storage-magazin.de

Ausgabe **2-2021**

Eine Publikation von **speicherguide.de**

Foto: iStockphoto.com / Erich Fend

Backup für den Mittelstand

Marktüberblick Backup-Software

Datensicherungsstrategie: Wichtiger denn je!

Karl Fröhlich, Chefredakteur speicherguide.de

Liebe Leserinnen und Leser,

beim Thema Backup & Recovery erlebe ich irgendwie ein dauerhaftes Déjà-vu. Es gibt schon laufend etwas Neues, aber im Kern schreibe ich seit Jahrzehnten immer wieder das Gleiche. Einerseits sind wir schon darüber hinweg, Aufklärung zu betreiben, warum ein Backup überhaupt notwendig ist. Andererseits belegt eine Studie, 54 Prozent aller Backups schlagen fehl. Das kann doch nicht sein!?

Ausfälle sind keine Seltenheit: Fast alle der befragten deutschen Unternehmen hatten in den letzten zwölf Monaten damit zu kämpfen und bei jedem vierten Server gab es im vergangenen Jahr mindestens einen unerwarteten Ausfall. Genau aus diesem Grund treffen wir Vorkehrungen, dass der Betrieb ungehindert weiterlaufen kann, keine Daten verlorengehen und sich bei Bedarf zügig wiederherstellen lassen.

Der Wille zur Modernisierung ist vorhanden, jedoch sehen 29 Prozent die wirtschaftliche Unsicherheit als Hindernis. Dies ist grundsätzlich verständlich, nur sollte eine mangelhafte Datensicherungsstrategie nicht noch für extra Schaden sorgen.

Natürlich ist Corona so etwas wie eine Blutgrätsche, für unseren beruflichen wie privaten Alltag. Die wirtschaftlichen Folgen sind nicht abzusehen. Quasi über Nacht mussten mobile Arbeitsplätze ins Backup integriert werden. Gleichzeitig öffnete dies unzählige ungesicherte Einfallstore. Für Ransomware & Co ist Corona ein Glücksfall.

Weltweit fallen alle 14 Sekunden Unternehmen einem Ransomware-Angriff zum Opfer. Der dabei entstehende Schaden beziffert sich auf über 10,6 Milliarden Euro, mit steigender Tendenz. Betroffen sind Firmen jeder Größe. In meinem engeren Bekanntenkreis arbeitet beispielsweise jemand im Raum Augsburg bei einem Zulieferer für Medizinprodukte. Für Außenstehende ein unscheinbares Unternehmen, welches sich mit einer zweistelligen Millionensumme(!) von einem Hackerangriff freikaufen musste.

Nicht zuletzt wegen Ransomware ist Tape plötzlich wieder eine Hype-Technologie. In dieser Ausgabe schauen wir unter anderem auf LTO, welche Abwehrmaßnahmen gegen Ransomware zu treffen sind und was alles in ein IT-Notfallhandbuch gehört. Zudem geben wir einen Überblick über die wichtigsten Backup-Software-Produkte.

Außerdem möchte ich Ihnen unsere Kongress-Plattform und On-demand-Mediathek ans Herz legen. Dort finden Sie eine breite Auswahl an Vorträgen zu Backup & Recovery, Data-Protection und IT-Sicherheit.

Ihr Karl Fröhlich, Chefredakteur speicherguide.de

Inhalt

FAST LTA
Wir sichern Petabytes.

Setzen Sie immer noch auf **Tape** für Ihr **Backup** ?

Weil man Ihnen erzählt, Tape wäre **günstiger**, **sicherer**, „mit klarer **Roadmap**“, und „**ohne Tape geht es nicht**“?

Zeit für einen **Faktencheck**.

Komplettes, modernes und flexibles Backup – ganz ohne Tape. Dafür inklusive Flash-Speicher, flexibler Skalierbarkeit, Air Gap und S3 Object Store.
Made in Germany.

Silent Bricks.

https://fastlta.com/faktencheck

Problemfall Datensicherung

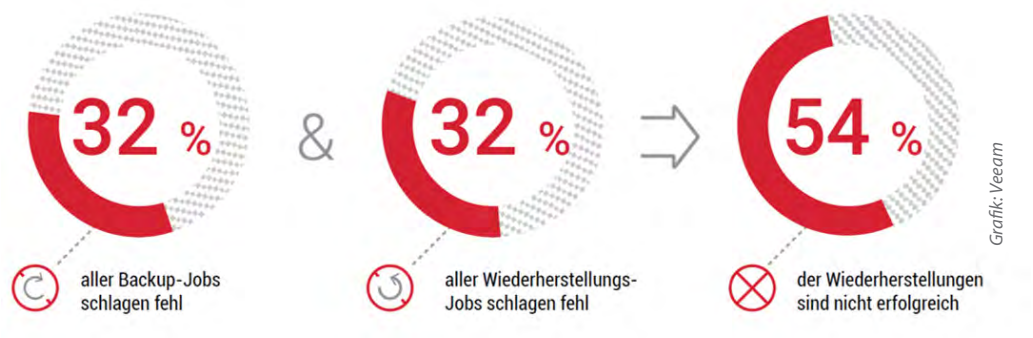
54 Prozent aller Backups schlagen fehl

Von 100 Versuchen deutscher Unternehmen, gesicherte Daten wiederherzustellen, misslingen 54. Der Wille zur Modernisierung ist vorhanden, jedoch sehen 29 Prozent die wirtschaftliche Unsicherheit als größtes Hindernis.

■ Michael Baumann

Laut dem ***Veeam*** *Data Protection Report 2021* beeinträchtigen Probleme mit der Datensicherung Unternehmen dabei, Maßnahmen zur digitalen Transformation (DX) umzusetzen.

Nach Angaben der 302 deutschen Umfrageteilnehmer sind die wichtigsten Aspekte einer modernen Backup-Lösung integrierte Features für Datensicherung und Sicherheit (34 Prozent), Portabilität für Cloud-Workloads (40 Prozent) und die Möglichkeit einer Cloud-basierten Disaster-Recovery (36 Prozent). Darüber hinaus sind unerwartete Ausfälle keine Seltenheit: 95 Prozent der Unternehmen hatten in den letzten zwölf Monaten damit zu kämpfen und bei jedem vierten Server gab es im vergangenen Jahr mindestens einen unerwarteten Ausfall.



Krisengebiet Backup – deutsche Unternehmen kämpfen mit dem Erfolg ihrer Datensicherungen.

Cloud-basiertes Backup auf dem Plan

In den nächsten zwei Jahren erwarten die meisten Unternehmen, dass die Hälfte der Produktions-Workloads bis 2023 in der Cloud gehostet wird.

Entsprechend verlagert sich die Datensicherung von On-Premises- zu Cloud-basierten Lösungen. Dies geschehe bei mit einem erwarteten Wachstum von 29 Prozent im Jahr 2020 auf voraussichtlich 46 Prozent im Jahr 2023. Dabei ist die Verbesserung der Backup-Zuverlässigkeit für 31 Prozent der Unternehmen ein Hauptgrund zu wechseln. 80 Prozent der Unternehmen bestätigen eine »Verfügbarkeitslücke« zwischen der tatsächlichen und der eigentlich angestrebten Dauer für die Wiederherstellung von Anwendungen. 76 Prozent bemängeln eine »Datensicherungslücke« zwischen der Häufigkeit der Datensicherung und dem tolerierbaren Datenverlust bei Ausfällen.

Als Lösung planen 46 Prozent der Unternehmen bis 2023 mit einem Backup-as-a-Service-Anbieter (BaaS) zusammenarbeiten und 51 Prozent planen, im gleichen Zeitraum Disaster-Recovery-as-a-Service (DRaaS) einzuführen.

Corona und die Auswirkungen

28 Prozent der Befragten legten Pläne zur digitalen Transformation auf Eis. In den ersten Monaten der Pandemie nutzten 92 Prozent der Unternehmen Cloud-Services in deutlich größerem Umfang als zuvor. Dies lag vor allem daran, dass Mitarbeiter im Home-Office SaaS-Lösungen für die Zusammenarbeit nutzten und die Aufrechterhaltung des Betriebs physischer Systeme in der lokalen Umgebung für die IT schwieriger wurde. ■

Weitere Informationen

Lesen Sie eine ausführliche Fassung zur Veeam-Studie auf speicherguide.de

Gezielte Cyberattacken setzen Unternehmen unter Druck

Backups alleine schützen nicht mehr vor Ransomware

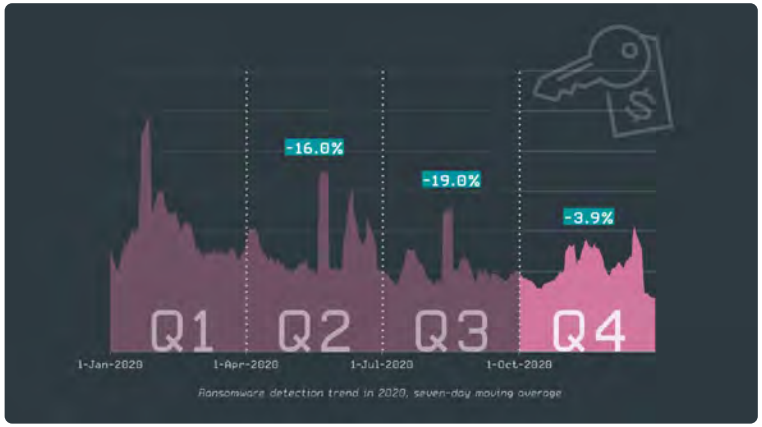
Ransomware-Angriffe richten sich immer häufiger und immer gezielter gegen Firmen. Die Angreifer wissen genau was sie tun und kennen die Sicherheitsvorkehrungen ihrer Opfer teilweise sehr präzise. Sich bei der Widerherstellung ganz auf das klassische Backup zu verlassen, kann sich daher als fataler Fehler erweisen.

■ Peter Marwan

Mindestens 10,1 Milliarden Euro konnten Kriminelle 2019 mittels Ransomware von Firmen erpressen, berichtete die **European Union Agency for Cybersecurity** (ENISA) im Oktober 2020. Das waren 3,3 Milliarden mehr als 2018. Grund für die Zunahme ist, dass Angreifer immer häufiger finanzkräftige Opfer auswählen. Das bestätigen auch das **Bundeskriminalamt** (BKA) im »Bundeslagebild Cybercrime 2019« und **IBM** im »2021 X-Force Threat Intelligence Index«. 2020 entfielen demnach 23 Prozent aller Cyberattacken auf Ransomware – mehr als auf jede andere Angriffsart. Dem Mitte März veröffentlichten »Unit 42 Ransomware Threat Report« zufolge verdoppelte sich zudem der durchschnittlich als Lösegeld für ihre Daten von Unternehmen bezahlte Betrag von 115.123 (2019) auf 312.493 US-Dollar (2020). Zum Vergleich: 2015 lag, **Symantec** zufolge, eine durchschnittliche Forderung noch bei 294 US-Dollar.

Prominente Ransomware-Opfer im vierten Quartal 2020 waren **Honda**, **Mattel**, bereits zum zweiten Mal der italienische Energiekonzern **Enel**, der US-Buchhändler **Barnes & Noble**, die Zeitarbeitsfirma **Randstad**, der Spieleentwickler **Ubisoft**, der US-Einzelhändler **Kmart** und der Haushaltsgerätehersteller **Whirlpool**. Man sieht: Keine Branche ist vor den Angriffen sicher – auch wenn Einrichtungen des Gesundheitswesens in der Vergangenheit besonders oft betroffen waren. Laut ENISA stellten von ihnen 2019 zwei Drittel eine Ransomware-Attacke fest.

Experten fordern seit Jahren, bei Ransomware-Angriffen keinesfalls Lösegeld zu zahlen, um die Kriminellen nicht noch zu ermutigen. Einer Studie der **Cyber Edge Group** zufolge hielten sich 45 Prozent der Firmen nicht daran. Allerdings bekam nur etwa die Hälfte tatsächlich wieder Zugriff auf ihre Daten. Ein weiteres Problem heißt *Double Extortion*. Dabei ziehen Angreifer Daten ab, bevor sie IT-Systeme ihrer Opfer verschlüsseln, und drohen damit, die Daten zu



Grafik: Eset

Security-Anbieter Eset hat 2020 immer weniger, dafür immer zielgerichtetere Ransomware-Attacken auf Firmen dokumentiert.

Grafik: Unit42/Palo Alto Networks

Table 1: Costs Associated with Ransomware Incidents in 2020 in the US, Canada, and Europe (US$)

	2020 Data	Earlier Data (Where Available)
Avg. ransom demand	$847,344	–
Avg. ransom paid	$312,493	$115,123 (2019)
Highest ransom demand	$30,000,000	$15,000,000 (2015–2019)
Highest ransom paid	$10,000,000	$5,000,000 (2015–2019)
Lowest ransom demand	$1,000	–
Avg. cost of forensic engagement	$73,851	$62,981 (2019
Avg. cost of forensic engagement, small and midsize business	$40,719	–
Avg. ransom demand, small and midsize business	$718,414	–
Avg. cost of forensic engagement, large enterprise	$207,875	–
Avg. ransom demand, large enterprise	$2,923,122	–

Die abgestuften Lösegeldforderungen der Angreifer belegen, dass sie inzwischen sehr genau wissen, wen sie erpressen und was sie dabei herausholen können.

veröffentlichen. »Damit werden die Betroffenen unter verstärkten Druck gesetzt, die Lösegeldsummen zu zahlen. Hier ist nicht nur die Verfügbarkeit der kryptierten Daten bedroht, sondern auch deren Vertraulichkeit«, fasst das BKA zusammen.

Seit Jahren betonen Experten, wie wichtig Backups sind, um nach einem Ransomware-Befall die Systeme wieder herstellen zu können. Aber regelmäßige Backups alleine reichen nicht aus. »Fortschrittliche Ransomware-Varianten sind in der Lage, auch auf Backups zuzugreifen und diese ebenfalls zu verschlüsseln«, warnt das BKA. Daher sei es empfehlenswert, Offline-Backups zu führen, die nicht jederzeit per Netzwerk oder File-Shares erreicht und damit verschlüsselt oder überschrieben werden können.

Angebote für solche eine Sicherungsstrategie mit einem Medienbruch haben etwa **Fast LTA** oder **Actidata**. Alternativ bieten sich Lösungen wie *Amazon S3 Object Lock* oder *Blocky for Veeam* an, letzteres eine gemeinsame Entwicklung von **Grau Data** und **Cristie Data**. Sie sorgen dafür, dass Backups nicht überschrieben und damit auch nicht von Ransomware verschlüsselt werden können. ■

Weitere Informationen

Lesen Sie eine ausführliche Fassung dieses Beitrags speicherguide.de

Proaktive Maßnahmen zur Überwindung der Ransomware-Bedrohung

Raus aus der Ransomware-Falle

Ransomware stellt eine der größten Bedrohungen für Unternehmen dar. Es reicht nicht mehr aus, einfach Cybersecurity-Software zu installieren und weiter auf eine vorhandene Backup-Lösung zu setzen. Der Backup- und Recovery-Plan muss im Lauf der Zeit weiterentwickelt und regelmäßig angepasst werden.

Ines Wolf, Quantum

Gemeinsam mit Malware und Phishing stellt Ransomware mittlerweile die mit Abstand größte Bedrohung für Unternehmen dar. Sie ist damit gefährlicher als Naturkatastrophen, Hardware-Ausfälle oder selbst eine Zero-Day-Attacke. Um dagegen vorzugehen setzen viele Unternehmen auf Cybersecurity-Software, um Hacker-Angriffe abzuwehren. Damit ist aber erst die Hälfte gewonnen. Ebenso wichtig ist die Storage- und Backup-Infrastruktur.

Allerdings werden Sicherheitsrichtlinien und Backup-Strategien allzu oft vernachlässigt. So haben Angreifer ein leichtes Spiel, wenn es darum geht, Lösegeld für Daten zu erpressen. Den Unternehmen bleibt meist keine andere Wahl als zu zahlen, da es ihr einziges Ziel ist, die Daten schnellstmöglich wiederherzustellen und zum normalen Betrieb zurückzukehren. Sie setzen daher oft auf den Abschluss einer Cyberversicherung, unter deren Schirm die Zahlungen ausgehandelt werden, sodass im Anschluss die regulären Abläufe wieder etabliert werden können.

Der richtige Ansatz wäre, dass Unternehmen proaktiv gegen die Attacken vorgehen und einen robusten Datenschutzplan erstellen. Es reicht heute nicht mehr aus, einfach weiter auf eine vorhandene Backup-Infrastruktur zu setzen. Ein Backup- und Recovery-Plan muss im Lauf der Zeit weiterentwickelt und regelmäßig angepasst werden.

Checkliste für die Absicherung des Unternehmens und seiner Daten

1. Erarbeiten Sie eine gut überlegte Strategie zur Datensicherung.
2. Stellen Sie den Plan Ihren Vorgesetzten vor, um deren Zustimmung und Unterstützung zu erhalten.
3. Installieren Sie eine Antivirussoftware, um die »Vordertür« des Netzwerks zu schließen.
4. Nutzen Sie Verschlüsselungstechnologie in jeder Phase des Lebenszyklus Ihrer Daten – für die Ablage, während der Übertragung und bei der aktiven Nutzung.
5. Bieten Sie Sicherheitsschulungen an und fördern Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter.
6. Implementieren Sie lokale Disk-Backups mit File-/Objektsperre, um die schnelle lokale Wiederherstellbarkeit zu gewährleisten und Ihre RPO/RTO-Vorgaben zu erfüllen.
7. Replizieren Sie die Daten für DR-Zwecke mithilfe einer Cloud- oder Object-Storage-basierten Lösung an einen entfernten Standort.
8. Implementieren Sie eine Tape-Lösung als lokalen »Air-Gap«-Schutz für Ihre Backups oder Archive.
9. Schließen Sie als letzten Ausweg eine Cyberversicherung ab.

Der Schutz der Daten vor Cyberattacken beginnt mit dem Offensichtlichen. Prüfen Sie, ob Backup-Software und -Ziele die nötigen

Tape-Speicher: der kosteneffizienteste Schutz vor Ransomware

Foto: Quantum

Voraussetzungen erfüllen, um Ihre RPO- und RTO-Vorgaben zu erfüllen und die Sicherheit Ihrer Daten zu gewährleisten. Wenn Ihre Backup-Software keinen Schutz vor Ransomware bietet, so ist sie vielleicht nicht die richtige Lösung für Sie.

Auswahl der richtigen Storage-Lösung: welche Plattform ist die richtige?

Der Vorteil von NAS-Lösungen liegt (je nach SLAs) in der schnellen Wiederherstellung. Allerdings bleiben die Daten dabei immer online. Damit ist es nur eine Frage der Zeit, bis Kriminelle eine Möglichkeit finden, den operativen »Air-Gap«-Schutz (also die Lücke zwischen Produktionsspeicher und unerreichbarem Speicher) zu überwinden. Viele Anbieter wenden unterschiedliche Methoden an, um die Objekte oder Dateien in den Systemen »einzusperren«. Da die Daten aber immer online sind, lässt sich das Risiko nicht komplett ausschließen. Letztlich lassen sich die Daten nach einem Angriff aber mit dieser Verteidigungsmethode am schnellsten wiederherstellen.

Als Offline-Speichermedium bietet Tape einen physischen »Air Gap«-Schutz. Die Daten sind vor Ransomware sicher, da Angreifer die physische Barriere zwischen den Daten und dem Netzwerk nicht überwinden können. Tape spielt dabei eine zentrale Rolle, da die Technologie nicht nur einen physischen Schutz Ihrer Daten bietet, sondern zudem eine kostengünstige langfristige Archivierung Ihrer Daten ermöglicht.

Object-Storage verteilt die Daten auf mehrere Nodes und sperrt sie, sodass keine Änderungen möglich sind. Je nach Lösung können Object-Storage-Daten auch nach dem Ausfall einzelner oder mehrerer Nodes bereitgestellt werden.

Backups für Ihr Backup – Datensicherung nach dem 3–2–1–1-Prinzip

Als robuste Strategie zur Datensicherung empfiehlt sich die Backup-Erstellung nach dem 3–2–1–1-Prinzip. Diese sieht vor, drei Kopien der Daten auf zwei unterschiedlichen Medienformaten aufzubewahren sowie eine Kopie extern vorzuhalten und eine Kopie offline. Dieser Ansatz ähnelt der 1–10–60-Regel, nach der Sicherheitsteams Bedrohungen in der ersten Minute erkennen, die Bedrohung innerhalb von zehn Minuten verstehen und dann innerhalb von 60 Minuten darauf reagieren sollen. In beiden Fällen wird eine proaktive Strategie benötigt, um akuten Bedrohungen einen Schritt voraus zu sein. ■

Weitere Informationen

Quantum Böhmenkirch GmbH & Co. KG
Willy-Brandt-Allee 4, 81829 München
Tel. +49 89 94 303–0
E-Mail: info.de@quantum.com

Informationen zu den Quantum Ransomware-Lösungen

Sehen Sie sich unser On-Demand-Webinar an

Tape bleibt kostengünstigstes Speichermedium

LTO-9: Flaggschiff (noch nicht) am Horizont

Für die nächste LTO-Generation wurden erst im Herbst die Spezifikationen final festgelegt, und damit die Roadmap wieder einmal nach unten korrigiert. Begründet wurde dies vom Hersteller-Konsortium mit einer schnelleren Marktreife von LTO-9. Allerdings werden sich die Anwender auf absehbare Zeit noch mit dem Vorgänger der achten Generation begnügen müssen.

■ Michael Baumann

Die großen Hyperscaler und Public-Clouds mit ihren riesigen Storage-Farmen sind heute die größten Abnehmer von Tape als Kapazitätsspeicher. Bänder sind aber auch in herkömmlichen Rechenzentren das kostengünstigste Medium pro TByte und die letzte Verteidigungslinie gegen Gefahren wie Cyberkriminalität. Selbst Unternehmen, die bereits vollständig zur Disk gewechselten waren, kehren zum Tape zurück als »Cold Data«-Online-Speicherklasse, Offline-Backup und Archivierungsmedium.

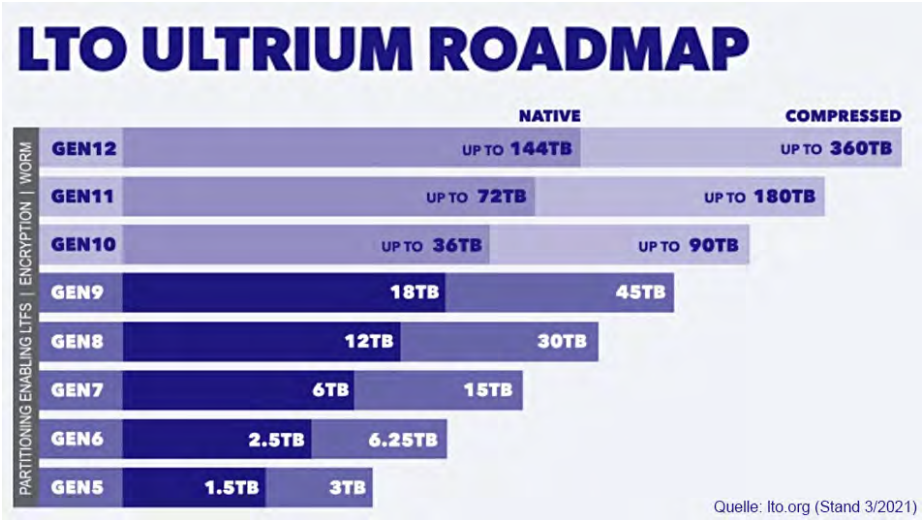
Der aktuelle Bandstandard LTO-8 ist seit Oktober 2017 auf dem Markt. Gegenüber der Vorgänger-Generation hatte sich die unkomprimierte Speicherkapazität von sechs auf zwölf TByte verdoppelt. In Aussicht steht mit LTO-9 jetzt nicht mehr die traditionelle und angestrebte Verdoppelung, sondern 18 TByte pro Tape. Die Performance-Historie sieht derzeit 300 MByte/s (LTO-7), 360 MByte/s (LTO-8) und 400 MByte/s (LTO-9) vor. Diese Angaben basieren auf unkomprimierten Daten, ungeachtet der inzwischen üblicherweise eingerechneten 2,5:1-Komprimierung.

2015, 2017…2021?

Die letzten Generationen kommen für die Massenfertigung dabei eher entschleunigt auf den Markt: 2015, 2017 und im besten Fall 2021. Der letzte relevante LTO-Entwickler **IBM** präsentierte im Labor auch Tapes mit 580 TByte pro Cartridge und geht nach wie vor davon aus, dass die Tape-Kapazität wie in der Vergangenheit um rund 34 Prozent jährlich gesteigert werden kann. Dies entspräche dem allgemeinen Datenwachstum. Diese Art Monster-Tape wird jedoch erst in acht bis zehn Jahren Produktreife erlangen. Tape-Entwicklung und -Herstellung biete zudem annähernd konstante Produktionskosten und damit entsprechend sinkende Preise pro TByte. Die Disk-Entwicklung dagegen sei dazu weder kapazitiv noch im Preis-/Leistungsverhältnis in der Lage, weil geringere Fortschritte dort in immer teurere Technologie-Kosten münden würden. Ob diese Kapazitäts-/Zeit-Kalkulation so aufrechterhalten werden kann, wird sich in Zukunft erst zeigen.

Die Markteinführung ist für Sommer angedacht, damit plant man beispielsweise bei **Fujifilm**.

Wir hören von manchen Anbietern, dass LTO-9 frühestens Mitte/Ende des Jahres in größeren Stückzahlen und den Einbau in



LTO-9 mit einer Kapazität von 18 TByte wird für Mitte / Ende 2021 erwartet.

Automationslösungen verfügbar werden wird. Andere haben bereits offiziell verlautbart, dass sie Bestellungen für Automation-Produkte aufnehmen.

LTO-9: Stabiler Fortschritt, wenig Neuerungen

Bis dahin bleibt die Version 8 das Flaggschiff der Flotte, also 30 TByte und 750 MByte/s mit besagter 2,5:1-Kompression. LTO-8 unterstützt SDLC-Datenkomprimierung, Hardware-Verschlüsselung (AES-256-Bit), 8-Gbit-FC- und 6-Gbit-SAS-Schnittstellen, 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 und in hierarchisierte Umgebungen mit kalten und warmen Daten integrieren.

LTO-9 wird all diese Leistungsmerkmale auch mitbringen. An technischen Neuerungen sind darüber hinaus keine Wunder zu erwarten. Laut Spezifikationen sollen LTO-9-Laufwerke standardmäßig mit dualen 12-Gbit/s-SAS-Schnittstellen (zuvor 6 Gbit/s) ausgestattet werden. Allerdings wurde offenbar an der Robustheit gegen Lesefehler gearbeitet, die Tapes häufiger nachgesagt wird. Die URE-Rate (Unrecoverable Read Errors) der neuen Generation soll von 10^{19} auf 10^{20} exponentiell verbessert worden sein.

Kosten- und Entscheidungsfaktor Rückwärtskompatibilität

Beide Versionen sind jeweils nur eine Generation rückwärtskompatibel. Für Nutzer bedeutet dies, dass gegebenenfalls große Datenmengen migriert werden müssen. Ältere Archiv-Tapes benötigen ein funktionierendes Laufwerk. In einer TCO-Kalkulation für den Mittelstand schlägt das durchaus zu Buche.

Unbestritten bleibt Tape aber das kostengünstigste Speicher-Medium am Markt. Interne LTO-8-Streamer finden wir im Handel ab etwa 2.750 Euro und 80 Euro pro Einzel-Band netto. Nach dieser einfachen Rechnung (ohne Support, Automation, Software, Energie und andere Parameter) liegen die Kosten dann bei 2,60 Euro pro TByte – noch bevor die neunte Generation da ist.

Mittelständler wie Hyperscaler, der Zeitpunkt eines Ein-, Um- oder Rückeinstiegs in das Tape-Backup mit LTO mag gut kalkuliert sein. Konstant bleibt, dass die LTO-Roadmap weiterhin bis zur Generation 12 reicht. Die suchenden Blicke an den Horizont werden sich also wiederholen. ■

Tape-in-NAS: Plattform-unabhängige B2D2T-Lösung

Uns ist es (fast) egal, welche Backup-Software Sie einsetzen!

Als Plattform-basierende Produktlinie Ti-NAS stellt actidata ein System vor, das ein leistungsgerechtes RAID-System als NAS-Speicher mit einem bewährten LTO-Bandlaufwerk kombiniert. Als Betriebssystem wird eine CAL-free-Variante vom Windows Server 2019 eingesetzt, auf der eine Backup-Software, die LTO-Bandlaufwerke unterstützt, installiert und betrieben werden kann.

actidata Ti-NAS RT als kombiniertes NAS- und Backup-System im 2U Rackmount-Format.

Albrecht Hestermann, actidata

Ti-NAS steht für Tape-in-NAS und beschreibt die kombinierten Systemplattformen der **actidata**. Diese stellt einen Hardware-RAID-beschleunigten NAS-Speicher über mindestens zwei vorhandene optische 10Gb-Ethernet-Schnittstellen zur Verfügung sowie ein eingebautes LTO-Bandlaufwerk für die interne Datensicherung. Jede, für den *Windows Server 2019* zertifizierte Backup-Software, die LTO-Streamer unterstützt, lässt sich auf den actidata Ti-NAS-Plattformen betreiben.

Welche Backup-Software ist die richtige?

Hier scheiden sich die Geister, denn – auch wenn manche das nicht glauben wollen – jede Systemumgebung hat eigene Anforderungen. Jedes Unternehmen hat eigene Vorgaben und für jeden Systemadministrator gelten besondere Leistungsmerkmale als wichtig. Letztlich gibt es also nicht die »richtige« Backup-Software, sondern Anforderungen und Präferenzen, die zu definieren sind. Insofern ist es wichtig, seitens der Hardware die nötige Flexibilität zur Verfügung zu stellen. Die actidata Ti-NAS-Plattformen setzen genau auf diese Anforderungen und bieten mit dem *Windows Server 2019 in der IoT*-CAL-free-Variante ein ideales Hardware-System an.

Ti-NAS ist vorbereitet für Backup-to-Disk-to-Tape (B2D2T)

Im Rahmen einer B2D2T-Datensicherungsstrategie lassen sich die actidata Ti-NAS-Plattformen idealerweise einsetzen. Hierbei nutzt dann die vom Anwender betriebenen Datensicherungs-Software das integrierte NAS-System als Backup-Ziel, wobei auch für mehrere Backup-Sets je noch Konfiguration bis zu 108 TByte Brutto-Speicherkapazität zur Verfügung stehen. Im zweiten Schritt der B2D2T-Strategie werden die Daten von dem internen RAID-System auf das eingebaute LTO-Bandlaufwerk übertragen. Bis zu 12 TByte, native (LTO-8) lassen sich so auf einem einzelnen, auswechselbaren Medium übertragen, die dann an einem externen Lagerplatz (z.B. Banktresor) deponiert werden können.

Separat installiert und somit entfernt von Produktivsystemen

Sinnvollerweise wird eine Backup-System entfernt von den Produktivsystemen an einem anderen Ort installiert und betrieben. Somit wird dem Anspruch Rechnung getragen, dass beispielweise bei einem Brandfall im Serverraum die Daten der letzten Sicherungen nach wie vor separat zur Verfügung stehen. Dank der vorhandenen optischen 10Gb-Ethernet-Schnittstellen können auch größere Entfernungen mit Glasfaser-Kabeln überbrückt werden. ■

Weitere Informationen

actidata Storage Systems GmbH
Wulfshofstr. 16 – Indupark
44149 Dortmund
T: 02 31/96 36 32 – 0
E-Mail: info@actidata.com
www.actidata.com

Actidata

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

Sitz der Gesellschaft:
Dortmund

Niederlassung in Deutschland:
Dortmund

Jahr der Gründung:
2009

Zielgruppe: **Systemhäuser, VARs und Industriekunden**

www.actidata.com

Quantum

Mit Technologien und Services von Quantum lassen sich digitale Inhalte erfassen, verarbeiten und gemeinsam nutzen – und außer-dem für Jahrzehnte vorhalten und sichern. Unsere Plattformen bieten die schnellste Performance für große Datenmengen, industrielles IoT und hochauflösendes Film- und Bildmaterial – für jede Phase des Datenlebenszyklus – von der Kollaboration und Analyse in Echtzeit bis zur kostengünstigen Archivierung.

Sitz der Gesellschaft:
San Jose, USA

Niederlassung in Deutschland:
München

Jahr der Gründung:

1980

Zielgruppe: **Mittelständische und große Unternehmen**

www.quantum.com/de

FAST LTA

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

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

Sitz der Gesellschaft:
München

Niederlassung in Deutschland:
München

Jahr der Gründung:
1999

Zielgruppe: **KMUs, VARs und Industriekunden**

www.fast-lta.de

N-able Technologies

Wir lassen IT einfach aussehen.

Wir sind ein führender Hersteller leistungsstarker und erschwinglicher IT-Infrastrukturmanagement-Software. Unsere Produkte bieten Unternehmen jeder Art und Größe weltweit leistungsstarke Tools zum Überwachen und Verwalten der Leistung ihrer IT-Umgebungen, egal wie komplex ihre IT-Infrastruktur ist – ob lokal, in der Cloud oder in hybriden Modellen.

Sitz der Gesellschaft:
Morrisville, North Carolina

Niederlassung in Europa:
Dundee

Jahr der Gründung:
1999

Zielgruppe: **Systemhäuser, VARs und Industriekunden**

www.n-able.com

Expertengespräch mit Jan Gerzinus Jongsma, N-able

Cloud First: Nur ein Remote-Backup ist ein gutes Backup

»N-able Backup« basiert auf Cloud-Services, die keine lokalen Speicher-Ressourcen zur Datensicherung benötigen. Hersteller N-able (ehemals Solarwinds MSP) sieht sich als Alternative zu herkömmlichen Ansätzen und verspricht mit bis zu 50-fach niedrigeren Änderungsraten eine schnelle und effektive Sicherung in die Wolke. Wir sprachen mit Jan Gerzinus Jongsma, Director Sales Engineering bei N-able, über die Cloud-First-Strategie des Herstellers und Entwicklung im MSP-Markt.

■ Karl Fröhlich

Einer N-able-Umfrage zufolge hat die Corona-Krise Auswirkungen auf den Geschäftsbetrieb von MSPs und künftige Marktchancen?

Jongsma: Die überwiegende Mehrheit der befragten Betriebe konnte ihr Personal in der Krise halten. Das ist ein ermutigendes Signal, schließlich haben MSPs für andere Unternehmen in puncto digitale Transformation eine wichtige Unterstützungsfunktion. Die Tech-Branche und der MSP-Vertriebskanal haben viel Widerstandskraft und Potenzial. Covid-19 hat den Wert, den MSPs für Unternehmen haben, noch einmal unterstrichen. MSPs stocken die Leistung unternehmensinterner IT-Teams auf. Die kümmern sich meist hauptsächlich um Risikominderung und Business Continuity.

Jan Gerzinus Jongsma
Director Sales Engineering

»Werden die Daten stündlich gesichert und geht der Restore sehr schnell, ist ein Ausfall ärgerlich, aber kein Drama.«

Viele Betriebe wären ohne MSPs in einer schwierigen Lage gewesen und hätten nie so schnell auf Homeoffice-Betrieb umstellen können. Das fachliche Know-how und Können von MSPs waren in diesen Krisenzeiten ganz entscheidend. Man kann sagen, MSPs sind systemrelevant.

Was unterscheidet N-able von klassischen Backup-Technologien? N-able unterscheidet sich aber vom Geschäftsmodell. Anwender-Unternehmen sind eigentlich nicht Ihre Kunden.

Jongsma: Datensicherung ist einer der Kernaufgaben einer Unternehmens-IT. Zudem sollte sie sich aber ebenfalls um strategische Themen kümmern. Die Freiräume, die sie dazu benötigt, schaffen Managed-Service-Provider mit unseren Tools. Eines davon ist Backup.

Die Angebote unserer MSP-Kunden sehen allerdings recht unterschiedlich aus, je nachdem, welche Dienstleistungen sie in ihre Pakete integrieren, ob etwa automatisierte Backup- und Restore-Tests dabei sind oder die Bereinigung personenbezogener Daten in älteren Sicherungsdateien. Viele MSPs bieten N-able Backup auch unter ihrem eigenen Brand an. Einer verkauft seinen Kunden sogar eine Backup-Flatrate.

Das heißt, Sie sehen sich mit N-able gut aufgestellt?

Jongsma: N-able konzentriert sich darauf, eine breite Palette an Werkzeugen bereitzustellen, die MSPs dabei helfen sollen, ihre Geschäfte effektiv zu führen und im Gegenzug ihre Endkunden effektiv zu bedienen. N-able Backup ist eines dieser Werkzeuge, aber wir liefern auch vollständige Fernüberwachung und -verwaltung sowie eine Vielzahl anderer Sicherheitslösungen. Wir sind bestrebt, über eine integrierte Plattform Flexibilität und Skalierbarkeit zu bieten. N-able Backup läuft auf herkömmlichen Maschi-

nen und liefert Backup-to-Storage über IP. Kunden können dazu ihre eigenen Systeme verwenden, allerdings nutzen 95 Prozent unseren Cloud-Speicher. Dafür unterhalten wir unsere eigenen Storage- und Server-Kapazitäten in Rechenzentren überall auf der Welt. Der Kunde hat dabei die Wahl, an welcher Lokation seine Daten liegen.

N-able Backup ist Cloud-nativ und unterscheidet sich von den klassischen Technologien. Wie eigentlich genau?

Jongsma: Wenn wir über Datensicherung nachdenken, stellen wir die Anforderungen des Endkunden in den Mittelpunkt. Die Frage ist: Welches Service-Level ist sinnvoll, um die Arbeit des Anwenders optimal zu schützen.

Es ist ein einfaches Rechenbeispiel: 50 Mitarbeiter eines Unternehmens arbeiten an einem Projekt. Läuft die Datensicherung einmal die Woche, verliert das Unternehmen bei einem Vorfall im schlimmsten Fall 250 Manntage Arbeit (50x5 Werktage) plus die Zeit, die es dauert, bis das Backup zurückgespielt ist.

Für ein Unternehmen ist das teuer, für die Mitarbeiter frustrierend. Läuft die Datensicherung täglich, gehen »nur« 50 Manntage Arbeit verloren. Sichert das System die Daten stündlich und geht der Restore sehr schnell, ist ein Ausfall ärgerlich aber kein Drama.

Ein stündliches Backup klingt sinnvoll, aber ist das angesichts immer größerer Datenmengen als Cloud-Backup ohne eigene Infrastruktur vor Ort überhaupt realistisch machbar und nicht viel zu teuer?

Jongsma: Genau das war unsere Aufgabenstellung. Backup muss zuverlässig funktionieren, aber für die Kunden berechenbar und erschwinglich sein. Und natürlich gilt unsere wichtigste Prämisse: »Nur ein Cloud-Backup ist ein gutes Backup«.

Unsere Lösung ist es, durch intelligente Verfahren nur die Daten zu sichern, die wirklich relevant sind. Das funktioniert nur, wenn man das Backup direkt auf der jeweiligen Maschine erstellt und eben nicht von außen. Die klassische Vorgehensweise speichert einen Snapshot und beginnt dann, die Daten mit Kompression und Deduplizierung zu reduzieren. Wir sagen: Mit dem Snapshot ist das Problem schon in der Welt. Deduplizierung, egal wie gut, hat dann nur noch kosmetische Effekte.

Weitere Informationen

N-able
The Vision Building,
20 Greenmarket
Dundee, DD1 4QB
(Scotland) UK
www.n-able.com

Wir sichern nur die echten Veränderungen, und zwar direkt von der Maschine. Alle Overheads und Umorganisationen, etwa durch das Betriebssystem, filtern wir von vorne herein aus. Damit reduzieren sich die Backup-Daten um den Faktor 30 bis 50.

Das klingt zwar plausibel, aber wo genau liegen die Vorteile?

Jongsma: Es gibt drei Vorteile. Tatsächlich sind die Datenmengen so klein, dass sie auch über eine nicht ganz so schnelle Datenleitung bequem übertragbar sind. Und sie belegen überschaubaren Platz im Rechenzentrum. Vorteil Nummer 2: Viele Kunden haben das Problem, dass sie nie genau wissen, wie hoch ihre Backup-Rechnung bei ihrem Service-Provider ausfällt, weil nicht klar ist, wie viel Platz ihre Daten im Rechenzentrum belegen. Das kann mit N-able Backup nicht passieren. Die Unternehmen benötigen drittens keine eigene Backup-Infrastruktur, deren Anschaffung und Betrieb teuer ist.

Lokales Backup vs. Cloud-Backup
Wie lassen sich die Kunden überzeugen, ihre Backup-Infrastruktur komplett zu verändern?

Jongsma: Die Kunden können, wenn sie es wünschen, über unsere Software auch eine lokale Sicherung parallel nutzen. Andere Anbieter sagen »local first«, bei uns ist es umgekehrt: »Cloud First«.

Wir bieten dafür die Flexibilität einer Cloud-Lösung, nicht nur technologisch, sondern auch Lizensierungen mit monatlicher Kündigung. Dies hilft, maximalen Investitionsschutz zu versichern, was gerade in der derzeitigen wirtschaftlichen Lage sehr wichtig ist.

Sie sagen, Cloud gewinnt an Akzeptanz, aber nutzen tatsächlich auch Großunternehmen N-able Backup?

Jongsma: Unser größter Kunde ist ein internationales Hosting-Unternehmen. In Deutschland nutzen viele kleine und mittlere MSPs und deren mittelständische Unternehmen unsere Lösung. Zugang finden wir, unter anderem, durch existierende N-able-Geschäfte aus anderen Bereichen wie den Infrastrukturlösungen und erhalten viel positives Feedback. Gleichzeitig setzen in Deutschland noch viele auf Tape oder lokales Backup, da sie denken, sie bräuchten riesige Maschinen und Bandbreiten für ein Cloud-Backup. Das stimmt – egal wo – so nicht, zumindest mit unserer Lösung.

Wie sieht es mit den Kosten aus?

Jongsma: Der Preis skaliert vor allem über Volume, also die Anzahl der Backup-Server, und in Teilen über die Laufzeit. Mit jedem

Server kommen 500 GByte, mit jeder Workstation 100 GByte inklusive.

Dies ist natürlich ausbaubar. Letztlich hängen die Endkunden-Preise stark von unseren MSP-Partnern und ihren Margen ab.

Auf der Produktseite gab es zuletzt Zuwachs im Bereich Backup für Office 365.

Jongsma: Richtig, mit unserer *MS 365 Cloud Backup*-Lösung sichern wir unter anderem *Exchange*, *SharePoint* und *OneDrive*. Wir können Backups aus den Microsoft-Rechenzentren auf unseren Storage migrieren, um schnelle Restores über eine Management-Oberfläche zu fahren.

Ein neues Feature ist das automatisierte Recovery-Testing an einer dritten Lokation. Je nach Kundenwunsch führen wir alle zwei oder vier Wochen einen kompletten Restore von Maschinen in unserer Umgebung durch, die als virtuelle gemountet und auf Vollständigkeit getestet wird.

Dies ist die Phase I des Recovery-Testing. In Zukunft werden wir die Frequenz der automatisierten Wiederherstellungen erhöhen und den Kunden den Zugriff auf die Testumgebung ermöglichen. Auch weitere Cloud-Umgebungen sollen hinzukommen. Alle haben verstanden, wie wichtig Backup ist, aber die wenigsten testen den Restore. Deswegen pushen wir diese Lösung in den nächsten Monaten. ■

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. Diese ist heute in der Regel Teil von umfassenden Service-Plattformen, die On-Premises ebenso wie in der Multi-Cloud funktionieren muss.

Michael Baumann

Im Mittelstands- und Enterprise-Segment überzeugen die meisten Datensicherungs-Produkte durch universelle Leistungsvielfalt, nur wenige sind eher »Spezialisten«, und diese dann »Cloud only«. Neben klassischen Lizenzmodellen setzen sich zunehmend Abo-, Backup-as-a-Service- (BaaS) und Disaster-Recovery-as-a-Service-Dienste (DRaaS) durch.

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.

Neben konventionellen Anforderungen an *Response Time Objectives* (RTO) und *Response Point Objectives* (RPO), herkömmlichen Sicherheits- und Kostenbetrachtungen und der eher neueren Flexibilität-Erfordernis durch Multi-Cloud, gibt es bei nahezu allen Anbietern (und wohl Anwendern) ein beherrschendes Thema: Der Schutz vor Ransomware.

Bei unserem Überblick spielt zunächst die weltweite Marktdurchdringung bei Großunternehmen (hauptsächlich *Gartner Magic Quadrant* und *Forrester Wave*) eine Rolle. In Gartners jüngstem *Data Center Backup and Recovery Solutions*-Bericht vom Herbst 2020 verdrängt beispielsweise der Virtualisierungs-Spezialist **Veeam** erstmals den Traditionsanbieter **Commvault** von der Top-Position, zumindest in der Kategorie »Execution«. Andere wenden sich ungewöhnlich scharf und öffentlich gegen ihre Einordnung. So können Marktübersichten nie komplett sein, über die Kategorien kann trefflich debattiert werden. Unter den Top 10 im erwähnten Bericht gibt es allein sieben Leader, alle finden sich natürlich in dieser Übersicht. Nicht berücksichtigen können wir alle Sicherungs- und Kopierdienste, die nicht zentraler Teil des Cloud-Dienstes sind. Dagegen berücksichtigen wir auch dedizierte Backup-Produkte, die hauptsächlich im deutschsprachigen Raum ihre Liebhaber finden und tendenziell am Mittelstand orientiert sind. Da wir kein Ranking bieten können und wollen, listen wir alphabetisch.

Anbieter	Produkt
Acronis	Cyber Backup
Actifio	VDP (Virtual Data Pipeline)
Altaro	VM Backup
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	DataCenter
Rubrik	Cloud Data Management
SEP	sesam Beefalo
Unitrends	Enterprise Backup
Veeam	Availability Suite
Veritas	NetBackup/BackupExec

Acronis Cyber Backup

Neben seinem Angebot für Privatanwender und KMUs wendet sich der Hersteller auch an professionelle User: **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 beispielsweise durch *Acronis Disaster Recovery* (as-a-Service), *Cyber Infrastructure* und einer neuen *Cyber Appliance*-Hardware.

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 einfache Handhabung und überschaubare Kosten. Für die Standard-Suite fallen jährlich derzeit 349 Euro pro Server, 409 Euro pro Virtual-Host und 55 Euro pro Workstation an. Für die *Advanced Edition* in der aktuellen Version 12.5 sind 539 Euro pro Server fällig bzw. 729 Euro pro Virtual-Host und 75 Euro pro Workstation. Kostenlose Testversionen sind verfügbar.

Altaro VM Backup

Altaro *VM Backup* 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.

Sehen Sie unser ausführliches Video-Interview zu Altaro VM Backup auf speicherguide-campus.de.

Arcserve UDP

Arcserve *Unified Data Protection* (UDP) gibt es derzeit in der Version 8.0, in Kooperation mit **Sophos** auch zum Schutz gegen Ransomware. 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-basierte Datensicherung, Disaster-Recovery-Technologien und Deduplizierung zu einer Komplettlösung. In Zentrale und Außenstellen werden dazu Recovery-Point-Server (RPS) installiert, über den sich die Host-Plattformen anbinden lassen. 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), Exchange, *MS SQL*, Dateiserver, *Microsoft IIS*, *Active Directory*, *Oracle Database*, *PostgreSQL, VMware vSphere* (agentenlos), *Hyper-V* (agentenlos) und *Nutanix AHV*.

Die Kosten für Arcserve UDP Advanced Edition in der aktuellen Version für eine Server-OS-Instanz inklusive Enterprise-Wartung liegen bei etwa 500 Euro pro Jahr.

Cohesity Data Protect

Zusammen mit *Rubrik* gehört **Cohesity**, vor allem hierzulande, zu den Senkrechtstartern im Bereich der Backup-Anbieter für Unternehmen. *Forrester* ordnet beide im Bereich der Marktführer ein. Auch im aktuellen Magic-Quadranten von *Gartner* zählt Cohesity zu den »Leadern«. Zusammen mit **Pure Storage** will man zudem die Lösung *FlashRecover*, *Powered by Cohesity* vermarkten.

Cohesity DataProtect ist eine Cloud-native Datenmanagement-Lösung. 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 bis in den fünfstelligen Bereich jährlich kosten kann. Zudem ist der Dienst als Add-on zur Cohesity Data-Platform verfügbar, die in der Premium-Edition für etwa 1.200 Euro jährlich buchbar ist, wiederum mit unzähligen Variablen.

Sehen Sie unser ausführliches Video-Interview zu Cohesity auf speicherguide-campus.de.

Collage: speicherguide.de und die jeweiligen Hersteller

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, so der Hersteller.

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

Im Online-Shop des Distributors ADN rangiert Commvault Complete Backup und Recovery mit 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. Beim Online-Händler Portwork kostet die 5-Jahreslizenz für eine physische Instanz etwa 3.500 Euro.

Dell EMC Networker

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.

Neben der Integration mit *PowerProtect für Cloud-Workloads* 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 *Ready Stack* 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). Weite-

re Details zu den Kosten stehen uns nicht zur Verfügung.

Druva Cloud Platform

Mit **Druva** gibt es einen relativ erfolgreichen Cloud-nativen Anbieter im Bereich Data-Protection. *Druva Cloud Platform* ist eine SaaS-Plattform für die Sicherung von lokalen physischen und virtuellen Servern bis hin zu mobilen Endgeräten.

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.

In der Data Center-Variante *Phoenix business* starten die Preise bei 210 US-Dollar pro Terabyte und Monat. Verschiedene Module kommen hinzu, beispielsweise sieben US-Dollar pro Server und Monat in der AWS-Infrastruktur und acht US-Dollar pro Endpunkt, User und Monat.

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. Inkludiert sind 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 es man 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 Data Protector

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.

Bacula – Open-Source-Backup

Das Open-Source-Tool **Bacula 11.0.1** 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 Updates und verschiedene Support-Levels eingekauft werden. Genaue Preise kommuniziert der Anbieter allerdings nicht.

www.baculasystems.com

NovaStor DataCenter

Das in Hamburg ansässige Unternehmen **Novastor** bietet mit *NovaStor DataCenter* eine ganzheitliche Datensicherung für physische und virtuelle Server auf derselben Oberfläche, zentralisiert die Sicherung verteilter Daten und das Medien-Management von Cloud, Disk und Tape inklusive Datenauslagerung.

Der Hersteller verspricht freie Wahl bei Speichermedien und -herstellern, hohen Automationsgrad, Fehlertoleranz und effiziente Speichernutzung. Adressiert werden primär mittelständische Unternehmen, Be-

hörden und öffentliche Verwaltungen, die Lösung skaliert aber auch auf mehrere tausend Server.

Eine NovaStor DataCenter-Lizenz inkl. einem Jahr *NovaCare*-Support für 5 TByte finden wir im Online-Handel ab etwa 850 Euro.

Rubrik Andes

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*, aktuell in der Version 5.3. On-Premises-, Edge- und Multi-Cloud-Workloads können mit Rubrik gesichert werden, in der Cloud.

Der Andes-Service beinhaltet Data-Protection, Ransomware-Recovery, Compliance 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.

Gartner Magic Quadrant Data Center Backup and Recovery Solutions 2020

SEP Sesam

Der deutsche Datensicherungs-Spezialist **SEP** bietet im Rahmen seiner *Hybrid Backup & Recovery*-Dienste die *SEP sesam Beefalo v2*-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*. Assistenz-Tools für die Rücksicherung gibt es für die Datenbank-Applikationen von Oracle, SAP HANA und SQL-Server in Form von *AlwaysOn Availability Groups* (AOAG). Auch die Rücksicherung der *VMware Sandbox* wird assistiert.

Das Lizenzmodell *SEP sesam VM Essential Edition* für zwei Sockel in Virtualisierungs-Servern und unlimitierter Nutzung von VMs beginnt bei 750 Euro netto und beinhaltet zwölf Monate Maintenance.

Solarwinds Backup

Nach dem Motto Cloud First wurde *Solar-Winds Backup* eigens für die Datensicherung in der Cloud entwickelt. Sie basiert im Gegensatz zu herkömmlichen Ansätzen auf SaaS-Services, die keine lokale Speicher-Ressourcen zur Datensicherung benötigen.

Statt Image-basierter Sicherung verarbeitet die Software Datenänderungen im lokalen Server und erzielt durch True-Delta-Deduplizierung, Datenkomprimierung und WAN-Optimierung nach eigenen Angaben etwa 50-fach niedrigere Änderungsraten, die dadurch ohne lokale Speicher schneller in die Cloud verschoben werden. Dort können eigene Kapazitäten oder jene von Solarwinds genutzt werden.

Über ein zentrales Web-Dashboard werden virtuelle und physische Server, Workstations, *Microsoft 365*-Daten und Geschäftsdokumente gesichert. Die Wiederherstellung erfolgt auf Ordner- und Dateiebene. Auch komplette Systemwiederherstellungen mit Bare-Metal- oder Virtual-Disaster-Recovery sind möglich, wie auch automatische Recovery-Tests.

Laut Hersteller ist die Lösung extrem skalierbar, Hot-Spot sind aber eher mittelständische Firmen. So sollen auch die Kosten im »mittleren Bereich« liegen. Preise nennt der Hersteller keine. Im Web recherchieren wir einen jährlichen Abopreis ab 2.440 Euro, für die Backup-Software und den Speicherplatz in der Solarwinds-Cloud.

Veeam Backup & Replication

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. *Veeam Backup & Replication 11* ist zentraler Bestandteil der Suite.

Die Availability Suite unterstützt fast zwei Duzend 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. 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.

Die Einstiegslösung *Veeam Backup Essentials* schlägt ab etwa 900 Euro zu Buche. Die Kauflizenz inklusive einem Jahr Support für Veeam Availability Suite Enterprise Plus (V11) ist für knapp 3.000 Euro erhältlich. ■

Weitere Informationen

Lesen Sie eine ausführliche Fassung des Marktüberblicks auf speicherguide.de

Kommentar

Preise & Lizenzen: Hersteller müssen umdenken

Wenn es etwas gibt, was IT-Manager, Entscheider und Einkäufer auf die Palme bringt, ist es die Preis- und Lizenzpolitik der Backup-Software-Hersteller. Die undurchsichtige Preis- und Lizenzpolitik! Wir haben dies auf unserem *speicherguide.de Campus*-Meetup diskutiert und unter den ITlern gibt es diesbezüglich keine zwei Meinungen.

Die Forderungen lauten, mehr Transparenz und Übersicht. Da es sich um Standardprodukte handelt, sei nicht verständlich, warum da so ein »Gewese« gemacht werde. Natürlich gebe es diverse Add-ons und aufgrund der benötigten Anzahl der Lizenzen könne es einen Spielraum geben, aber eine grundsätzliche Orientierung muss möglich sein.

Die anwesenden Herstellervertreter mussten letztendlich zugeben, es geht darum nicht vergleichbar zu sein. Viele wollen sich nicht in die Karten schauen lassen. Werden zur Software auch Hardware und/oder Services angeboten, dürfe man davon ausgehen, dass noch viel hineingerechnet wird. Zudem sei Backup-Software nicht Backup-Software. Je mehr Möglichkeiten Produkte bieten, zum Beispiel in punkto Schnittstellen, Protokolle und Anbindungen, desto intransparenter wird es.

Kann man so sehen, allerdings ist ein Hauptgrund für den Erfolg von Cloud-Angeboten definitiv die Preistransparenz. Daran werden sich die Anbieter von Backup-Software noch gewöhnen müssen.

Auch die Ausrede, wir verkaufen über den Handel und der macht die Preise ist Quatsch. Wer als Hersteller die Preise seiner Produkte nicht kennt, kann einpacken. Ein Preisbeispiel,

Karl Fröhlich, speicherguide.de

»Bei Bundles: Unbedingt Einzelpreise auflisten lassen, sonst rächt sich dies bei Erweiterungen und Wartung.«

wie es die *speicherguide.de*-Redaktion immer einfordert, muss jeder Anbieter jederzeit angeben können.

Ein weiterer Vorwurf sind undurchsichtige Lizenzmodelle, die oft nicht kundengerecht sind. 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.

Meine Meinung: Wer mir keinen Preis nennt, hat etwas zu verbergen. Produkte, die ich vorab nicht einordnen kann, haben bei mir keine Chance in die engere Auswahl zu kommen.

FAST LTA
Wir sichern Petabytes.

S3: ja, bitte –
Cloud: nein, danke?

Sie wollen Daten aus Office365® oder im Veeam® Capacity Tier sichern, aber die vollständige **Datenhoheit** behalten?

On Premise
Object Store.

Neben NFS und SMB lassen sich Silent Bricks auch als **On Premise Object Store mit S3-Anbindung** nutzen. Einfach so. Ohne Aufpreis.

Silent Bricks.

https://fastlta.com/de-s3

Im Ernstfall helfen nur vorab definierte Prozesse

Jedes Unternehmen braucht einen IT-Notfallplan

Bei einer IT-Störungen im Unternehmen entscheidet eine schnelle und richtige Reaktion über das Ausmaß des Schadens. Ein IT-Notfallhandbuch bietet die erforderliche Orientierung. Tritt der Ernstfall ein, bleibt meist keine Zeit, sich zu überlegen was nun zu tun sei. Hier bekommen Sie Hinweise, was im IT-Notfallhandbuch Ihres Unternehmens enthalten sein muss.

■ Peter Marwan

Das bekannteste Notfallhandbuch ist wahrscheinlich »The Hitchhiker's Guide to the Galaxy«. Ganz wichtig auf dem Einband sind die beruhigenden Worte »Don't Panic«. Im Inneren finden sich umfangreiche Hinweise und Handlungsempfehlungen für alle möglichen Ereignisse bei Reisen »per Anhalter durch die Galaxis«. Den Leser bewahren sie aber nicht davor, immer wieder in neue Schwierigkeiten zu geraten – wie jeder weiß, der das Buch gelesen oder den Film gesehen hat.

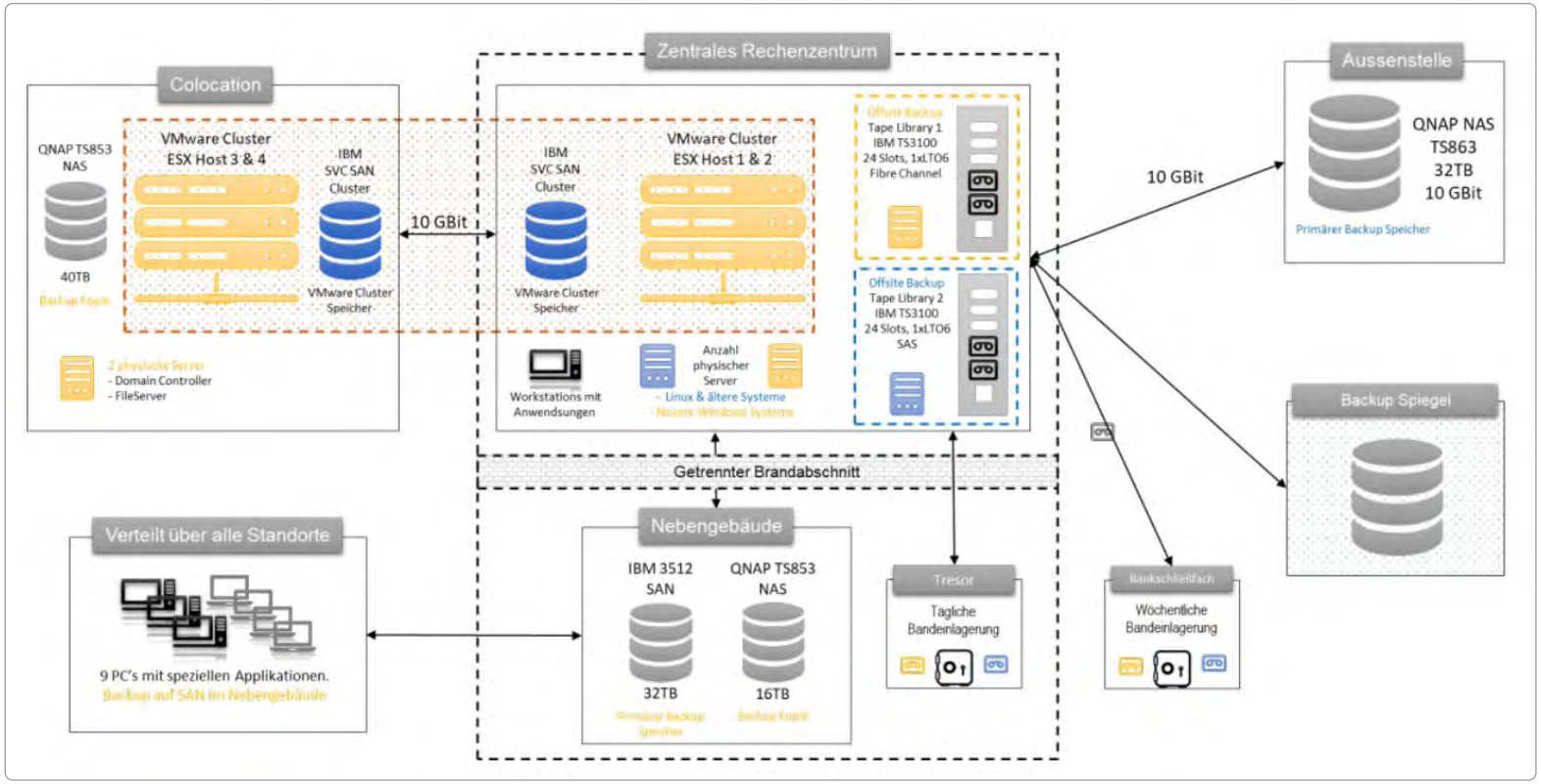
An ein IT-Notfallhandbuch hat man andere Erwartungen: Es soll dazu beitragen, dass bei einer Störung des IT-Betriebs alle Personen im Unternehmen richtig reagieren und genau wissen, was zu tun ist. Das IT-Notfallhandbuch ist somit eine taktische Maßnahme und unterstützt strategische Bemühungen um Business-Continuity-Management und Cyber-Resilienz. Beides sind nicht nur modische Schlagworte, sondern Ausdruck der Tatsache, dass Firmen immer stärker von funktionierender IT abhängig sind.

Die Aufgabe des IT-Notfallmanagements

IT-Notfallmanagement ist Teil eines Business-Continuity-Management-Systems (BCMS). Dessen Aufgabe ist es, die Ausfallsicherheit der Geschäftsprozesse zu erhöhen und die Voraussetzungen dafür zu schaffen, in einer Krise schnell, zielgerichtet und angemessen zu reagieren. Es soll also sowohl die Widerstandsfähigkeit (Resilienz) des Unternehmens erhöhen als auch dafür sorgen, dass die Geschäftstätigkeit nach einem Ausfall so schnell wie möglich wieder aufgenommen werden kann.

Die Verfügbarkeit von IT ist dazu ein entscheidender Baustein. Wichtige Normen in dem Umfeld sind ISO 22.301 (Business Continuity), ISO 27.031 (IT-Service Continuity Management/ITSCM) und der BSI-Standard 100-4 (Notfallmanagement). Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* erarbeitet mit dem BSI-Standard 200-4 (Business Continuity Management) derzeit zudem eine weiteres Dokument, dass bei der strukturierten Planung von Notfallmanagement und Disaster-Recovery helfen kann.

Bild: via Canva Pro



Grafik: Novastor

Ein Backup-Konzept dokumentiert die aktuelle Infrastruktur und sollte Teil eines IT-Notfallhandbuchs sein.

Ohne Risikoanalyse kein IT-Notfallmanagement

Ein IT-Notfall kann viele Ursachen haben. Erfolgreiche Cyberangriffe, etwa mittels Ransomware, sind nur eine davon. Auch technische Probleme, Naturkatastrophen, Stromausfall oder ein Brand im Unternehmen gehören dazu. Mit der Nutzung externer Ressourcen bei Cloud- und SaaS-Anbietern können dieselben Ursachen auch dort zu einem Notfall für das eigene Unternehmen führen. Denn in der Regel sagen Cloud-Dienstleister nur die Verfügbarkeit ihrer Dienste und Services zu. Sicherung und Wiederherstellung der Daten liegen dagegen in der Verantwortung der Nutzer. Notfallkonzepte und dementsprechend auch das Notfallhandbuch müssen also auch diesen Bereich abdecken. IT-Risiken zu definieren, ist eine wichtige Voraussetzung für ein gutes IT-Notfallhandbuch. Denn im Notfall lassen sich Prioritäten nur dann sauber festlegen, wenn bekannt ist, welche Auswirkungen einzelne Aspekte auf den Betrieb haben. Dazu wird in einer Risikoanalyse ermittelt, welche Geschäftsprozesse unverzichtbar sind und welche Ressourcen dafür benötigt werden.

Als Grundlage für das Risikomanagement bietet sich unter anderem der BSI-Standard 200–3 als Orientierungshilfe an. Für kleine und mittelgroße Unternehmen hat der *Bitkom* einen Leitfaden zum IT-Risikomanagement erstellt, der kostenlos als PDF zum Download bereitsteht. Einen guten Einstieg und hilfreiche Anregungen auch für kleinere Firmen bietet zudem das von der *Allianz für Cyber-Sicherheit für Unternehmensvorstände und Aufsichtsräte* angebotene Handbuch zum Management von Cyber-Risiken.

Richtige Alarmierung ist der erste Schritt

Bei einem IT-Notfall ist schnelles und zielgerichtetes Handeln gefragt. Erster Schritt dazu ist die richtige Reaktion aller Beteiligten – auch derjenigen, die nicht zur IT-Abteilung gehören. Dafür hat das BSI die IT-Notfallkarte erarbeitet. Ähnlich wie das bekannte Hinweisschild »Verhalten im Brandfall« führt sie kurz auf, was im IT-Notfall zu tun ist.

Die IT-Notfallkarte gibt knapp und übersichtlich Informationen dazu, wer auf welchem Wege zu alarmieren ist, welche Bedeutung die Weitergabe wichtiger Informationen zu IT-Notfällen hat und warnt vor womöglich kontraproduktiven, eigenmächtigen Maßnahmen. Hinweise zur Verwendung der IT-Notfallkarte und den Nutzungsbedingungen finden sich auf der Webseite des BSI.

Arten von IT-Notfallplänen

In einem IT-Notfallplan ist detailliert festgehalten, wie bei einem Störfall weiterhin auf wichtige Systeme zugegriffen, die Informationssicherheit aufrechterhalten und der Betrieb schnell und effektiv wiederhergestellt wird. Viele wünschen sich dafür eine konkrete Anleitung, am besten als PDF zum Download.

Das ist jedoch der falsche Ansatz. Ein gutes IT-Notfallhandbuch muss die individuellen Unternehmensstrukturen berücksichtigen. Manche Unternehmen sind zum Beispiel ohne E-Mail-Zugriff handlungsunfähig. Andere können mehrere Stunden darauf verzichten – nicht dagegen auf ihren Webshop, ihre Call-Center-Anwendung oder eine branchenspezifische Software. Außerdem unterscheiden sich Zuständigkeiten und Informationswege in allen Unternehmen.

Generell gibt es mehrere Ansätze, ein IT-Notfallhandbuch aufzubauen. Welcher gewählt wird, ist teilweise Ansichtssache, teilweise durch die Strukturen im Unternehmen bedingt. Die Einteilung nach Prozessen scheint aus Sicht von Business Continuity Management sinnvoll, wo es um die Verfügbarkeit von Geschäftsprozessen geht. In der Praxis können prozessübergreifende oder nicht den ganzen Prozess erfassende Zuständigkeiten jedoch zu Schwierigkeiten führen.

Die Gliederung nach Phasen setzt das Verständnis der Mitarbeiter dafür voraus, in welcher Notfallphase sie sich gerade befinden, um richtig handeln zu können. Möglich ist auch eine Unterteilung des IT-Notfallhandbuchs nach Ebenen der Verantwortlichkeit. Vorteil dabei: Jede Ebene (Mitarbeiter, Führungskräfte, Support und IT-Mitarbeiter) kann Informationen in der für sie verständlichen und erforderlichen Detailtiefe erhalten. Nachteil: An Schnittstellen drohen Informationsdefizite.

Auf jeden Fall zu empfehlen ist ein modularer Aufbau: Niemand liest das Handbuch in einem Notfall in aller Ruhe von vorne nach hinten durch. Bewährt hat sich ein zweigliedriger Aufbau: Der erste Teil bietet allgemeine Informationen wie Begriffsdefinitionen, Zuständigkeiten, Kontaktmöglichkeiten und Meldeketten. Der zweite Teil behandelt konkrete Schadensereignisse – und verweist gegebenenfalls auf die relevanten Stellen im ersten Teil.

Ganz wichtig ist, das IT-Notfallhandbuch regelmäßig und zentral zu pflegen: Veraltete Informationen sind fast noch schlimmer als fehlende Informationen, gaukeln sie doch eine trügerische Sicherheit vor. Mindestens ebenso wichtig ist, zumindest gelegentlich stichprobenartige Notfallübungen durchzuführen. Durch sie zeigt sich schnell, ob die im Notfallplan angebotenen Informationen verständlich sind und die Reaktionen planmäßig verlaufen – oder ob Nachbesserungen erforderlich sind. Einen guten Einstieg in die Entwicklung des eigenen IT-Notfallhandbuchs bietet der Maßnahmenkatalog zum Notfallmanagement des BSI.

Die IT-Notfallkarte des BSI bietet eine erste Orientierung.

Grafik: BSI

Die wichtigsten Punkte eines IT-Notfallplans

IT-Notfallhandbücher müssen die individuellen Bedürfnisse des Unternehmens berücksichtigen. Einige Aspekte sollten jedoch immer enthalten sein. Dazu gehören:

- **Sofortmaßnahmen:** Darunter fallen einerseits Maßnahmen zur Rettung oder Evakuierung von Personen zum Beispiel bei Brand oder Wassereinbruch im Rechenzentrum, andererseits aber auch klassische IT-Maßnahmen, etwa die Trennung vom Netz oder zumindest Netzsegmenten bei einem erkannten Angriff, um ihn einzudämmen.
- **Notfallkommunikation:** Klare und verständliche Kommunikation ist im Notfall Trumpf. Dazu muss geregelt sein, wer wen in welcher Form informieren muss – aber auch, was vielleicht nicht gesagt werden darf, etwa in der Kommunikation mit Kunden und Lieferanten. Je nach Situation ist in diesem Teil auch festgelegt, wie Öffentlichkeit und Medien sowie wie und wann Datenschutz- und andere Aufsichtsbehörden zu informieren sind.
- **Leitfaden für den Krisenstab:** Unvorhergesehene Notfälle lassen sich am besten durch ein zuvor festgelegtes Team mit allen relevanten Experten meistern. Widersprüchliche Anordnungen lassen sich vermeiden, Lagebeurteilungen schneller abgeben, wenn mögliche Optionen bereits vor dem Notfall übersichtlich zusammengefasst wurden. Auch abzuarbei-

tende Aufgaben, die dazu erforderlichen Rechte und die richtigen Ansprechpartner sollten hier vermerkt sein.

- **Business-Continuity-Pläne:** Als Ergebnis der Risikoanalyse ist bekannt, welche Geschäftsprozesse welche Ausfallzeiten verkraften. Daraus leitet sich die Priorisierung der Maßnahmen zur Wiederherstellung des Normalbetriebs ab. Gleichzeitig ist dadurch klar, für welche Bereiche der – hoffentlich vorher geplante – Notbetrieb aufzunehmen ist, um die Zeit bis zum Normalbetrieb zu überbrücken.
- **Rückkehr zum Normalbetrieb:** Hat sich die Lage stabilisiert, ist es meist noch ein weiter Weg bis zum Normalbetrieb. Nach einem Cyberangriff steht oft eine forensische Analyse an, bei Brand und anderen physischen Ursachen der Ersatz oder die Neuanschaffung von Hardware. Außerdem ist zu prüfen, ob durch die Unterbrechung Daten verloren gingen.

Dabei hilft ein vorher erarbeitetes Backup-Konzept. Es dokumentiert die jeweils aktuelle Backup-Infrastruktur mit sämtlichen Systemen und Datenmengen. Ein Backup-Konzept stellt zudem sicher, dass alle Ausfall-Szenarien abgedeckt sind, die relevanten Business-Anforderungen und gesetzlichen Vorgaben erfüllt werden und die Backup-Infrastruktur bestmöglich geschützt ist. ■

Cloud: Schutz der Daten liegt in der eigenen Verantwortung

Warum eine Sicherung von Office 365 unverzichtbar ist

Microsoft verpflichtet sich, bei Office 365 die technische Funktionsfähigkeit und Verfügbarkeit sowohl der Plattform als auch der Anwendungen zu gewährleisten. Von den Daten ist da nicht die Rede. Die fallen nach wie vor in die Verantwortung der Kunden.

■ Peter Marwan

Der Brand im **OVH**-Rechenzentrum in Straßburg Anfang März hat zahlreiche Diskussionen um die Sicherheit von Daten in der Cloud nach sich gezogen. Kein Wunder: Viele Nutzer hatten sich darauf verlassen, dass ihre Daten »in der Cloud« sicher sind. Die Kritik am Brandschutz ist vollkommen berechtigt, das bis in den Feuilleton der *FAZ* und den Wirtschaftsteil der *Zeit* vorgedrungene Jammern um den Verlust der Daten und die Sorge um einen Rückschlag für Europas Souveränitäts-Bemühungen dagegen nicht.

Denn bei fast allen Cloud-Angeboten sind die Kunden für die Sicherung ihrer Daten verantwortlich. Der Cloud-Betreiber übernimmt in der Regel die Verantwortung für den Betrieb der Infrastruktur, als SaaS-Anbieter auch der Anwendungen. Aber schon bei Dateien, die Anwender in den Papierkorb verschieben, hört sein Verantwortungsbereich auf – wie kürzlich Nutzer von *Google Drive* lernen mussten.

Dabei ist **Google** keine unrühmliche Ausnahme. Auch **Salesforce** hatte im Sommer 2020 sein Angebot *Data Recovery* eingestellt und verweist seitdem auf Anbieter wie **Avepoint**, **Commvault**, **Druva**, **SEP** und **Netapp**, die diese Aufgabe schon länger, wesentlich effizienter und schneller sowie oft sogar günstiger als Salesforce erledigen können.

Ähnliches gilt für *Microsoft 365* (einst *Office 365*). Auch hier sind die hauseigenen Backup-Werkzeuge – vor allem bei den günstigeren Tarifvarianten – völlig unzureichend. Zum Beispiel erstellt **Microsoft** Backups von Inhalten in *SharePoint* und *OneDrive* nur alle zwölf Stunden, Backups von Sharepoint-Daten hält es standardmäßig nur 30 Tage, solche aus OneDrive nur vierzehn Tage vor. Einzelne, gelöschte Dateien oder E-Mails stellt Microsoft überhaupt nicht wieder her.

Dass Microsoft diesen Sachverhalt nicht direkt als erstes erwähnt, ist verständlich. Allerdings weist es in seiner Leistungsvereinbarung ebenso wie andere SaaS-Anbieter deutlich auf das Konzept der »Shared Responsability« – also der geteilten Verantwortung hin. Der Konzern empfiehlt inzwischen im Rahmen seines »ISV Showcase« als Security- und Storage-Lösung **Barracuda** für die Sicherung von Office 365. Das Unternehmen bietet das *Cloud-to-Cloud-Backup* genannte Produkt seit kurzem nicht nur für E-Mail, sondern auch für Onedrive, Sharepoint und *Microsoft Teams* an. Schließlich sind bei der Nutzung dieser Tools im Unternehmen auch dort geschäftsrelevante Daten enthalten, die daher ebenfalls gesetzeskonform gesichert werden müssen. Alternativ können Firmen auch hier Dienste von Avepoint, Commvault, Druva, SEP und Netapp nutzen. Auch **Arcserve**, **Datto** und **Veeam** haben entsprechende Angebote. Mit der Übernahme von Altaro ist auch **Hornetsecurity** in diesen Markt eingestiegen. Für KMU, die lediglich Microsoft 365 verwenden, bietet **Synology** als Teil seiner Firmware und **Qnap** mit der Software *Boxafe* Sicherungsoptionen.

Die Möglichkeiten zur Sicherung von Office 365 sind also vorhanden. Welche für das eigene Unternehmen jeweils die beste ist, hängt auch davon ab, welche weiteren SaaS-Anwendungen sonst noch genutzt und ob die mit abgedeckt werden. ■

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.

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. ■

Grafik: speicherguide.de

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

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, Peter Marwan

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:
Foto: iStockphoto.com / Erich Fend

Mediaberatung:
Bettina Röber
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

Peter Marwan
Redaktion
speicherguide.de

Bettina Röber
Mediaberatung
speicherguide.de