pläne, Maßnahmen und Strukturen sind zuerst zu schaffen, die die rechtlichen Anforderungen abdecken und die SLAs sind zu definieren, so dass entsprechende IT-Strukturen aufgebaut werden können«, rät SEP-Manager Mayer, wenn Firmen ihre Data-Protection-Umgebung auf den Prüfstand stellen. Die eingesetzte Backup/Recovery-Lösung soll diesen Bedarf mit entsprechenden RPOs und RTOs abdecken sowie die technische Sicherheit bieten. Das heißt, auch Funktionalitäten zur Umsetzung der Compliance-Anforderungen zur Verfügung stellt.

»Im Vordergrund stehen Automatisierung und Orchestrierung, von Backup über Recovery-Self-Services bis hin zu Failover- und Failback-Mechanismen bei ungeplanten Ausfällen«, sagt Veeams Sander. »Dafür muss ein Unternehmen aber seine Daten und sein Geschäft kennen, also, die Datenquellen, geschäftskritische Prozesse, Zugriffsrechte und Absicherungsmechanismen.« Ziel müsse ein integriertes Datenmanagement sein, damit digitale Prozesse umfassend unterstützt werden können. ■

Markt im Wandel: Forrester bewertet Backup-Anbieter neu

Backup und Daten-Resilienz

Die traditionellen Begriffe Backup und Recovery scheinen nicht mehr auszureichen, um Datensicherheit zu beschreiben. Darin scheinen sich die Analysten von IDC und Forrester Research einig. »Data Resiliency« ist der Begriff, der die neuen Anforderungen rund um die Sicherung von Daten in der Ära der digitalen Transformation beschreiben soll. Wir wagen einen Blick hinter die Kulissen.

Karl Fröhlich

Ähnlich wie **IDC** sieht **Forrester Research** die Anforderungen durch die Folgen der digitalen Transformation nicht mehr durch die Begriffe Backup und Recovery abgedeckt, und stützt sich neuerdings auf den Begriff der Daten-Resilienz. Forrester betont die Notwendigkeit Policy-basierter Speicherprozesse, die Fähigkeit, Daten effektiv wiederherzustellen und vor allem die Sicherheitsaspekte moderner heterogener Infrastrukturen, die neue, übergreifende Lösungen verlangen.

Im Zuge dessen bewertet Forrester Backup-Anbieter neu. In dem traditionellen, nicht immer progressiven Markt könnte dies einigen Anbietern gar nicht gefallen. Plötzlich erscheinen im Legacy-Markt neue Player. Ein Markt im Wandel, wie es scheint.

Forrester hat nach 2017 erneut die zehn wichtigsten Backup- und Recovery-Anbieter bewertet: **Commvault** baut seine Führungsposition demnach aus, aktuelle Verfolger sind das Startup **Rubrik**, **Cohesity** und **Veeam**. Etablierte Anbieter schneiden schlechter ab als noch zwei Jahre zuvor, besonders **Dell EMC** verliert aus Sicht der Analysten an Boden. Das besagt der aktuelle *The Forrester Wave: Data Resiliency Solutions, Q3 2019*-Report. Er vergleicht die Marktführer bei Backup und Recovery in Bezug auf Produktangebot und Marktstrategie bzw. -präsenz, und konstatiert beachtliche Veränderungen im Markt.

Forrester orientiert sich in der Wave-Darstellung offensichtlich am *Magic Quadrant* von **Gartner** und etabliert für seine Version vier Kategorien: marktführende »Leader«, gut positionierte »strong Performer«, markt-

relevante Wettbewerber als »Contender« sowie »Challenger« als Herausforderer. Bewertet werden die Anbieter nach gegenwärtigem Produktportfolio und ihrer Marktstrategie bzw. -präsenz. Laut Forrester wurden 40 Kriterien für die Bewertung analysiert.

Newcomer im Aufwind

Nach Forrester und Stand im dritten Quartal 2019 bleibt Commvault der Top-Leader, und konnte seine Position im Vergleich zu zwei Jahren zuvor sogar stärken. Verfolger sind in dieser Reihenfolge und beide neu in der Kategorie Leader Rubrik und Cohesity. Das Startup Rubrik wird bei der Marktstrategie sogar am besten bewertet. An vierter Stelle als Leader folgt Veeam. Dem Hersteller wird zwar das zweitbeste Produktangebot zuerkannt, die Marktstrategie fällt aber in der Gesamtbeurteilung ab.

Performer nach Forrester sind **Veritas**, **Druva** und **Actifio**. Zur Gruppe der Contender gehören **IBM** und **Micro Focus**, Dell EMC bildet das Schlusslicht als einziger Challenger unter den analysierten Top-10-Anbietern. Allerdings räumt Forrester selbst ein, dass Dell EMC die Teilnahme am vollständigen Evaluierungsprozess abgelehnt habe.

Etablierte verfehlen Anforderungsprofile

Im Vergleich zu 2017 ist signifikant, dass sich mit Rubrik, Cohesity und Druva drei Neulinge in starker Position in den Top 10 etabliert haben, die vor zwei Jahren noch gar nicht erfasst wurden. Neben diesen haben sich lediglich Veeam und der Top-Leader Commvault verbessert.

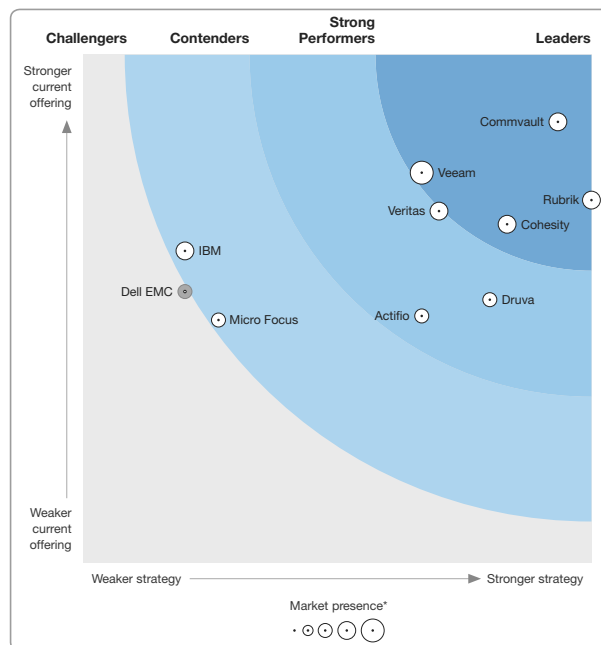
Zum Teil deutlich herabgestuft wurden dagegen Veritas, Actifio, IBM, HPE/Micro Focus und Dell EMC. Forrester kommentiert die Abwertung einiger etablierter Hersteller damit, dass aktuelle Anforderungen der Anwender nicht ausreichend abgebildet würden. Dies seien eine zentrale Verwaltung aller Datenquellen, ein umfassendes Policy-Management, leistungsfähige Wiederherstellungsmechanismen und Security-Aspekte.

Ranking in Deutschland sicher anders

Für Deutschland ist die Forrester-Wave allerdings nur bedingt aussagefähig. Commvault ist, vor allem über das Partnergeschäft, natürlich auch bei uns vorne mit dabei. Veritas ist traditionell bei vielen KMUs gesetzt, wie auch Dell EMC mit seinem *Networker*. Der Aufsteiger der letzten Jahre lautet aber sicher Veeam. Cohesity und Rubrik haben bei uns eher noch einen Newcomer-Status. **Acronis** sollte in Deutschland sicher genannt werden, wie auch die in Holzkirchen ansässige Software-Schmiede **SEP** sowie **Novastor** aus Hamburg.

Zerto-/IDC-Studie: Chefetagen verschlafen das Thema IT-Resilienz

Einen etwas anderen Ansatz verfolgt IDC, aktuell im Auftrag des israelischen Recovery-Spezialisten **Zerto**. Hier geht es um die Anwender und ihre Motivationen, nicht primär um Anbieter. Die IDC-Studie besagt, dass die obersten Management-Ebenen in Unternehmen haben nach wie vor Nachholbedarf, wenn es vor dem Hintergrund der digitalen Transformation um die Einschätzung der Widerstandsfähigkeit ihrer IT-Infrastruktur geht. 80 Prozent der Führungskräfte geben an, dass die obersten Unternehmens-



Forrester vergleicht in seiner Data-Resiliency-Solutions-Studie im Q3/2019 die Marktführer bei Backup und Recovery in Bezug auf Produktangebot, Marktstrategie und -präsenz.

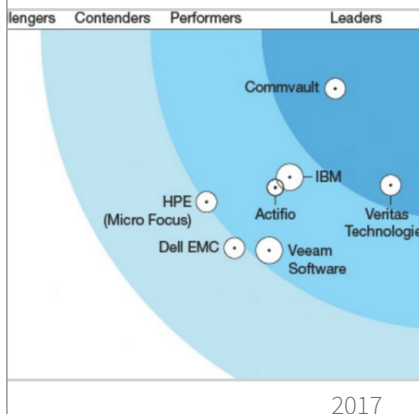
lenker den Zusammenhang für den Geschäftserfolg nicht ausreichend würdigen. Das besagt die von Zerto jährlich bei IDC in Auftrag gegebene Studie zur »IT-Resilienz«.

Dafür haben die Marktforscher von IDC 500 Führungskräfte aus der IT und anderen Geschäftsbereichen befragt und nun den *State of IT-Resilience Report 2019* vorgelegt. Allgemein herrscht Einigkeit darüber, dass eine stabile IT-Infrastruktur entscheidend für eine erfolgreiche digitale Transformation ist. Nur in den obersten Manage-

ment-Ebenen scheint diese Erkenntnis noch nicht angekommen zu sein.

IDC, nimmermüde in der Etablierung neuer Schlagworte, definiert IT-Resilienz als »Fähigkeit eines Unternehmens, Daten im Falle einer ungeplanten oder geplanten Störung zu schützen und gleichzeitig datenorientierte Initiativen zur Modernisierung des Geschäfts und zur digitalen Transformation zu unterstützen.« 82 Prozent der Befragten stimmen dem insofern zu, als sie dem Schutz und der Wiederherstellung von Daten für ihre Projekte zur digitalen Trans-

Grafik: Forrester



formation eine entscheidende Rolle zusprechen. Allerdings halten nur elf von Hundert und damit vier Prozent mehr als im Vorjahr dies für gewährleistet. 91 Prozent der Befragten gab an, dass ihr Unternehmen in den letzten beiden Jahren technologiebedingte Störungen erlitten haben. Rund 37 Prozent berichteten von unmittelbaren Umsatzeinbußen, 61 Prozent von Rufschädigung und 26 Prozent von einem dauerhaften Kundenverlust.

Chef, ich brauch' mehr Geld...

Immerhin gehen aber 90 Prozent davon aus, dass ihr Unternehmen in den nächsten zwei Jahren in die Absicherung ihrer Systeme investieren will. Ein wichtiger Baustein dieser Investitionen scheint die Zusammenführung von bisherigen Technologien zu sein. Ein hoher Prozentsatz der Befragten (93 Prozent) strebt zukünftig aktiv die Konvergenz von Lösungen für Backup und Disaster-Recovery an, um Redundanzen zu vermeiden.

Für Unternehmen bleibt demnach noch einiges zu tun. Das betrifft offenbar interne Aufklärungsarbeit für die obersten Chefetagen. 80 Prozent der Befragten geben an, dass das höhere Management ihres Unternehmens nicht von einem engen Zusammenhang zwischen der Verfügbarkeit von Daten sowie der erfolgreichen Umsetzungen von

Initiativen zur Digitalen Transformation und dem Unternehmenserfolg ausgehe.

Zudem halten 56 Prozent der Befragten an, dass die Ereignisse, die zu einem nicht wiederherstellbaren Datenverlust führten, meist vermeidbar waren. Das heißt, die Ereignisse traten beispielsweise zwischen Backups oder bei Ausfällen von Backup-/Wiederherstellungssystemen auf.

IDC sieht Transformationsprojekte gefährdet

Phil Goodwin, Research Director bei IDC, kommentiert: »Diese Umfrageergebnisse zeigen, dass die meisten Befragten ihre IT-Resilienz-Strategie nicht optimiert haben, was die zahlreichen IT- und geschäftsbezogenen Störungen zeigen. Die Mehrheit der befragten Unternehmen wird jedoch innerhalb der nächsten zwei Jahre ein Transformations-, Cloud- oder Modernisierungsprojekt durchführen. Hieran wird deutlich, dass alle Unternehmen einen Plan für die IT-Resilienz entwickeln müssen, um den Erfolg dieser Initiativen sicherzustellen. Ohne einen solchen Plan wird die Häufigkeit der beschriebenen Störungen, ungeplanten Ausfallzeiten und Datenverlusten weiterhin dazu führen, dass Cloud- und Transformationsinitiativen durch Verzögerungen oder Ausfällen gefährdet werden – was zu finanziellen Belastungen führt und sich negativ

auf den Wettbewerbsvorteil von Unternehmen auswirkt.«

Erkenntnisse der Befragung in der Übersicht:

- 91 Prozent gaben an, dass ihre Unternehmen in den letzten zwei Jahren technologiebedingte Störungen erlitten hätten.
- 56 Prozent der Befragten meinten, dass die Ereignisse, die zu einem nicht wiederherstellbaren Datenverlust führten, meist vermeidbar gewesen wären.
- 82 Prozent gaben an, dass der Schutz und die Wiederherstellung von Daten für ihre Projekte zur digitalen Transformation eine entscheidende Rolle spielten.
- 80 Prozent der Befragten glauben, dass das höhere Management ihres Unternehmens nicht von einem engen Zusammenhang zwischen der Verfügbarkeit von Daten sowie der erfolgreichen Umsetzungen von Initiativen zur digitalen Transformation und dem Unternehmenserfolg ausgehe.
- Nur rund 11 Prozent der Befragten gaben an, dass die Systeme ihres Unternehmens eine sehr ausgereifte IT-Resilienz auszeichneten.
- 90 Prozent der befragten Teilnehmer meinten, ihre Investitionen in die IT-Resilienz in den nächsten zwei Jahren erhöhen zu wollen.

- Rund 57 Prozent der Befragten glauben, dass die Anforderungen zum Datenschutz noch komplexer werden.
- Zirka 93 Prozent der Befragten werden mit hoher Wahrscheinlichkeit die Konvergenz von Backup- und Disaster-Recovery-Tools anstreben, um Redundanzen zu vermeiden.

»Die Resilienz der IT in Unternehmen wird ständig herausgefordert«, meint **Avi Rachiel**, CIO bei Zerto. »Bösartige Angriffe und Ausfälle verursachen Störungen von enormen Ausmaßen. Offensichtlich hapert es bei vielen Unternehmen an der Vermeidung von IT-Betriebsstörungen, wodurch die Unternehmen sogar davon abgehalten werden, sich auf die Entwicklung von Innovationen zu konzentrieren. IT-Führungskräfte und -Mitarbeiter sind sich über die Dringlichkeit von besserer Resilienz im Klaren, und alle Seiten profitieren von der dynamischen Entwicklung in puncto IT-Resilienz.«

Data-Resiliency etabliert sich als Schlagwort

Ähnlich wie IDC sieht Forrester die Anforderungen durch die Folgen der digitalen Transformation nicht mehr durch die Begriffe Backup und Recovery abgedeckt, und stützt sich ebenso wie IDC auf den Begriff der Daten-Resilienz. Forrester betont die Notwendigkeit Policy-basierter Speicher-

prozesse, die Fähigkeit, Daten effektiv wiederherzustellen und vor allem die Sicherheitsaspekte moderner heterogener Infrastrukturen, die neue, übergreifende Lösungen verlange. Vom Anforderungsprofil her ist dies bestimmt richtig, aber für uns sind hierzulande Begriffe wie Data-Resiliency nicht wirklich schön auszusprechen und auch nicht selbsterklärend. Dies gilt aus unserer Sicht auch für den Cyber-Protection-Ansatz von Acronis, der das Beste aus Data-Protection und Cyber-Security kombinieren soll. Wir halten es nicht für zu gewagt, wenn wir behaupten, dass IT-Abteilungen nach wie vor nach einer Backup-/Recovery-Lösung suchen, eventuell auch nach Data-Protection, aber nicht nach den neumodischen Wortkreationen.

Unstrittig dürfte aber sein, dass die Anforderungen an die Datensicherung nicht kleiner geworden sind. Die Digitalisierung und Parallelisierung aller Geschäftsprozesse sind der eher technische Aspekt, politische und wirtschaftliche Dynamiken sind ein weiterer. Und nicht zuletzt ist die zunehmend professionalisierte Cyber-Kriminalität ein Grund, sich dem oft vernachlässigten Thema anzunehmen, nennen wir es Backup und Recovery, oder neu Data-Resiliency. Wir sind gespannt, ob die Branche tatsächlich den Begriff der IT-Resilienz benötigt. ■

Nur eine Generation abwärtskompatibel

LTO-8: Doppelte Kapazität und etwas mehr Speed

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

Karl Fröhlich

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

LTO-8 unterstützt weiterhin eine Hardware-Verschlüsselung (AES-256-Bit), Datenpartitionierung sowie WORM-Funktionen

(Write-Once Read-Many). Auch LTFS (Linear Tape Filesystem) ist möglich, damit lassen sich die Tapes wie ein Block-Device ansprechen.

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

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

Ein interessanter Aspekt, der für LTO-8 spricht: LTO-8-Bandlaufwerke können neun

Nach einem Patentstreit zwischen Fujifilm und Sony kam die Auslieferung von LTO-8-Bändern fast komplett zum Erliegen, seit Sommer 2019 wird wieder produziert.

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

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



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

Einfache aber effektive Backup-Strategie

Unersetzlich: Die 3-2-1-Backup-Regel

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

Karl Fröhlich

Egal für welche Backup-Strategie man sich entscheidet, die 3-2-1-Backup-Regel gilt als kleinster gemeinsamer Nenner, den es zu erfüllen gilt. Das heißt, drei Kopien der Daten, gespeichert auf zwei unterschiedlichen Speichermedien (Medienbruch) und mindestens einer Offsite-Kopie. Im Detail kommt es natürlich auf die Art und Menge der Daten an und welche Technologien vorwiegend zum Einsatz kommen.

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

chermedien jeglicher Art wie Festplatten, Disk-Arrays, SSDs, Speicherkarten, aber auch der interne Speicher von Smartphones und Tablets, sind als mechanische und/oder elektronische Bauteile nicht für einen Ausfall gefeit. Ohne Kopie sind die Daten unweigerlich verloren. Datenrettungsdienste erreichen heutzutage durch-

aus kleine Wunder, verlassen kann man sich darauf aber nicht. Zudem ist Datenrettung ein mitunter kostspieliger Service. Je nach Art und Beschädigungsgrad des Mediums beginnen die zu kalkulierenden Einstiegs-kosten im vierstelligen Bereich. Zudem müssen Betroffene Zeit mitbringen. Die Wiederherstellungszeit bemisst sich in der

Regel in Wochen... Für eine größtmögliche Sicherheit sollten für die Datenkopien zwei unterschiedliche Speichertechnologien genutzt werden. Man spricht hier vom sogenannten Medienbruch. Dies soll die Ausfall-wahrscheinlichkeit verringern und für eine Risikoverteilung bei systembedingten Fehlern sorgen und vor Ransomware-Attacken schützen. Jede Internet-Anbindung ist ein potentes Einfallstor für Cyberangriffe.

Daher sollte sich eine ausgelagerte Kopie zudem an einem anderen geographischen Standort befinden. Alle vorangegangenen Bemühungen bringen nichts, wenn Originaldaten und Backups am gleichen Ort beispielsweise einem Brand oder Wasserschaden zum Opfer fallen. Auch ein Diebstahl lässt sich nie ganz ausschließen. In der Praxis kann es sich um Offline-Medien wie Tapes, RDX-Wechselkassetten, Speichersysteme mit Offline-Fähigkeit oder Cloud-Storage, aber auch einem Managed-Service handeln.

Speziell als Rückversicherung gegen Verschlüsselungsattacken erhält die 3-2-1-Backup-Regel neue Aktualität. Der Vorteil dieses Ansatzes, er ist relativ leicht umzusetzen. Zu bedenken ist aber auch, wie schnell die Daten im Schadensfall wieder zur Verfügung stehen sollen. Für zusätzlichen Schutz sorgen Abwandlungen in eine 3-1-2-, 3-2-2- oder 3-2-3-Strategie. ■



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

storage-magazin.de

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

Chefredaktion, Konzept:

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

Redaktion:

Karl Fröhlich, Wolfgang Stief

Schlussredaktion:

Brigitte Scholz

Layout/Grafik:

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

Titelbild:

iStockphoto.com / PeopleImages

Mediaberatung:

Kerstin Mende-Stief
Tel.: +49 8683 / 890 3285
E-Mail: media@speicherguide.de

Webkonzeption und Technik:

Günther Schmidlehner
E-Mail: webmaster@speicherguide.de

Urheberrecht:

Alle in »storage-magazin.de« erschienenen
Beiträge sind urheberrechtlich geschützt. Alle

Rechte (Übersetzung, Zweitverwertung)
vorbehalten. Reproduktion, gleich welcher
Art, sowie elektronische Auswertungen nur
mit schriftlicher Genehmigung der Redaktion.
Aus der Veröffentlichung kann nicht geschlos-
sen werden, dass die verwendeten Bezeich-
nungen frei von gewerblichen Schutzrechten
sind.

Haftung:

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

speicherguide.de
Das Storage-Magazin



Unser Team



Karl Fröhlich,
Chefredakteur
speicherguide.de



Jens Leischner,
Redaktion & Beratung
speicherguide.de



Wolfgang Stief,
Redaktion & Beratung
speicherguide.de



Kerstin Mende-Stief,
Mediaberatung
speicherguide.de