storage-magazin.de

Ausgabe **2-2020**

Eine Publikation von **speicherguide.de**

Grafik: Adobe Stock / Sikov

Backup & Recovery

Marktüberblick Backup-Software

Backup-Software: Abrechnungsmodelle oft sehr kreativ

Liebe Leserinnen und Leser,

Karl Fröhlich, Chefredakteur speicherguide.de

Backup & Recovery gehören zu den Themen, über die sich vortrefflich diskutieren lässt. Ich will nicht sagen streiten, aber Sie kennen es vielleicht, dass Kollegen, interne wie externe, durchaus anderer Meinung sind. Unter den ITlern gilt zwar der Spruch, »Kein Backup, kein Mitleid«, aber das war es Großteils auch schon mit den Gemeinsamkeiten. Dies liegt natürlich an den unterschiedlichen Erfahrungen der einzelnen sowie den zu betreuenden Umgebungen.

Einer neuen Hardware stehen viele aufgeschlossen gegenüber, bei der Software sieht es schon ganz anders aus. Schneller, mehr Leistung und höhere Kapazitäten gehen immer, sich in der Bedienung von etwas umzustellen schon weniger. Hier müssen sich die Software-Anbieter anstrengen, um überhaupt Gehör zu finden. Wobei es schon auch genug »Angriffspunkte« gibt.

Über die Jahre und diverse Entwicklungsstufen später wurde schon manch eigentlich überschaubares Produkt zu einem überfrachteten Ungetüm. Ein modularer Aufbau hat Vorteile, werden aber viele Module genutzt, wird es unübersichtlich. Und bei »unübersichtlich« und »kompliziert« sind wir auch schon bei den Kosten und Lizenzmodellen.

Vor allem bei der Verschleierung der Kosten sind einige Hersteller sehr kreativ. Abgerechnet wird beispielsweise nach Anzahl der zu sichernden Hosts, VMs, der installierten CPUs oder Kerne, nach der zu sichernden Kapazität und/oder der genutzten Module. Die Möglichkeiten sind extrem vielfältig. Hinzukommt, dass man sich kein Software-Paket mehr kauft, sondern diese nur noch über ein Lizenzmodell mietet oder abonniert.

Wenn ich ehrlich bin, gehöre ich schon noch zu denjenigen, die lieber eine Box im Regal bevorzugen. Da habe ich etwas in der Hand, dort finde ich den Lizenzschlüssel und früher haben die Programme auch ohne Internet funktioniert.

Ich sehe natürlich auch die Vorteile, wenn mir plötzlich Funktionen zur Verfügung stehen, die ich sonst erst mit dem nächsten (kostenpflichtigen) Upgrade erhalten hätte. Die Tools sind immer auf dem neuesten Stand und ich muss eben keinen Datenträger suchen, sondern installiere »einfach« aus dem Browser heraus.

Wie ist das bei Ihnen, sind Sie mit den angebotenen Lizenzmodellen zufrieden? Wenn Sie in Bezug auf Backup-Software zwei Wünsche hätten, welche wären das?

Ich bin sehr gespannt, wie unterschiedlich diese ausfallen werden.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Inhalt

Backup/Recovery: Realität oft weit vom Idealfall entfernt

Problemfall Endgeräte und Cloud-Anwendungen

Backup-Administratoren sind auf der Jagd nach den Endgeräten. Mobiles Arbeiten ist zwar nicht neu, wurde aber in der Corona-Zeit mit der Flucht ins Home-Office zusätzlich befeuert. Die Daten wurden zuletzt noch schneller mobil, sei es auf diversen Geräten oder Cloud-Anwendungen und entziehen sich dadurch oft genug dem geplanten Backup. Die ideale IT-Welt sieht einen zentralen Storage vor, die Praxis setzt dagegen meist auf eine Vielzahl an möglichen Speicherplätzen.

Karl Fröhlich

Auch die Bereiche Backup und Data-Protection bleiben nicht vom Corona-Virus verschont. Vor allem die geradezu fluchtartige Umstellung auf das Arbeiten im Home-Office stellt IT-Abteilungen vor eine Herausforderung. Wer seine Anwender mit einem virtuellen Desktop (VDI) bedient, ist klar im Vorteil. Die Infrastruktur und Prozesse sind definiert und lenken die Nutzer in vorgegebene Bahnen, egal ob dabei ein PC, ein Notebook oder Tablet zum Einsatz kommt.

Oft genug sind allerdings Endgeräte draußen bei den Nutzern ungesichert. »Gefühlt beobachte ich dies bei zirka 75 Prozent«, erklärt IT-Experte **Carsten Haak** im *speicherguide.de*-Talk. »In einer idealen IT-Welt hätte der User keine Möglichkeit, etwas an seinem Endgerät und am Speicherort zu verändern. Die Realität ist aber durchaus eine andere. Speziell in der Corona-Zeit wurden schnell Notebooks gekauft, mit einer vorinstallierten Windows-Version, die auch nicht entscheidend verändert wurde.« Dadurch haben die Nutzer die Freiheit, Daten lokal zu speichern. Dies führe dazu, dass eventuell nicht alle Verzeichnisse erfasst werden, selbst wenn ein mobiles Notebook gesichert wird.

Anwender halten sich nicht an Regeln

Die IT-Abteilungen stehen daher vor der Schwierigkeit, den sogenannten Endpoint wieder »einzufangen«. »Es ist nahezu unmöglich die Nutzer dazu zu bewegen, Regeln zu folgen, die das Rechenzentrum vorgibt«, meint Haak. Die Anwender seien hier durchaus sehr kreativ, Vorgaben zu umgehen.

Auch die klare Anweisung, wer die definierten Speicherplätze nicht benutzt, wird nicht mitgesichert und sei im Zweifel selbst schuld, funktioniert nur bis zu einem gewissen Grad bzw. Führungsebene. Moniert beispielsweise ein Abteilungs- oder Niederlassungsleiter das Fehlen von lokal gespeicherten Vertriebsdokumenten, wird sich die IT-Abteilung mit der Wiederherstellung befassen müssen, unabhängig von den dokumentierten Prozessen. Oft genug erkennen die Kollegen aber auch die Struktur nicht.

speicherguide.de-Talk #06:

Backup & Data-Protection,
hier geht's zur Aufzeichnung »

Otto-Normal-Anwender klickt auf »Speichern« und macht sich keine Gedanken, ob seine Datei auf der lokalen Festplatte landet oder auf einem zentralen Netzwerkspeicher.

Problemfall Office 365 und mobile Endgeräte

Auch die Cloud ist für viele Anwender keine Hilfe, speziell in *Office 365*-Umgebungen. Die werden zwar automatisch in der Microsoft-Cloud gespeichert, aber eben nicht gesichert. »Wenn jemand die Dateien löscht, sind sie weg – die meisten Anwender wissen dies nicht«, mahnt Haak. »Zu bedenken ist auch, dass es sich bei Endpoints nicht nur um Notebooks handelt, sondern auch auf Smartphones oder Tablets lassen sich Daten vervielfältigen und bearbeiten.« Deshalb müssen diese ebenfalls in der Backup-Strategie Berücksichtigung finden. ■

Hybride Backups schließen alle Arten von Daten mit ein, interne wie externe

Backup in Zeiten von Home-Office

Die Datensicherung darf auch im Home-Office nicht außer Acht gelassen werden. Systemausfälle, Benutzerfehler, aber auch Hackerangriffe und Ransomware bedrohen Unternehmensdaten, die remote erstellt werden. Backup-Spezialist SEP empfiehlt auch Strategien zu etablieren, die auch extern erzeugte Daten miteinschließt.

Klaus Riehm, SEP

Flexible Arbeitszeiten und -orte haben sich in den vergangenen Jahren zunehmend etabliert. Doch durch die Corona-Krise hat sich dieser Trend zu einer Notwendigkeit entwickelt. Viele Unternehmen schicken ihre Mitarbeiter zum Schutz vor einer Ansteckung – und sofern es möglich ist – ins Home-Office. Laut **Bitkom**-Umfrage von Mitte März, ist jeder zweite Berufstätige in Deutschland (49 Prozent) ganz oder temporär im Home-Office. Teilweise wurden extra Laptops angeschafft, um Heimarbeit zu ermöglichen.

Was bei der hektischen Einführung meist vergessen wird, ist das Einbinden der Remote-Arbeitsplätze in die Backup-Strategie. Denn wenn nun Daten außerhalb des Unternehmensnetzwerkes erzeugt werden, sind diese der Gefahr ausgesetzt, bei einem Systemausfall verloren zu gehen. Aber nicht nur Systemausfall, sondern auch vermehrte Hackerangriffe und Ransomware stellen eine Gefahr für die Unternehmensdaten dar.

Zuhause Firmendaten schützen und sichern

Gerade daheim in der privaten Umgebung ist das Risiko für einen IT-Ausfall und damit Datenverlust größer. Im Gegensatz zur Umgebung im Büro ist die Infrastruktur im Regelfall nicht auf den professionellen Einsatz ausgerichtet. Kaum vorhandene oder nur marginale Firewall-Funktionen des heimischen Routers sind ein Einfalltor für Bedrohungen. Daher müssen im Home-Office erzeugte Daten zunächst lokal gespeichert und dann in die Backup-Strategie des Unternehmens eingebunden werden. Dabei gilt generell, dass die Datenhaltung möglichst zentral verwaltet und damit auch zentral gesichert werden sollte. Das gilt auch für Anwendungen wie beispielsweise E-Mail. Diese werden am besten auf dem Mailserver im Unternehmen empfangen und abgelegt. In einer schnell eingerichteten Umgebung kann es passieren, dass die E-Mails lokal in eine Datei gespeichert werden. Im Fall eines Datenverlusts wären diese Nachrichten unwiederbringlich verloren.

Ein Szenario für extern erzeugte Daten etablieren

Sollte es dennoch nötig sein, dass lokal Daten abgelegt werden müssen, dann ist dafür zu sorgen, dass die Backup-Software die Client-Konfiguration über die Netzwerkinfrastruktur – per VPN oder DHCP – auch zuhause findet und mitsichert. In der Regel wird es eine reine Home-Office-Zeit nicht geben. Daher muss das Backup-Szenario so gewählt sein, dass, wenn die Mitarbeiter an einem oder mehreren Tagen im Büro sind, ein Voll-Backup inklusive großer

Grafik: SEP

SEP sesam Beefalo V2 passt sich flexibel den wachsenden Bedürfnissen einer sich wandelnden IT-Umgebung an.

Dateien über das schnelle Firmennetzwerk erfolgt. Ist aber auch dies für eine längere Zeit nicht möglich, muss zumindest sichergestellt werden, dass der Nutzer in seiner privaten Umgebung temporär für ein adäquates Backup seiner lokalen Daten sorgt. Das kann beispielsweise durch regelmäßige Kopien auf externen USB-Platten erfolgen. Dies benötigt allerdings ein hohes Maß an Verständnis wo welche relevanten Daten abgelegt sind. Außerdem müssen immer die Datenschutzregeln beachtet werden, daher sind unbedingt private und Firmendaten zu trennen. Am Ende der Home-Office-Zeit müssen die Firmendaten dann wieder vom privaten Rechner gelöscht werden.

Was passiert aber, wenn Daten verloren gehen? Für den Restore-Fall sollte die Backup-Software ein Browser-basiertes Web-Interface mit einem Self-Service-Restore-Wizard zur Verfügung haben. Das bedeutet, dass notwendige Logins mit Passwörtern für die Authentifizierung verfügbar sind und von den IT-Administratoren eine korrekte Rechtevergabe, also Autorisierung konfiguriert sein muss. Dann lassen sich sogar komplett neu aufgesetzte Rechner wieder mit den gesicherten Daten wiederherstellen.

Cloud-Lösungen aber auch sichern

Wenn Cloud-Lösungen genutzt werden, lassen sich die erzeugten Daten von Home-Office-Arbeitsplätze am einfachsten sichern. Allerdings nur, wenn die dort abgelegten Dateien auch in die Backup-Strategie eingebunden sind. Vielen Unternehmen ist nicht bewusst, dass beispielsweise bei *Microsoft Office 365*, der *Google G-Suite* oder *Salesforce* die Kunden für die Datensicherung zuständig sind – auch wenn die Dateien vermeintlich auf den Servern der Cloud-Anbieter liegen. Office 365 geht beispielsweise mit sehr begrenzten Möglichkeiten zur Sicherung und Wiederherstellung einher – man behilft sich dort mit Dateiversionierungen und Papierkörben als wichtigste Absicherung, was leider eine Menge Einschränkungen mit sich bringt. Wiederherstellungen, die über die eigene Fehlerkorrektur eines einzelnen Users hinausgehen, benötigen Eingriffe durch sehr erfahrene Administratoren – und die richtigen Daten zur Wiederherstellung überhaupt erst zu finden, kann äußerst zeitaufwändig sein. Diese limitierten Möglichkeiten bieten kein konsistentes Backup.

Darüber hinaus ist es notwendig, dass Ressourcen, die bei Cloud-Dienstleistern gehostet werden, ebenfalls im Datensicherungs- und Recovery-Konzept einbezogen sind. Ein im Cloud-Rechenzentrum laufender Server sollte bei einem Ausfall zügig wiederherstellbar sein, von dem Cloud-Service-Provider sowie auch vom User. Optimal ist es, wenn die Einstellungen und Daten regelmäßig auch aus der Cloud zurückgespiegelt werden und beim Nutzer und damit doppelseitig gesichert sind. Damit hat der Nutzer die Chance, dass er im Desaster-Fall schnell und gezielt sein Recovery machen kann und nicht auf den Provider warten muss. Allerdings muss auch hier, wie in allen Backup- und Restore-Plänen, ein regelmäßiger Wiederherstellungs-Test stattfinden, um den reibungslosen Ablauf und die Konsistenz der Sicherung zu gewährleisten.

SEP sesam für hybride Backups

Der Backup-Spezialist **SEP** stellt dafür seinen Kunden *SEP sesam Hybrid Backup* (für On-Premises, Cloud, virtuelle und physische Umgebungen) und die *Cloud Application Protection Services* (CAPS) zur Verfügung, bei denen der benötigte Speicherplatz gleich inkludiert ist, so dass der Kunde eine fertige, komplette Lösung erhält mit unlimitierter Aufbewahrungszeit. Diese basieren auf einem verschlüsselten Backup-Connector, der Microsoft Office 365-, Google G-Suite-, Salesforce- und Microsoft Dynamics-Daten in einem EU-Rechenzentrum mit fortschrittlicher Synchronisationstechnologie sichert, welches EU-DSGVO-konform ist.

Es wird keine Hardware vor Ort benötigt und die Einrichtung dauert nur fünf Minuten, um durch einen modernen Backup-Dienst geschützt zu sein. Auch die Wiederherstellung ist sehr einfach: Die Mitarbeiter können über mehrere Backup-Snapshots und Vorschau-Daten suchen, um sicherzustellen, dass die wiederherzustellenden Daten die richtigen Daten sind. Die relevanten Daten können vor Ort, als Links oder als Archiv angezeigt sein, so dass der Benutzer die benötigten Daten zur Wiederherstellung auswählen kann. Den Usern können auch hier Rechte zugewiesen werden und alle Vorgänge werden in manipulationssicheren Protokollen gespeichert.

Datensicherung – Backup und Restore – ist also auch für die Umgebung im Home-Office möglich. Allerdings muss auch dafür eine intelligente Strategie entwickelt sein, um im Falle des Falles jederzeit und sehr schnell Unternehmensdaten wiederherstellen zu können. ■

Weitere Informationen

SEP AG
Konrad-Zuse-Straße 5,
83607 Holzkirchen
Tel. +49 (0) 8024/463 31-0
E-Mail: info@sep.de
www.sep.de

Langfristigen Einsatz einplanen

Auswahlkriterien Backup-Software

Eine Backup-Software ist immer nur so gut wie die Strategie, die man hinein konfiguriert. Nichtsdestotrotz muss man bei der Anschaffung von Backup-Software die richtigen Fragen stellen und sich im Vorfeld die zu sichernde IT-Landschaft genau ansehen. Da eine Backup-Software in der Regel lange im Einsatz und eine Migration zu einem anderen Produkt meist aufwendig ist, gilt es den Auswahlkriterien möglichst große Aufmerksamkeit zu widmen.

Wolfgang Stief

Backup ist das eine, aber noch wichtiger ist, sich über das Restore einzelner Files, einzelner Server oder sogar ganzer Server-Räume Gedanken zu machen, ehe man sich für einen bestimmten Hersteller entscheidet. Backup/Recovery ist meist eine langfristige Investition, der Wechsel von einem zum anderen Hersteller geht nicht selten mit einer aufwendigen Migration noch aufzubewahrender Sicherungsbänder einher. Eine sorgfältige Auswahl ist daher sinnvoll.

Wichtig: Betriebssystem und Datenbanken

Offensichtlich ist, dass Backup-Software alle im Unternehmen verwendeten Betriebssysteme unterstützen muss. Nicht nur, dass es für alle Betriebssysteme einen Agenten geben sollte. Jedes Betriebssystem hat so seine Eigenheiten, dazu gehören unter anderem offene Dateien, die nur zur Laufzeit relevant sind und gar nicht erst gesichert werden müssen. Eine gute Backup-Software kennt diese Eigenheiten und kann sie entsprechend berücksichtigen.

Die meisten Anwendungen heutzutage benutzen in irgendeiner Weise Datenbanken im Backend. Dort liegt häufig der eigentliche Wert des Unternehmens, Datenbank-Backup ist also unabdingbar. Datenbanken halten im Betrieb meist eine Reihe Dateien offen, in die Updates geschrieben werden. Um einen konsistenten Zustand der Datenbank zu sichern, müssen diese Dateien vor einem Backup geschlossen werden. Dazu muss die Datenbank entweder beendet oder in einen Sicherungsmodus versetzt werden. Letzteres braucht wiederum spezielle Agenten der Backup-Software, die mit den zugehörigen Datenbank-Tools kommuniziert. Kommerzielle Backup-Software unterstützt alle aktuellen, gängigen Datenbank-Systeme, für weniger verbreitete Datenbanken lohnt sich vor dem Kauf ein Blick in die Support-Matrix der Backup-Software.

Backup: Augenmerk auf Branchen-Software

In vielen Unternehmen kommt spezielle Branchen-Software zum Einsatz. Haben Sie Branchen-Software im Einsatz, sollten Sie zunächst prüfen, ob es vom Hersteller bestimmte Vorgaben gibt, wie Daten der Branchen-Software zu sichern und im Disaster-Fall zu recovern sind. Für weit verbreitete Branchen-Software liefern manche Hersteller ebenfalls Agenten mit, manchmal ist Handarbeit in Form von Scripts zur Automation erforderlich. In dem Fall muss die Backup-Software eine Schnittstelle anbieten, solche Scripts einzubinden, die vor oder nach einem Backup gestartet werden müssen.

Sonderbehandlung für Filer

NAS-Systeme sind nicht per Agent zu bändigen. Sie bieten aber meistens eine sogenannte NDMP-Schnittstelle (Network Data Management Protocol), um auf Anforderung Daten an ein Backup-System weiter zu geben. Über dieselbe Schnittstelle erfolgt auch ein Restore. Die Backup-Software muss ihrerseits natürlich NDMP unterstützen und beim Filer einen entsprechenden Request auslösen können. Jede halbwegs moderne, kommerzielle Backup-Software hat eine NDMP-Schnittstelle, ebenso eine Reihe großer, etablierter Backup-Systeme aus dem Open-Source-Ökosystem.

Keine Software ohne Hardware

Natürlich müssen die Backup-Daten irgendwo hingeschrieben werden. Die Anschaffung einer Backup-Software geht deshalb immer auch einher mit dem Kauf von Hardware für das Backup, bzw. muss die Software zur vorhandenen Hardware passen. Hier gilt es insbesondere darauf zu achten, dass ein eventuell vorhandener Bandroboter bzw. eine Tape-Library angesteuert werden kann. Diese Geräte gibt es von ganz klein mit einem Laufwerk und fünf Tape-Slots bis zu Installationen so groß wie eine Lkw-Garage. Größere Geräte haben in der Regel einen Barcode-Scanner am Greifarm, so dass Bänder identifiziert bzw. in der umfangreichen Library auch gefunden werden. Backup-Software, die Tape-Librarys ansteuern kann, kann normalerweise auch problemlos mit Barcode-Labels umgehen.

Tape-Technologie gibt es zwischenzeitlich gar nicht mehr so besonders viele verschiedene. Aktuell gebräuchlich und erhältlich sind im Wesentlichen das *LTO Ultrium*- und *3592 Tape Cartridge*-Format. Altinstallationen nutzen gelegentlich noch *DDS* (auch als *DAT* bekannt) oder *DLT*. Um eine Backup-Installation aktuell zu halten, ist alle paar Jahre ein Medienwechsel auf eine dann aktuelle Version von zum Beispiel LTO erforderlich. Alte Backups müssen dabei gegebenenfalls migriert werden. Professionelle Backup-Software stellt für eine solche Migration Mechanismen und Tools bereit.

Um Backup-Fenster möglichst kurz zu halten, spielt auch Backup-to-Disk eine wesentliche Rolle. Die Expertenmeinung geht auseinander, ob Disk ein »richtiges« Backup-Medium ist. Die Hersteller von Backup-Software entgegnen dem mit der Option Backup-to-Disk-to-Tape, manchmal als B2D2T abgekürzt: Das Backup wird zunächst innerhalb des geforderten, kurzen Backup-Fensters auf (schnelle) Festplatten geschrieben, ehe die Daten danach in Ruhe auf (langsame) Tapes verlagert werden. Zusätzlicher Vorteil davon: je nach Größe des Festplattenbereiches passen dort eines oder mehrere Voll-Backups hinein. Der Restore einer gestern versehentlich gelöschten Datei kann so sehr schnell und einfach aus diesem Disk-Bereich erfolgen, es muss nicht erst vom Roboter das passende Band eingelegt und gespult werden.

Backup in der virtuellen Welt

Ein großer Teil von IT-Diensten wird heutzutage in virtualisierten Landschaften betrieben. Platzhirsch ist hier sicherlich *VMware*, aber auch *Microsoft HyperV* oder *Citrix Xen-Server* genießen eine gewisse Verbreitung. In der quelloffenen Linux-Welt greift man häufig und gerne zu *KVM*, oder nutzt gleich Container-Technologie wie beispielsweise *Docker*.

Was immer funktioniert: Daten innerhalb einer virtuellen Maschine mit dem Agenten der Backup-Software zu sichern. Aus Sicht des Backups gibt es hier keinen Unterschied zwischen physischem Server und virtueller Maschine. Was man aber häufig haben möchte: eine Datensicherung der virtuellen Maschine direkt über den Hypervisor. Diese Funktion wird mittlerweile von vielen Backup-Produkten unterstützt, zusätzlich gibt es einige Hersteller, die sich auf diese Art von Backup spezialisiert haben. Unterscheidungskriterium ist hier häufig, ob aus dem Backup der virtuellen Maschine auch einzelne Files restauriert werden können (sogenannter Single-File-Restore).

Backup in die Cloud – Backup aus der Cloud

Cloud-Architekturen spielen beim Backup gleich in verschiedenen Rollen mit. Zunächst kann man ein Backup der lokalen Daten natürlich direkt in die Cloud machen. Es gibt dazu verschiedene Anbieter, die wiederum eigene Agenten bieten. Hier gelten dieselben Annahmen und Überlegungen, wie sie in diesem Artikel zur Auswahl von Backup-Software ausgeführt werden. Je nach Cloud ist zu bedenken, dass es typischerweise recht preiswert ist, Daten in eine

Cloud zu bekommen, die Anbieter aber gerne die Hand aufhalten, wenn man Daten aus der Cloud zurück ins eigene Rechenzentrum kopiert. Was bei einem Cloud-Backup ja der Fall ist.

Andersrum kann man auf die Idee kommen, dass die IT-Teile, die in eine Cloud ausgelagert wurden, zurück ins On-Premises-Backup gesichert werden sollen. Je nach Level der Abstraktion, den man in der Cloud fährt, ist das kein Unterschied zu einem Backup virtueller Maschinen. Man kann also den Backup-Agenten der Backup-Software in seine Cloud-Maschinen installieren und loslegen. Auch hier wieder der Hinweis: Datenvolumen, das aus einer Cloud abfließt, ist in der Regel extra zu bezahlen.

Schließlich bieten alle Cloud-Anbieter für ihre Dienste auch ein Backup innerhalb der Cloud, dass man sich einfach als weiteren Dienst dazu bucht. Diese Sorte Backup betrachten wir in diesem Artikel nicht weiter.

Endgeräte-Sicherung: Vom Problem des Handlungsreisenden

Nein, es geht hier nicht um das mathematische Problem des »Traveling Salesman«. Es geht hier um mobile Geräte. Waren das früher insbesondere Laptops von Außendienstmitarbeitern, hat man zwischenzeitlich einen ganzen Zoo an unterschiedlichen Geräten und Betriebssystemen, und in Zeiten von Home-Office oder Remote-Office auch sehr viel mehr von diesen kleinen digitalen Begleitern.

Laptops mit handelsüblichen Betriebssystemen sind dabei noch am einfachsten einzufangen. Diese Geräte unterscheiden sich wenig von Desktop-Arbeitsplätzen. Einzige Herausforderung: Laptops sind nicht zuverlässig immer mit einem Netzwerk verbunden und manchmal ist das Netzwerk eher schmalbandig. Ein tägliches Voll-Backup würde man da also vermeiden. Viele Hersteller bieten dazu spezielle Agenten, die zu sichernde Daten lokal am Endgerät analysieren, nur wirklich geänderte Daten übertragen, und die Daten bei der Übertragung auch noch komprimieren. Man muss dann nur noch dem Mitarbeiter beibringen, sein Laptop regelmäßig mit einem Netzwerk zu verbinden.

Ähnliche Lösungen gibt es auch für Smartphones und Tablets, dabei ist es normalerweise egal ob *Android* oder *iOS*. Beide Betriebssysteme sind in der Geschäftswelt etabliert, für beide Betriebssysteme gibt es Anbieter mit passenden Backup-Agenten.

Vertrauen ist gut — Kontrolle ist besser

Sobald man mehr als eine Handvoll Clients im regelmäßigen, nächtlichen Backup drin hat, möchte man brauchbares Monitoring.

Checkliste Backup-Software

- ☐ Gibt es für alle zu sichernden Betriebssysteme in ihrem Unternehmen die passenden Agenten? Denken Sie bitte auch an mobile Endgeräte und Smartphones.
- ☐ Stehen Backup-Agenten für die bei Ihnen eingesetzten Datenbanken zur Verfügung?
- ☐ Macht der Hersteller Ihrer Branchen-Software spezielle Vorgaben an eine Backup-Umgebung?
- ☐ Sollen auch Ihre Netzwerk-Filer mit ins Backup? Achten Sie bei der Backup-Software auf NDMP!
- ☐ Wird ihre vorhandene Tape-Library unterstützt? Auch der Roboter darin? Und die Tape-Drives?
- ☐ Backup-to-Disk und Backup-to-Disk-to-Tape sind Möglichkeiten zur Verkürzung des Backup-Fensters. Achten Sie auf entsprechenden Support, wenn Sie diese Funktionen nutzen möchten.
- ☐ Unterstützt die Software Disk-Images von virtuellen Maschinen?
- ☐ Kann die Software ggf. ein Backup in einen Cloud-Storage speichern?
- ☐ Können Sie ihre IT aus der Public-Cloud mit ins Unternehmensbackup integrieren?
- ☐ Werden alle Arten mobiler Geräte unterstützt, die im Unternehmen eingesetzt werden (Android, iOS)?
- ☐ Kann das Backup-System einen Backup-Status regelmäßig automatisiert berichten und bei Fehlern alarmieren?
- ☐ Kommt ihre Netzwerk-Security-Abteilung mit Backup-Agenten in der DMZ klar, die viele TCP-/UDP-Ports nach innen offen halten während eines Backup-Laufs?

Kein Backup-Admin setzt sich dann noch jeden Vormittag hin und liest File-Listen der Dateien, die gesichert wurden. Ihre Backup-Software sollte in der Lage sein, nicht durchgelaufene Backup-Jobs automatisch zu berichten. Sehr verbreitet ist eine Benachrichtigung per E-Mail. Alle ernsthaften Backup-Produkte haben das umgesetzt. Einige können zusätzlich auch noch per SMS alarmieren.

Weit verbreitet im RZ-Betrieb sind Monitoring-Plattformen. Diese sammeln Status-Informationen von laufenden Diensten per SNMP oder über einen eigenen Agenten. Eine SNMP-Schnittstelle bieten alle professionellen Backup-Umgebungen an. Mit den verbreiteten Systemen *Nagios/Icinga* oder *Zabbix* wird die Luft schnell dünn, wenngleich insbesondere Zabbix auch prima SNMP-Meldungen verarbeitet. Einige wenige Hersteller bieten Schnittstellen zu Nagios/Icinga und anderen quelloffenen Monitoring-Systemen. Wer beim Backup-Produkt seiner Wahl oder seines Vertrauens hierzu nicht fündig wird, muss sich wohl oder übel mit Handarbeit herumschlagen. Und dabei hoffen (oder vorab prüfen), dass vielleicht die emsige Community des Monitoring-Produkts das Problem für einen bereits gelöst hat und fertigen Code zur Verfügung stellt.

Nicht alle Wege führen zum Server

Eine unangenehme Eigenschaft von Backup-Software ist, dass ein Client (Agent) über mehrere TCP/UDP-Ports mit dem Server kommuniziert. Wer dabei welche Verbindungen in welche Richtung öffnet, muss man dem Handbuch des Herstellers entnehmen, hier gibt es keine einheitliche Regelung oder ein für alle etabliertes Verfahren. Handbuchstudium und Diskussion mit der hauseigenen Netzwerk-Abteilung vor dem Kauf liefert hier sicherlich sachdienliche Hinweise zur richtigen Kaufentscheidung.

Backup ist etwas Langfristiges

Eine Backup-Software ändert man langsamer, als das Betriebssystem seiner IT-Plattform. Tausch der Backup-Software geht meistens einher mit einer zeitaufwendigen Migration von vielen Komponenten und Prozessen. Das wird man in der Regel vermeiden wollen, nicht zuletzt sind damit auch entsprechende Kosten verbunden. Im Umkehrschluss heißt das bei der Auswahl: der Software-Hersteller sollte erkennen lassen, dass er es mit seiner Software ernst meint, und noch etliche Jahre damit am Markt bestehen möchte. Das ist von außen nicht immer einfach zu beurteilen, als Endkunde hat man häufig nur hochglanzpoliertes Marketingmaterial zur Verfügung. Papier jedoch ist geduldig. Helfen kann hier die vertrauensvolle Zusammenarbeit mit einem Systemhaus, das im Idealfall sogar mehrere Hersteller im Portfolio hat.

Man sieht, beim Kauf einer Backup-Software gibt es eine Reihe sehr unterschiedlicher Dinge zu beachten. Häufig wird ein Upgrade der bestehenden Software die erste Wahl sein. Oft genug ist man aber mit bestimmten Funktionalitäten unzufrieden oder ärgert sich über deren Abwesenheit, also wird man eine neue Software von vorne auswählen. Mein guter Rat: Nehmen Sie sich die Zeit die Sie brauchen, denn gut Ding will bekanntlich Weile haben. Nur so kann eine spätere Verärgerung oder Enttäuschung vermieden werden. ■

Anwenderbericht: Cölner 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 Cölner 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 **Cölner 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 Brauhaus 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 zukunftssicher 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: Cölner Hofbräu

Cölner 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 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 HD-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, 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. ■

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

Mini-Guide: Silent Bricks & Veeam V10

Neben der Integration von Backup und Archiv in einem System war der Abschied von Tape das zweite große Ziel. Zur Archivierung wurden Silent Bricks WORM eingesetzt, für das Backup Silent Bricks mit SSDs und HDDs. Wie man trotz Verzicht auf Tape dennoch höhere Sicherheit inklusive Air-Gap erhält, zeigen die Mini-Guides.
https://fastlta.com/sb-veeam

Weitere Informationen

FAST LTA AG
Rüdesheimer Str. 11, 80686 München
Tel. 089/89 047-610
E-Mail: info@fast-lta.de
www.fast-lta.de

Mit modernem Data-Management zum Schutz vor Ransomware

Superschnelle Restores lassen Angriffe ins Leere laufen

Ransomware-Angriffe sind unter den aktuell größten Cyberbedrohungen nach wie vor an der Tagesordnung. Unternehmen verschiedener Branchen waren bereits betroffen, ebenso wie das Gesundheitswesen. Die Angreifer haben oft Kliniken ins Visier genommen und den Betrieb erheblich gestört. Airlines, Flughäfen und Bahnunternehmen waren auch bereits betroffen. Pure Storage erläutert, wie Unternehmen durch modernes Data Management die Angriffe ins Leere laufen lassen können.

Markus Grau, Pure Storage

Die negativen Auswirkungen erfolgreicher Ransomware-Attacken sind vielfältig – für die Reputation, für das Vertrauen und natürlich auch die Finanzen. So soll der finanzielle Schaden zwischen 2015 und 2019 laut **TechRepublic** um das 479-Fache gestiegen sein. Auch wenn die genauen Zahlen schwer zu bestimmen sind, stellt sich die Frage, warum es den Unternehmen bislang nicht gelang, dieses Problem in den Griff zu bekommen. In Diskussionen und Studien kommen mehrere Hauptprobleme zum Vorschein:

Asymmetrie der Kosten: Es ist billig für die Angreifer, weiterhin anzugreifen, und teuer für die Opfer, die auf die Lösegeldforderungen eingehen, also eine sehr einfache Kosten-Nutzen-Analyse für die Angreifer.

Komplexität des modernen IT-Stacks: In einer modernen RZ-Umgebung gibt es viele Angriffsvektoren in Form von Komponenten, die aktualisiert und gepatcht werden müssten.

Diskrete Zahlungsmethoden: Die Cyberkriminellen greifen weiterhin erfolgreicher auf Bitcoin oder andere Kryptowährungen als relativ zuverlässige und anonyme Zahlungsmethoden zurück.

Verfügbarkeit: Ransomware-as-a-Service-Kits sind für Akteure, die wissen, wo sie suchen müssen, problemlos verfügbar. Angreifer können Kits mit einer Reihe von erforderlichen technischen Fähigkeiten, Verschlüsselungsarten und mehr erwerben.

Verteidigung – einfach in der Theorie, schwer in der Praxis

Wie bei vielen Sicherheitsthemen ist »Defense in Depth«, also eine »Verteidigung in der Tiefe« erforderlich. Es gibt jedoch so viele mögliche Angriffsvektoren, die kontrolliert werden müssen, was die Aufrechterhaltung einer umfassenden Verteidigung schwierig macht. Wirklich entschlossene und versierte Angreifer arbeiten sich jedoch oft durch jede mehrschichtige Verteidigung vor. In diesem Fall wird die Datensicherung dann zur Verteidigung der letzten Instanz. Warum also zahlen betroffene Unternehmen das Lösegeld, wenn es theoretisch so einfach ist, eine Wiederherstellung aus der Sicherung durchzuführen? Oft funktionieren die Datensicherungen nicht effektiv oder Wiederherstellungen sind nicht schnell genug, wenn sie am meisten gebraucht werden. Tägliche Ausfälle von Backups sind fast schon der Normalfall im IT-Betrieb.

Im Falle eines Ransomware-Angriffs sind die Auswirkungen von fehlgeschlagenen Backups, beschädigten Backup-Daten oder langsamen Wiederherstellungen jedoch viel größer als bei anderen Szenarien. Ein Ransomware-Angriff ist somit trotz statistisch geringer Wahrscheinlichkeit ein potentielles Ereignis mit großer Auswirkung, vor dem sich Unternehmen schützen sollten. Ebenso schließen Privatpersonen Versicherungen ab für Ereignisse, mit denen sie nicht rechnen, die aber möglich sind.

Bei einem System, das hochkomplex ist und tägliche Pflege erfordert, wie im Fall von Bandlaufwerken für die Datensicherung, ist fraglich, ob es einwandfrei funktioniert, wenn es darauf ankommt. Aus IT-Sicht gibt es täglich Probleme bei der Aufgabe, solche Systeme am Laufen zu halten. Während Ransomware eine konstante und wachsende Bedrohung darstellt, ist die

Wiederherstellung nach einem Ransomware-Angriff kein alltäglicher Vorgang. Selbst wenn die Backups erfolgreich ausgeführt werden, gibt es bereits Ransomware-Angriffe, die sowohl auf Backup-Daten und -Kataloge als auch auf Speicher-Array-Snapshots abzielen.

Unternehmen benötigen eine Kombination aus unveränderlicher, einfacher Speicherung und hoher Wiederherstellungsgeschwindigkeit, um nach Ransomware-Angriffen schnell wieder zum Normalbetrieb überzugehen. Dies ist mit einer vollständig auf Flash basierenden Datei- und Objektspeicherplattform möglich, die konzeptionell von Haus aus auf Skalierbarkeit und Durchsatz ausgelegt ist. Die Unveränderlichkeit verhindert, dass Backups von Angreifern kompromittiert werden, und unterstützt damit eine einfache und schnelle Wiederherstellung.

Abschwächung der Auswirkungen von Ransomware-Angriffen

Zwei Wiederherstellungsfunktionen sind für die Milderung der Auswirkungen eines Ransomware-Angriffs von entscheidender Bedeutung: die Zuverlässigkeit und die Geschwindigkeit der Datensicherung und -wiederherstellung.

Erstens, müssen Daten gesichert und die Backups vor absichtlichem, böswilligem Löschen geschützt werden. Dazu muss das Speichersystem, das die Backups aufnimmt, einfach, zuverlässig und unveränderlich sein. In diesem Fall bezieht sich die Unveränderlichkeit auf die Fähigkeit eines Systems, Änderungen oder das Löschen eines Objekts nach seiner Erstellung zu verhindern. Unveränderlich bedeutet auch, eine Kompromittierung der Datensicherung zu verhindern, selbst wenn die Administrator-Berechtigungsnachweise kompromittiert worden sind.

Zweitens, muss das Backup-System auch in der Lage sein, Daten schnell wiederherzustellen. Mit anderen Worten: Wenn sich Backups nicht schnell genug wiederherstellen lassen, um größere Auswirkungen zu vermeiden, was nützen diese Backups dann? Die Frage ist also, ob das bestehende Backup-System schnell genug Wiederherstellungen durchführen kann, falls nach einem Ransomware-Angriff große Teile des Rechenzentrums aus dem Backup wiederhergestellt werden müssen.

Die meisten Backup-Systeme sind nicht dafür ausgelegt, einen großen Prozentsatz einer Kundenumgebung innerhalb eines kurzen Zeitrahmens wiederherzustellen. Bei einem Ransomware-Angriff ist jedoch die Recovery-Geschwindigkeit kritisch. Mit herkömmlichen Speichersystemen können die Wiederherstellungszeiten sich über Monate hinziehen. Dies ist für die Geschäftskontinuität eindeutig inakzeptabel.

Worauf es beim Speichersystem ankommt

Eine zeitgemäße Datei- und Objektspeicher-Plattform muss drei entscheidende Anforderungen erfüllen:

Einfachheit: Die Lösung sollte leicht einzurichten, zu verwalten, zu erweitern und in Backup-Software zu integrieren sein.

Unveränderlichkeit: Unveränderliche Speicherung gewährleistet, dass Backups nicht durch Angreifer kompromittiert werden, selbst in Szenarien, in denen der Admin-Zugang kompromittiert wurde.

Geschwindigkeit: Die Wiederherstellung muss schnell genug erfolgen, um größere Auswirkungen auf den Geschäftsbetrieb zu vermeiden.

Mittels einer modernen Datei- und Objektspeicher-Plattform wie *FlashBlade* von Pure Storage lässt sich in der Praxis die Wiederherstellungs-Geschwindigkeit einer Datenbank um einen hohen zweistelligen Faktor erhöhen und nach Bedarf skalieren. Das ist eine Größenordnung, die Unternehmen im Ernstfall die Gewissheit gibt, dass ihre Backups tatsächlich schnell genug zur Verfügung stehen.

Um sich insbesondere vor gezielten Angriffen zu schützen, bietet Pure Storage eine Funktion namens *SafeMode* in der Speicherplattform selbst an. *SafeMode* hindert Ransomware-Angreifer daran, auf der Plattform gespeicherte Backups überhaupt erst zu löschen. Nach der Inbetriebnahme werden automatisierte Snapshots erstellt, die für eine festgelegte Zeitspanne aufbewahrt werden und weder vom Kunden noch von Personen mit Admin-Zugriff auf das Speichersystem gelöscht werden können.

Natürlich erfordert dies zusätzlichen Speicherplatz auf dem System, um die Snapshots über die angegebene Zeitspanne vorzuhalten. Speicheranbieter unterstützen ihre Kunden aber bei der Größenbestimmung, um Klarheit über den benötigten Platz und die daraus resultierenden Kosten zu schaffen. FlashBlade bietet die entscheidende Kombination aus Einfachheit, Unveränderlichkeit und Geschwindigkeit. Bei der dringenden Wiederherstellung nach Ransomware-Angriffen kommt es genau darauf an. ■

Weitere Informationen

Pure Storage Germany GmbH
Mies-van-der-Rohe-Straße 6
80807 München
Tel. +49 (0)89/120 89 253
E-Mail: info@purestorage.com
www.purestorage.com/de/

Marktüberblick Backup-Software

Backup & Recovery für Mittelstand und Enterprise

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

Michael Baumann

Anbieter	Produkt
Acronis	Cyber Backup
Actifio	VDP (Virtual Data Pipeline)
Arcserve	UDP (Unified Data Protection)
Cohesity	DataProtect
CommVault	Complete Backup und Recovery
Dell EMC	Networker Data Protection Suite
Druva	inSync
IBM	Spectrum Protect
Micro Focus	Data Protector
Novastor	NovaBackup
Rubrik	Cloud Data Management
SEP	sesam Beefalo
Unitrends	Enterprise Backup
Veeam	Availability Suite
Veritas	NetBackup/BackupExec

Im Mittelstands- und Enterprise-Segment überzeugen manche Datensicherungs-Produkte durch universelle Leistungsvielfalt, andere sind eher »Spezialisten«. Dennoch: Für uns sollte Backup-Software idealerweise eine breite Palette an Hosts, Anwendungen, Speichertechnologien und Datensicherungs-Strategien unterstützen. Die Software sollte modular aufgebaut, skalierbar und mit einer Vielzahl von Plattformen, Betriebssystemen, Tape-Librarys, Laufwerken und Topologien kompatibel sein. Auch Mobilität bzw. die Sicherung am Front-End rücken für RZ-Administratoren zunehmend in den Fokus.

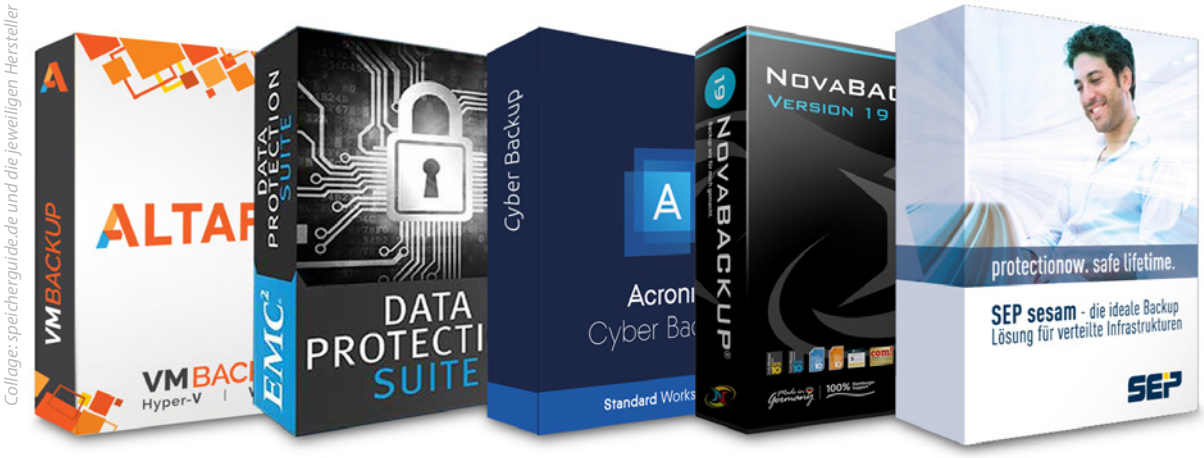
Marktübersichten können nie komplett sein. Bei unserem Überblick spielt zunächst die weltweite Marktdurchdringung bei Großunternehmen (nach *Gartner* und *Forrester*) eine Rolle, wir berücksichtigen aber auch Produkte, die hauptsächlich im deutschsprachigen Raum ihre Liebhaber finden und tendenziell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

Acronis Cyber Backup

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

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

Die Acronis-Software steht im Ruf einer Mittelstandslösung, ist aber auch im Enterprise-Segment gefragt, wenn die Datensicherung in der Cloud/SaaS ergänzt wird durch On-Premises. Demnach punktet die Software durch einfa-



Collage: speicherguide.de und die jeweiligen Hersteller

che Handhabung und überschaubare Kosten. Für die Standard-Suite fallen jährlich derzeit 369 Euro pro Server, 449 Euro pro Virtual Host und 55 Euro pro Workstation an. Für die Advanced Edition 639 Euro pro Server, 729 Euro pro Virtual Host und 75 Euro pro Workstation. Kostenlose Testversionen sind verfügbar.

Arcserve UDP

Arcserve *Unified Data Protection* (UDP) basiert auf den Wurzeln von *Arcserve Backup* und letztlich auf der Weiterentwicklung des Erbes von *CA Technologies*. In der Regel findet die Software eher Anwendung bei mittelständischen Anwendern, große Oracle-Umgebungen beispielsweise sind eher die Ausnahme, glaubt man den Analysten.

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

Zur Liste unterstützter Plattformen gehören Windows, Linux, Amazon EC2, Microsoft Azure, Office 365 (Exchange Online, SharePoint Online und OneDrive for Business), Microsoft Exchange, MS SQL, Dateiserver, Microsoft IIS, Microsoft Active Directory, Oracle Database, PostgreSQL, VMware vSphere (agentenlos), Microsoft Hyper-V (agentenlos) und Nutanix AHV. Die Kosten für Arcserve UDP Advanced Edition in der aktuellen Version (v. 7.0) für eine Server-OS-Instanz inklusive Enterprise-Wartung liegen bei etwa 550 Euro pro Jahr.

Cohesity

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

Von einer einheitlichen Benutzeroberfläche können laut Hersteller Hypervisoren (Vmware, Nutanix AHV, Microsoft Hyper-V, RHeV), traditionelle und moderne Datenbanken (Oracle, SQL, MongoDB, Cassandra, CouchbaseDB, Hbase) und Anwendungen (SAP HANA, EPIC, Office 365, Kubernetes), Big-Data-Hadoop-Workloads, Speicher (Pure, Netapp, Cisco, Dell EMC) und physische Workloads (Microsoft, Solaris, Linux, AIX) verwaltet, gesichert und wiederhergestellt werden.

Cohesity Data Protect ist ein Abonnement-Dienst, der je nach Funktionalität und Kapazität zwischen 400 Euro bis in den fünfstelligen Bereich jährlich kosten kann. Zudem ist der Dienst als Add-on zur Cohesity Data-Platform verfügbar, die in der Premi-

um-Edition für etwa 1.200 Euro (netto) jährlich buchbar ist, wiederum mit unzähligen Variablen.

Commvault Complete Backup und Recovery

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

Mit Commvaults Flaggschiff *Complete Backup und Recovery* stehen über 40 Cloud-Speicherungsoptionen in öffentlichen und privaten Clouds zur Verfügung. 16 Hypervisoren, quasi alle File-Systeme und 15 Datenbanken werden unterstützt. Auf der Kompatibilitätsliste stehen über 30 Primär-Storage-Plattformen und eine Vielzahl an Tape-Systemen (Adic, Dell EMC, H3C, HPE, IBM, Quantum, Spectra Logic).

Multi- und Hybrid-Cloud-Support, Remote-Duplikation, Deduplikation und Encryption sind inkludiert, ebenso Engines für intelligente Archivierung von Nutzerdaten in lokalen und in der Cloud gespeicherten Mailboxen sowie in anderen nutzerbasierten Datenspeichern. Künstliche Intelligenz und Algorithmen für maschinelles Lernen sollen die Leistung optimieren, Muster analysieren und Anomalien melden, erklärt der Hersteller.

Flankiert wird Commvault Complete Backup und Recovery vom SaaS-Angebot *Commvault Metallic Core* und der Scale-out Backup-Appliance *HyperScale*.

In Online-Shops rangiert *Commvault Complete Backup und Recovery* bei einem Listenpreis von 1.792 Euro netto für eine dauerhafte Lizenz für einen physischen Server bzw. eine OS-Instanz. Für zehn VM-Instanzen fallen etwa 2.600 Euro an und die 5-Jahreslizenz für eine physische Instanz beläuft sich auf rund 3.500 Euro.

Dell EMC Networker Data Protection Suite

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

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

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

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

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

Altaro VM Backup 8

Altaro *VM Backup 8.13* unterstützt die Sicherung von Hyper-V- und VMware-Maschinen und ermöglicht ein lokales Backup auf einen Netzwerk-Share sowie mehrere Offsite-Kopien sowohl an einen anderen Altaro-Server als auch an unterschiedliche Cloud-Anbieter wie Amazon S3, Azure oder Wasabi. Lizenzen werden per Backup-System ausgegeben, weder per CPU noch per Kern oder nach Workload. In der Unlimited Edition beginnt der Preis bei 595 Euro netto pro Backup-Host. Lesen Sie mehr in der Produkt-Review auf speicherguide.de.

Druva

Mit **Druva** gibt es einen weiteren relativ erfolgreichen Newcomer im Bereich Data-Protection. *Druva Phoenix* ist eine SaaS-Plattform für die Sicherung von lokalen physischen und virtuellen Servern. *Druva inSync* legt den Schwerpunkt auf Endpunkt-Datensicherheit, d. h. insbesondere auch die professionelle Datensicherung mobiler Endgeräte.

Die Cloud-Plattform baut auf AWS auf, kombiniert diese Endpoint- mit SaaS-Anwendungsdaten und ermöglicht deren Verwaltung. Insbesondere werden Dienste für mobiles Personal geboten und im Gegenzug für das Unternehmen Compliance- und Governance-Services vorgehalten.

Im AWS-Marketplace ist Insync in der Enterprise-Version ab 480 US-Dollar im Abo

für zehn Nutzer (G-Suite und Office 365) sowie 960 US-Dollar ohne Anwendungsrestriktion erhältlich. Die Elite-Version beinhaltet eDiscovery und Compliance-Funktionen und ist entsprechend teurer.

IBM Spectrum Protect

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

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

Zu Preisen, der Lizenzstruktur, vor allem im Verbund mit etwaigen Hardware-Verkäufen und damit verbundenen Rabatten, ist es uns nahezu unmöglich, Aussagen zu treffen. Dafür gibt es aber eine Heerschar an Vertriebs- und Beratungskräften, die sich darauf spezialisiert haben.

Micro Focus

Das in Großbritannien niedergelassene Unternehmen ist in Deutschland noch nicht sehr etabliert. Durch die Übernahme großer Teile der *HPE*-Software-Sparte und einem Umsatz von 4,4 Milliarden US-Dollar kann man allerdings nicht von einem Start-up sprechen. Datenmanagement rund um die digitale Transformation hat sich das Unternehmen auf die Fahnen geschrieben.

Im Bereich Datensicherung steht der **Micro Focus** *Data Protector* im Portfolio. Das Produkt adressiert Enterprise-Kunden, inkludiert Security-Aspekte und Analytics-Funktionen. Entsprechend der Historie verwendet Data Protector dieselben Snapshot-APIs wie HPE, so dass sich hier ein großes Spektrum an Kompatibilitäten bietet. Dazu gehören *StoreOnce, Nimble, SimpliVity* sowie die Integration in *HPE Catalyst* und *Recovery Manager Central*.

Das NDMP-basierte Backup unterstützt aber auch *Dell EMC Data Isilon*, *Domain* und *Unity*, *Nutanix*, *NetApp*- und *Hitachi*-Systeme. Neben lokalen Ressourcen wird über das *Microsoft StorSimple*-Gateway die Cloud erreicht. Dort stehen dann *Azure*- und *Amazon S3*-kompatible Services bereit. Nur Vmware und Hyper-V werden nativ, KVM funktional unterstützt. Ein Schwerpunkt liegt auf Analytics, Automation und Orchestrierung.

Die Software kann als Express-(virtuell) und Premium-(hybrid) Variante lizenziert werden. Neben einer kostenlosen Testversion kann Express ab 1.000 US-Dollar pro CPU-Socket erworben werden.

Novastor NovaBackup

Das in Hamburg ansässige Unternehmen **Novastor** bietet mit *NovaBACKUP Business Essentials* eine Datensicherungslösung für physische und virtuelle Maschinen. Adressaten sind eher kleine bis mittelständische Unternehmen, wie Arztpraxen, Kanzleien und Handwerksbetriebe.

NovaBackup bietet universelles Backup und Restore für Windows-Server, SQL-Backup im laufenden Betrieb, Sicherung von *Exchange*-Datenbanken, Vmware- und Hyper-V-Sicherungen von beliebig vielen virtuellen Maschinen und Image-Backups zum Schutz vor einem Systemausfall oder Festplattenfehlern. Unterstützt werden lokale Speichermedien (USB, Tape, RDX, NAS) sowie Cloud-/File-Sharing-Dienste (z. B. Sharepoint, Onedrive, Dropbox, Amazon S3).

NovaBackup Business Essentials 19 kostet voll lizenziert 599 Euro bzw. ab 269 Euro im Jahres-Abo.

Rubrik

Neben Cohesity ist **Rubrik** ein neuer »Stern« am Data-Protection-Himmel. Dynamisch wie die Datenwelt präsentiert sich das Unternehmen mit seinem Cloud-Data-Management-Produkt *Andes*. On-Premises-, Edge- und Multi-Cloud-Workloads können mit Rubrik gesichert werden, in der Cloud. Der Andes-Service beinhaltet Data-Protection, Ransomware-Recovery, Compliance

Bacula – Open-Source-Backup

Das Open-Source-Tool Bacula 9.6.3 kann es nach Meinung der Open-Source-Szene durchaus mit kommerziellen Programmen aufnehmen. Die Software ist modular aufgebaut und kommt mit einer netzwerkfähigen Client-/Server-Architektur.
Neben der Free-Version wird über Bacula Systems auch eine kostenpflichtige Enterprise-Edition angeboten. Diese wird über ein Abomodell mit jährlicher Preisgarantie angeboten. Zudem ist eine dauerhafte Lizenzierung möglich, mit einer zusätzlichen jährlichen Zahlung können Support und Updates eingekauft werden. Genaue Preise kommuniziert der Anbieter als nicht öffentlich.
https://www.baculasystems.com/

nach individuellen Vorgaben und generell Datenmobilität durch die Sicherung in der Wolke mit einem gewissen Grad an Automation und API-Offenheit. Datenklassifizierung, Archivierung, Disaster-Recovery und Migration will der Dienst bieten. Dies soll Endgeräte ebenso beinhalten wie VMs und Datenbanken. Mit *Polaris Sonar* bzw. *Polaris GPS* bietet der Hersteller zudem eine Online-Plattform zur Datenklassifizierung.

Eigenen Angaben zufolge ermöglicht Rubrik Unternehmen ein leistungsstarkes, eng verzahntes Cloud Data Management, beispielsweise für Cloud als Archiv, DR in der Cloud, Test/Dev, Office 365. Die Lösung versteht sich als »Umbrella«-Management zwischen On-Premise- und Cloud-Workloads.

Banal ist der Service nicht: Integriert ist eine selbstheilende Masterless-Architektur, eine nativ integrierte und Vmware-zertifizierte CDP-Funktion (Continuous-Data-Protection) als Option in SLA-Domains, mit der Firmen ihre Datenschutzrichtlinien definieren können.

Smart-Data-Tiering-to-Azure, SaaS-basiertes Polaris GPS, verteilte Metadaten und Namespaces, richtliniengesteuerte Datenverwaltung, rollenbasierte Zugriffskontrolle, Nutzungs- und Compliance-Reports sowie die Integration mit Automatisierungs-Frameworks sollen zum Datensicherungsnutzen beitragen.

SEP Sesam

Der deutsche Backup- und Disaster-Recovery-Spezialist **SEP** wartete kürzlich mit der Version 2 seiner *SEP sesam Beefalo*-Software auf. Sie unterstützt neun Hypervisoren nativ, mehrheitlich mit der Möglichkeit für Single-File-Restore. Zuletzt wurde der *Oracle Linux Virtualization Manager* (OLVM) hinzugefügt und das LTO-Band-Handling optimiert.

SEP setzt zudem auf den Support von *HPE StoreOnce* und *Catalyst*. Assistentenwerkzeuge für die Rücksicherung gibt es für die Datenbank-Applikationen von Oracle, SAP HANA und SQL-Server in Form von *Always-On Availability Groups* (AOAG). Auch die Rücksicherung der *VMware Sandbox* wird assistiert.

Das Lizenzmodell beginnt bei SEP Sesam Beefalo mit einem Stream und der Sicherung von einem TByte auf Festplatte und eine unbegrenzte Anzahl an Wechselmedien bei 290 Euro netto und beinhaltet 12 Monate Maintenance.

Veeam Availability Suite

Aus der Virtualisierungsszene kommend, gehört **Veeam** nach Umsatz mittlerweile zu den Top 5 der Data-Protection-Anbieter, so die Analysten. Für das Backup virtueller Vmware-Maschinen fast schon Standard, aber auch Hyper-V wird unterstützt. Dementsprechend wird bei der *Veeam Availability Suite* unkomplizierte Administration von Backup und Restore von VMs vorausgesetzt.

Die Availability Suite unterstützt 19 Dateisysteme und ermöglicht die Wiederherstellung von virtuellen Festplatten aus VMs und einzelner Dateien, auch auf abweichenden Hosts. Die Software unterstützt die Wiederherstellung einzelner Objekte aus Microsoft Anwendungen wie SharePoint, SQL-Server, Exchange und Active-Directory mit dem *Veeam Explorer*.

Über U-AIR und Veeam Explore für Oracle lassen sich einzelne Objekte aus Oracle-Datenbanken und beliebigen virtualisierten Anwendungen wiederherstellen. Dazu zählen unter anderem *MySQL* und *PostgreSQL*-Kompression und Deduplizierung sind inkludiert. Auch die Migration von VMware VMs über Storage vMotion und VMware vMotion sind schnell und einfach von der Hand.

Potenzielle Kunden mit dem Bedarf an der Datensicherung von virtuellen und physischen Komponenten müssen sich über die Hardware-Unterstützung der Suite informieren. Plattform-seitig werden Windows, Linux und AWS unterstützt.

Veeam Availability Suite Enterprise (V10) ist ab 1.850 Euro pro Lizenz und Jahr erhältlich, ohne Support. Mit Betreuung steigen die Kosten auf 2.750 Euro netto.

Veritas Technologies

Veritas ist der Dino in der Software-Data-Protection-Szene. Mit *Backup Exec* eher auf KMU abzielend, adressiert Veritas mit *NetBackup* größere Umgebungen im gehobenen Mittelstand und Enterprise-Bereich. Aus der langen Historie ergibt sich eine breite Unterstützung für Hard- und Software, und viele Add-Ons, die je nach Bedarf interessant sein können.

Netbackup ermöglicht über den *NetBackup CloudCatalyst* den Zugriff auf über 40 Cloud-Konnektoren. Aktiv unterstützt werden *AWS Glacier* und *Deep Archive* mit orchestriertem Disaster-Recovery sowie das Azure-Archiv. Für Vmware steht ein agentenloses File-Recovery zur Verfügung.

Die Wurzeln von Netbackup reichen bis in die frühen 1990er Jahre zurück. Daher darf das Produkt in der Version 8.2 in Sachen 3rd-Party-Support und Kompatibilität durchaus als ausgereifte Lösung bezeichnet werden. Auch Unix-Files versteht das System. Eine On-Premises-Lizenz kostet um die 2.700 Euro (netto). ■

Weitere Informationen

Lesen Sie eine ausführliche Fassung des Marktüberblicks auf speicherguide.de


Backup/Recovery
Produkt-Reviews
NAS-Systeme
Storage-Management
Datenrettung
Cloud
Festplatten
Archivierung
News
SoHo-NAS
Management
iSCSI-SAN
Speicher
Hochverfügbarkeit
Optical-Storage
Solid-State-Disk
Controller & Interface
Bandroboter
Disk-Backup
speicherguide.de
Das Storage-Magazin
KOSTENLOSER
Storage-Newsletter
Aktuelle Storage-Meldungen und die neuesten Beiträge kompakt serviert auf speicherguide.de
Unser Newsletter erscheint immer Mittwochs und Freitags.
Hier abonnieren ›

speicherguide.de-Leserbefragung

Backup/Recovery: Tape ja, Cloud nein

In unserer Leserbefragung kristallisieren sich eindeutige Trends heraus: Knapp die Hälfte der Umfrageteilnehmer setzen auf eine Backup-to-Disk-to-Tape-Strategie, knapp ein Viertel sichert nur noch auf Disk. Die Cloud erhält als Backup-Medium dagegen eine klare Abfuhr. Über ein Drittel agiert bei den täglichen Sicherungen im zweistelligen TByte-Bereich (und mehr).

Karl Fröhlich

Das Thema Backup ist komplex und wird aus unterschiedlichen Sichtweisen diskutiert. In der *speicherguide.de*-Redaktion kennen wir das aus unzähligen Gesprächen mit Herstellervertreter, Händlern und Consultants sowie Experten aus den Rechenzentren. Einig sind sich alle darin, dass eine kontinuierliche Datensicherung wichtig ist. Beim »Wie« trennen sich die Meinungen durchaus und diese reichen von »wir machen CDP (Continuous Data Protection) im Minutentakt« bis hin zu »wir halten alles als Snapshot fest«.

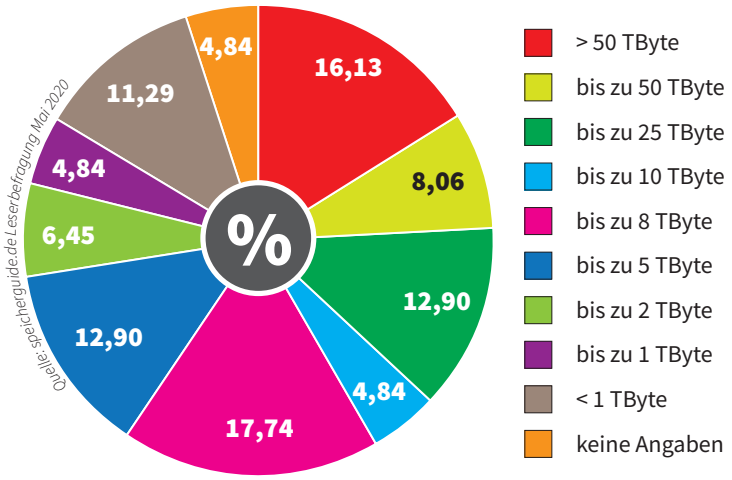
Einigermaßen überraschend ist die relativ große Einigkeit der *speicherguide.de*-Leser bei unserer Backup-/Recovery-Umfrage: Natürlich war es vorhersehbar, dass Tape nicht mehr das Backup-Medium Nummer 1 ist. Interessant ist trotzdem: Knapp die Hälfte der Teilnehmer (48 %) setzt auf eine Backup-to-Disk-to-Tape-Strategie und etwas über ein Viertel sichert nur noch auf Disk (27 %). Immerhin bezeichnen immer noch elf Prozent Tape als das einzig wahre Backup-Medium. Für die überwältigende Mehrheit ist die Cloud keine Alternative für ihre Backups. Hier ist das Ergebnis mit rund 68 Prozent sehr eindeutig. Nicht ganz zehn Prozent denken ernsthaft darüber nach bzw. sichern ihre Daten die Cloud.

Fast ebenso eindeutig ist die Meinung zu Open-Source. Mehr als die Hälfte (58 %) setzt auf kommerzielle Software, damit der Support des Herstellers gewährleistet ist. Fast 18 Prozent halten ihre Infrastruktur als zu groß, zu komplex bzw. zu kritisch für Open-Source-Backup.

Differenzierter sieht es bei der täglich zu sichernden Backup-Volumen aus. Wobei unsere Umfrage mit dem ungebremsten Datenwachstum einen der größten Problemherde belegt: 16 Prozent unserer Leser müssen täglich über 50 TByte sichern. Bei rund 20 Prozent sind es zwischen zehn und 50 TByte bzw. fünf bis zehn TByte. Fast 13 Prozent mühen sich mit zwei bis fünf TByte ab.

Die Top-Backup-Tools der *speicherguide.de*-Leser kommen im Übrigen von *Veeam*, *Commvault*, *SEP* und *IBM*. Nun ist unsere Backup-Recovery-Umfrage nicht ganz repräsentativ, für uns aber ein sehr guter Indikator. Noch haben wir die Miniumfrage nicht beendet, kommen Sie daher gerne noch mit dazu. Folgen Sie einfach diesem **Link**. ■

Tägliches Backup-Volumen



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. Speichermedien 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 einem Ausfall gefeit. Ohne Kopie sind die Daten unweigerlich verloren. Datenrettungsdienste erreichen heutzutage durchaus kleine Wunder, verlassen kann man sich darauf aber nicht. Zudem ist Datenrettung ein mitunter kostspieliger Service. Je nach Art und Beschädigungsgrad des Mediums beginnen die zu kalkulierenden Einstiegskosten im vierstelligen Bereich. Zudem müssen Betroffene Zeit mitbringen. Die Wiederherstellungszeit bemisst sich in der Regel in Wochen… Für eine größtmögliche Sicherheit sollten für die Datenkopien zwei unterschiedliche Speichertechnologien genutzt werden. Man spricht hier vom sogenannten Medienbruch. Dies soll die Ausfallwahrscheinlichkeit verringern und für eine Risikoverteilung bei systembedingten Fehlern sorgen und vor Ransomware-Attacken schützen. Jede Internet-Anbindung ist ein potentielles Einfallstor für Cyberangriffe.

Grafik: speicherguide.de

Daher sollte sich eine ausgelagerte Kopie zudem an einem anderen geographischen Standort befinden. Alle vorangegangen 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:
Michael Baumann, 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:
Grafik: Adobe Stock / Sikov

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

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

speicherguide.de
Das Storage-Magazin

Unser Team

Karl Fröhlich
Chefredakteur
speicherguide.de

Michael Baumann
Redaktion
speicherguide.de

Jens Leischner
Redaktion & Beratung
speicherguide.de

Wolfgang Stief
Redaktion & Beratung
speicherguide.de

Kerstin Mende-Stief
Mediaberatung
speicherguide.de