SWISS iT Magazine

Nr. 4 | April 2023 | Fr. 11.–

Ratschläge an Bundesrat Rösti
Seite 20

NEWS & TRENDS

Google streicht 250 Stellen in Zürich Seite 7

START-UP

Share.P bereitet der Parkplatz-Suche ein Ende Seite 12

CIO-INTERVIEW

Daniel Fiechter, CIO, Stobag Seite 14

SWISS MADE SOFTWARE

Planungstool für die Baubranche Seite 21

NEUE PRODUKTE

Managed Business-WLAN fürs Home Office Seite 54

IT@HOME

Logitech-Kopfhörer passen sich ihrem Besitzer an Seite 60

BACKUP & STORAGE

ab Seite 24

Storage-Strategien für die Cloud und On-Premises

Das Konzept der Datenplattformen

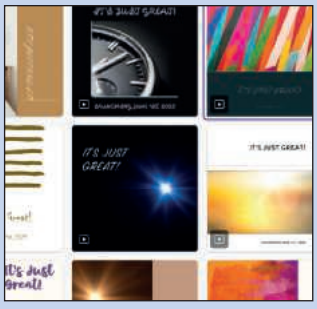
33 Cloud-Backup-Angebote aus der Schweiz

Depositphotos.com

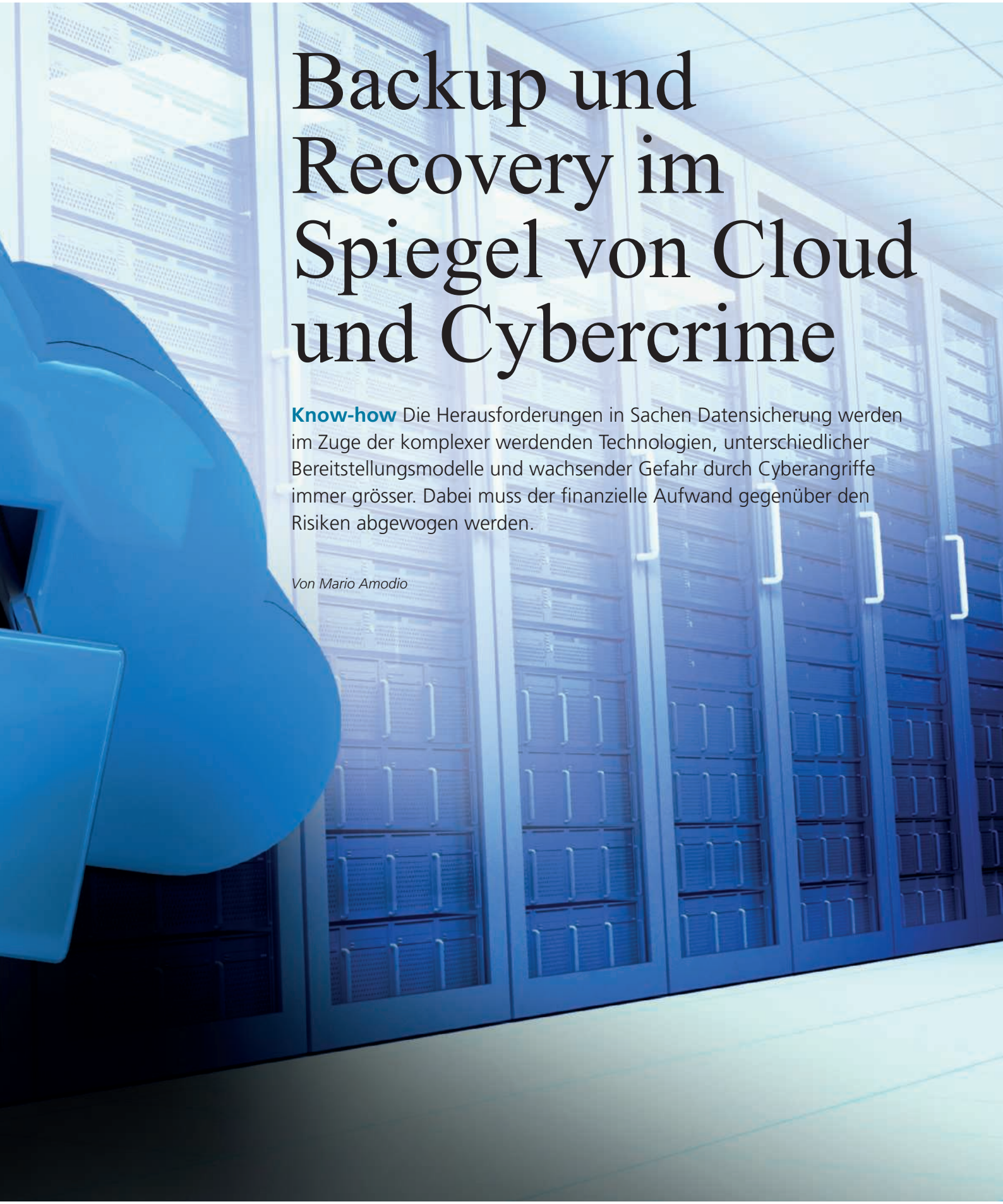
TEST CENTER

Was taugen Microsofts KI-Werkzeuge in der Praxis?

Microsoft hat eine ganze Reihe seiner Produkte mit Künstlicher Intelligenz (KI) versehen – so seine Suche, Teams Premium oder Microsoft Designer. Wir haben getestet, welchen praktischen Nutzen die KI in diesen Lösungen hat. Seite 46



INHALT



Backup und Recovery im Spiegel von Cloud und Cybercrime

Know-how Die Herausforderungen in Sachen Datensicherung werden im Zuge der komplexer werdenden Technologien, unterschiedlicher Bereitstellungsmodelle und wachsender Gefahr durch Cyberangriffe immer grösser. Dabei muss der finanzielle Aufwand gegenüber den Risiken abgewogen werden.

Von Mario Amodio

Die Anforderungen an die Gewährleistung der Datenverfügbarkeit steigt für Unternehmen von Jahr zu Jahr. Dabei sind nicht nur die Technologien einer ständigen Veränderung unterworfen. Auch die Bedrohungen für Datenverlust und die damit verbundenen Auswirkungen nehmen ständig zu. Hinzu kommt der allgemeine Druck auf die Kosten der Informatik und die Erwartung, dass Innovation und Digitalisierungsbemühungen mit Einsparungen bei den Betriebskosten finanziert werden sollen. Alles in allem sehen sich Verantwortliche bei Backup- und Storage-Bemühungen vor die Tatsache gestellt, die Geschäftstätigkeit zu garantieren und gleichzeitig die Kosten dafür im Griff zu behalten. Die Tatsache, dass zusätzlich zu neuen Technologien die Daten durch hybride und Multi-Cloud-Ansätze dezentral und verteilt in Umgebungen gehalten werden, lässt das Risiko für Datenverluste und die Schwierigkeit der Wiederherstellbarkeit zusätzlich grösser werden. Wenn Technologien unterschiedlicher Generationen die Datenlandschaft zunehmend fragmentieren, Arbeitslasten sich verteilen und Datensilos entstehen, erhöht dies die Komplexität und die Schwierigkeit, die Wiederherstellbarkeit von Daten über das gesamte Unternehmen hinweg zu gewährleisten und die Wahrung der Geschäftstätigkeit zu garantieren.

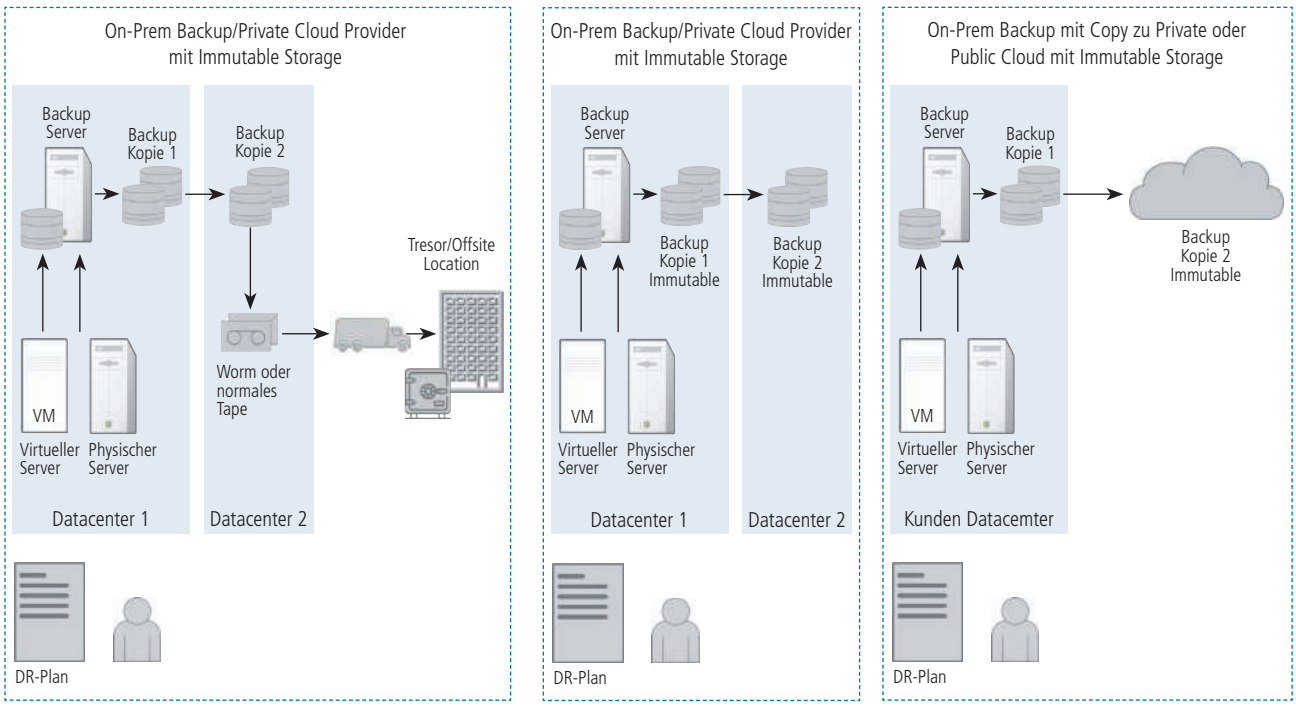
Cloud-Trend auch bei Storage und Backup

Die wachsende Bedeutung von Backup- und Storage-Lösungen zeigt auch ein Blick auf die Marktentwicklungen. Gemäss dem Marktforschungsunternehmen Global Industry Analysts soll der weltweite Gesamtmarkt für Datenbank-, Speicher- und Backup-Software von 172,3 Milliarden Dollar im Jahr 2020 jährlich um 11,8 Prozent auf 375,5 Milliarden Dollar im Jahr 2027 steigen. Der Trend zu Cloud Computing kommt den Marktforschern zufolge auch im Speichermarkt überproportional zum Tragen. Global soll der Cloud-Speichermarkt, der im Jahr 2020 auf 84,2 Milliarden Dollar geschätzt wurde, bis 2027 jährlich mit durchschnittlich 20,8 Prozent fast doppelt so stark auf 315 Milliarden Dollar anwachsen. Demgegenüber stehen die Ausgaben für herkömmliche Backup-Speicher, die zwischen 2020 und 2027 von 116,4 Milliarden Dollar um durchschnittlich gerade mal 3,8 Prozent auf 151 Milliarden wachsen. Glaubt man den weltweiten Befragungen, dürfte demzufolge innerhalb weniger Jahre bis 2027 die Verteilung zugunsten der Cloud-Backups mit einem Verhältnis von zwei zu eins resultieren.

Ein Viertel der Datensicherung schon in der Private Cloud

Dass der Trend zur Verlagerung von Datacenter-Kapazitäten in die Cloud auch Auswirkungen auf die Storage-Lösungen hat, zeigen Schweizer Zahlen von Profondia. Das Marktforschungsunternehmen erhebt Daten über die ICT-Infrastruktur bei über 13'000 Unternehmen. Bei der Betrachtung der Storage-Anteile wurden allerdings nur Firmen berücksichtigt, die zehn oder mehr physische oder virtuelle Server einsetzen oder mehr als 100 PC-Arbeitsplätze in der Schweiz haben. Ermittelt wurden Daten über die Marktdurchdringung einzelner Hersteller und Technologien. Demzufolge führten bei den befragten Unternehmen Synology (18 Prozent), HPE (17 Prozent), Dell EMC (11 Prozent), Netapp (9 Prozent), Qnap (7 Prozent), IBM (3 Prozent) und Hitachi (1 Prozent) die Liste der

BEISPIELE HEUTE GÄNGIGER BACKUP-VARIANTEN



DR-Plan = Data-Recovery-Plan; VM = Virtual Machine

Quelle: UMB

Egal ob Backup mit Private oder Public Cloud, die Datensicherung sollte heute immer die Unveränderbarkeit der Daten garantieren («immutable» oder WORM).

meisten installierten Produkte der SAN- und NAS-Hersteller an. 9 Prozent verfielen auf andere Anbieter. Der Anteil für Managed Cloud Storage hingegen, die nicht im eigenen Rechenzentrum, sondern bei einem Private-Cloud-Anbieter gehostet werden, wuchs gegenüber dem Vorjahr um 3 Prozent auf 24 Prozent. Über die Anteile der Hyperscaler gibt der Report keine Auskunft.

Die wichtigsten Backup-Faustregeln

Storage- und Backup-Strategien gibt es viele. Welche gewählt wird, hängt immer von den jeweiligen Anforderungen und Umständen des einzelnen Unternehmens ab. Für die Festlegung einer Strategie muss beurteilt werden, wie kritisch welche Unternehmensdaten für den Fortbestand der Geschäftstätigkeit sind respektive wie riskant der Verlust der unterschiedlichen Daten im Falle eines Datenproblems wäre. Schlussendlich müssen die Risiken dem finanziellen Aufwand gegenübergestellt werden. Als Faustregeln können folgende Grundsätze herangezogen werden. Sie haben im Zuge der steigenden Bedrohungen der Datensicherheit mehr denn je Gültigkeit:

- Zwingend einen Notfallplan erarbeiten: Ein einzelnes System stellt noch keine grosse Herausforderung dar. Müssen aber zum Beispiel nach einem Wasserschaden oder Feuer gleichzeitig viele Systeme wiederhergestellt werden, ist es wichtig zu wissen, welche priorisiert werden müssen. Wo gibt es Abhängigkeiten, wo können die grössten Schäden für das Business entstehen – dies sind Fragen, die beantwortet und für den Notfall sauber dokumentiert sein müssen.
- Mindestens einmal täglich ein Backup für produktive Systeme und
- mindestens einmal wöchentlich ein Full-Backup (aktiv oder synthetisch, siehe Kasten) erstellen.
- So häufig wie nötig Log-Backups von Datenbanken. Die Frage stellt sich hier, wieviel Zeit man verlieren darf, wenn die Daten nicht verfügbar sind. Bei hochkritischen Datenbanken darf ein Verlust von Log-Daten vielleicht zehn Minuten betragen. Das Log-Daten-Backup muss dann also alle zehn Minuten erfolgen. Bei weniger kritischen Datenbanken wie etwa solchen für Inventare von Umgebungen reicht üblicherweise eine tägliche Sicherung.
- Befolgen der 3-2-1-Regel: Von den zu schützenden Daten sollen mindestens drei aktuelle Version bestehen. Neben dem Original werden zwei Kopien auf zwei verschiedenen Arten von Speichermedien gespeichert und eine Kopie an einen externen Standort geschickt.
- Die logische Weiterentwicklung resultiert in der Formel 3-2-1-1-0. Die zweite 1 stellt eine weitere Kopie dar, die entweder offline (in einem Tresor) oder sogenannt «immutable» aufbewahrt wird. Somit sind die Daten sicher vor böswilliger Veränderung oder Diebstahl geschützt.
- Die Ziffer 0 in der oben genannten Formel bedeutet, dass keine fehlerhaften Backups existieren dürfen. Oder anders gesagt: Die Funktionsfähigkeit des Backups muss zwingend auch validiert und bei Fehlern entsprechend reagiert werden. Das geschieht über Alarmierungsmassnahmen oder manuelle, visuelle Kontrollen. Die Einhaltung von «3-2-1-1-0» wird angesichts der steigenden Bedrohung durch Cyberangriffe und insbesondere im Zuge der Verlagerung in die Public Cloud für immer mehr Unternehmen zur Pflicht.

Top-Trend Unveränderbarkeit

Dass Erpresser den Zugriff auf die Firmendaten, deren Nutzung oder gar das ganze System verunmöglichen und gravierende Schäden verursachen können, ist ein Schreckensszenario, mit dem mittlerweile Unternehmen jeder Grösse und Branche rechnen müssen. Unabhängig davon, welche Methode man für seine Backup-Strategie herbeizieht (s. Kasten) und wie die Architektur (s. Grafik) dafür aufgebaut wird, ist deshalb nach den sich in den letzten Monaten und Jahren häufenden Cyberangriffen durch Ransomware eine wichtige Erkenntnis gereift: Die Unveränderbarkeit der Daten muss eine Schlüsselrolle in Backup-Szenarien einnehmen. Denn durch entsprechende Vorkehrungen kann ein Angreifer auch mit einem gehackten Admin-Account den Daten nichts anhaben. Während unveränderliche Backups in gewissen Bran-

STORAGE-METHODEN: DIE QUAL DER WAHL

Bei der Wahl der Backup-Methode müssen Vor- und Nachteile der jeweiligen Konzepte in Betracht gezogen werden. **Vollständige Backups** bauen auf einer differenziellen oder inkrementellen Vorgehensweise auf. Bei einem **differenziellen Backup** werden die Daten, die seit der letzten Sicherung verändert wurden, kopiert. Bei einem vollständigen Backup am Montag werden demzufolge am Dienstag alle Dateien, die im Verlauf des Tages verändert wurden, gespeichert. Am Mittwoch werden alle seit dem Montag veränderten Daten kopiert, und so weiter. Das hat den Vorteil, dass man im Problemfall auf das (wöchentliche) Full Backup und das aktuellste differenzielle Backup zurückgreifen kann. Der Nachteil liegt beim ständig wachsenden Datenvolumen, das wegkopiert werden muss. Mit dieser Methode wird das für die Datensicherung nötige Zeitfenster dauernd verlängert und der Speicherplatz kann an seine Grenzen stossen.

Bei einem **inkrementellen Backup** wiederum werden nur die Inkremente, also die Daten, die sich an einem Tag seit dem letzten Backup verändert haben, gesichert. Bei einem Full Backup am Montag werden also die am Dienstag veränderten Dateien gespeichert, am Mittwoch diejenigen, die sich seit Dienstag verändert haben und so weiter. Die täglich zu kopierende Datenmenge ist damit kleiner als bei einem differenziellen Backup, das Zeitfenster kürzer und der Platzbedarf geringer. Die Kehrseite der Medaille ist, dass im Notfall eine Wiederherstellung aufwendiger wird, denn es werden das letzte vollständige und alle inkrementellen Backups dafür benötigt.

Ein **synthetisches Voll-Backup** enthält die gleichen Daten wie eine aktive Vollsicherung. Der einzige Unterschied besteht darin, wie die neue Sicherung erstellt wird. Anstatt Quelldaten zu kopieren, enthält die synthetische Vollsicherung die unveränderten Daten der Quelle sowie alle inkrementellen Sicherungen der geänderten Daten. Mit dieser Methode kann die Menge der hochgeladenen Daten reduziert und die Dauer für die Erstellung einer Vollsicherung verkürzt werden.

Mit **rückwärts (reverse) inkrementellem Backup** kann eine Sicherung ohne zusätzliche Verarbeitung auf dem letzten Stand wiederhergestellt werden, da der letzte Wiederherstellungspunkt eine vollständige Backup-Datei ist. Es wird standardmässig eine synthetische Vollsicherung durchgeführt. Die Inkremente werden jedoch beibehalten, um eine Wiederherstellung zu einem bestimmten Zeitpunkt zu ermöglichen.

chen schon früher notwendig waren, um gesetzliche Vorgaben oder Compliance-Richtlinien zu erfüllen, müssen mittlerweile Technologien für Immutable Backup für jedes Unternehmen zum Standard werden, damit Datensicherungen gegen böswillige Verschlüsselung, Manipulation oder (auch versehentliche) Löschung geschützt und Erpressungsversuchen vorgebeugt werden können.

Neben den schon seit vielen Jahren bekannten physischen Methoden für sogenannte WORM-Medien (Write Once Read Many), die ein Verändern der gespeicherten Daten zum Beispiel mit Schreiben auf CDs oder DVDs ermöglichen, gibt es auch Software-basierte und systemische Methoden. Dabei wird bei eigentlich wiederbeschreibbaren Medien wie Magnetbändern oder Festplatten eine Veränderung der Daten ebenfalls verhindert. Während man damit aber in der Vergangenheit vor allem Dateien wie etwa Verträge, Belege, Archivdaten und ähnliches für die Langzeitsicherung speicherte, sind sie angesichts der steigenden Bedrohung durch Erpresser mittlerweile für die Backup-Routine von proprietären und business-relevanten Applikationen im Tagesgeschäft notwendig geworden. WORM-Funktionalitäten werden immer häufiger auch auf Speichersystemen angeboten und da rein mit Software gelöst. In diesem Fall spricht man von Software-WORM oder Soft-WORM.

Backup nach S3

Das S3-Protokoll eröffnet eine weitere Möglichkeit, grosse Datenmengen gegen Veränderbarkeit zu schützen. Das ursprünglich von Amazon AWS für Objekt-Speicherung über ein Webinterface in der Cloud ins Leben gerufene Protokoll wird mittlerweile von allen Backup-Anbietern unterstützt und hat im letzten Jahr zunehmend an Bedeutung gewonnen. Es kann direkt aus der Backup-Software adressiert werden, um über die S3-Programmierschnittstelle aus Anwendungen Daten in einen Objektspeicher zu laden. Ausserdem können Regeln festgelegt werden, zum Beispiel dass Daten während einer festgelegten Zeit geschützt und danach gelöscht werden. Wie bei herkömmlichen WORM-Methoden gilt auch hier: S3 Storage kann Mehrkosten verursachen, weshalb es unabhängig von Branche oder Firmengrösse dort eingesetzt wird, wo business-relevante Daten geschützt werden müssen. Amazon S3 Object Lock verhindert, dass Objektversionen (versehentlich oder absichtlich) gelöscht oder verändert werden können. S3 Object Lock ist der Branchenstandard für die Unveränderbarkeit von Objektspeichern zum Schutz vor Ransomware und wird in Cloud-Speicher-, Sicherungs- und Datenschutzlösungen von Amazon-AWS-Partnern wie Commvault, Veeam, Veritas, Rubrik, Cohesity und vielen weiteren Anbietern eingesetzt.

Datensicherung ist nicht gleich Datensicherheit

Der Trend zu Cloud Computing hat insbesondere bei kleineren Kunden dazu geführt, dass neben den Rechenzentren in einer Public Cloud auch gleich das Backup bei einem Hyperscaler gewünscht wird. In gewissen Fällen kann es schon auch mal vorkommen, dass keine dritte Sicherungskopie mehr hergestellt wird. Solche Szenarien sollten dann aber erst recht mitberücksichtigen, dass Datensicherung nicht automatisch Datensicherheit garantiert. Denn immer häufiger werden auch kleinere Unternehmen Opfer von Datendiebstahl und Erpressungsversuchen. Die Unveränderbarkeit der Daten zu gewährleisten und einen Datenwiederherstellungsplan zu haben, bleibt deshalb auch für Firmen Pflicht, die sich ganz der Public Cloud verschreiben. Allgemein erhöhen Multi- und hybride Cloud-Umgebungen die Komplexität der Datensicherung. Es bedarf deshalb Lösungen, die leicht zu bedienen sind und eine durchgängige Kontrolle des gesamten Datenbestands ermöglichen – von lokalen, eigenen Ressourcen über solche bei Dienstleistern in privaten Clouds bis hin zu Public Clouds der Hyperscaler. Unternehmen sollten sich deshalb gut mit den verschiedenen Speichermodellen, deren Vorteilen und Einschränkungen vertraut machen. Denn wer allein auf den Preis für die Datensicherung schaut, kann bei einem Notfall böse Überraschungen erleben. Das Wegkopieren von Daten ist auf den ersten Blick manchmal verlockend günstig. Teuer wird's dann aber meistens, wenn die Daten (auch mehrmals) wiederhergestellt werden müssen. Unabhängige kleinere Anbieter können mit ihren Privaten Clouds besser als Hyperscaler auf spezielle Wünsche der Kunden eingehen, etwa spezielle Aufbewahrungsfristen oder Backup-Häufigkeiten gewähren oder aus der Cloud eine zusätzliche Backup-Kopie auf Tape für den Tresor in das Angebot einbauen. Schlussendlich müssten sich aber Kosten und Nutzen die Waage halten. Auf jeden Fall gilt: Immer auch das Kleingedruckte lesen. ■

DER AUTOR

Mario Amodio ist seit 2015 für UMB tätig und leitet seit 2016 das Team Data Management. Er war vorher Backup Engineer beim Schweizer IT-Dienstleister Osys und ist durch die Integration des Unternehmens zu UMB gestossen. Der IT-Dienstleister UMB betreibt IT-Infrastrukturen für Kunden aus verschiedensten Branchen, darunter geografisch getrennte Rechenzentren für das Backup von Kundendaten.