

iX *extra* Juni 2023 **Storage**

Backup und Archivierung

Cloud-Backup: viele Varianten und schwierige Auswahl

Vorteile des Cloud-Backups

Seite 104

Marktübersicht: Anbieter von Backup as a Service (BaaS)

Seite 108

Sicherung von Cloud-Softwarediensten

Seite 110

Ransomware, die allgegenwärtige Bedrohung

Seite 112

Vorschau aufs nächste iX extra:

Cloud: Identity and Access Management – IAM-Fähigkeiten von Cloud-Anbietern

Seite 113



iX extra zum Nachschlagen:
www.ix.de/extra

Cloud-Backup: viele Varianten und schwere Wahl

Daten in der Cloud zu sichern wird immer beliebter. Wer sich für diese Variante des Backups entscheidet, hat die Wahl zwischen vielen Anbietern. Welcher den eigenen Bedürfnissen am ehesten entgegenkommt, ist in der Fülle der Offerten schwer auszumachen.

■ Bis 2025 sollen sich 100 Zetabyte, also einhundert Milliarden TByte, in der Cloud befinden, schätzt das Cloud-Consulting-Unternehmen Sequafy in seinen „26 Cloud Computing Statistiken & Trends 2023“ (siehe ix.de/z481). Wie viel davon Backup-Daten sind, ist nicht klar. Klar ist allerdings, dass die Nachfrage nach Backup-Services aus der Cloud steigt.

Dazu gibt es unterschiedliche Prognosen, die alle eine deutliche Tendenz nach oben haben. Einige Beispiele: Laut dem Marktforschungsunternehmen imarc erreichte der weltweite Cloud-Backup-Markt 2022 ein Volumen von 3,7 Milliarden US-Dollar, bis 2028 sollen es 11 Milliarden Dollar sein. Ein anderes Marktforschungsunternehmen, Technavio, gibt das weltweite Marktvolumen von Backup as a Service (BaaS) für das Jahr 2021 mit 17,73 Milliarden Dollar an und prognostiziert für die Zeit bis 2026 ein durchschnittliches jährliches Wachstum von 33,15 Prozent. Was immer von solchen Prognosen zu halten ist: Unzweifelhaft sind Backup-Services zu einem wichtigen Betätigungsfeld der Cloud-Service-Provider geworden und ihre Bedeutung steigt weiter.

Vorteile des Cloud-Backups

Das verwundert nicht, denn die Vorteile des Cloud-Backups liegen auf der Hand: Die Daten werden von Profis auf Clouds gehalten, wo der Ausfall einer Festplatte keine Katastrophe ist, sondern einfach kompensiert wird. Brennt das eigene Geschäft ab, liegen die Daten andernorts.

Dazu sinken die Belastung des Storage-Personals und der Hardwarebedarf: Wer keine eigenen Sicherungen im Haus fährt und hält, braucht auch keine Backup-Systeme und -medien, muss alte Medien nicht von Zeit zu Zeit migrieren und so weiter. Wer Backup as a Service bucht, muss sich nicht mehr groß kümmern, denn der Provider übernimmt die Aufgabe, die Daten zu den festgelegten Zeiten aus den Systemen zu pumpen, und auch, sie bei Bedarf wieder zu-

rückzuspielen. Den Konfigurationsaufwand, also die Bestimmung dessen, was und wie oft gesichert werden soll, kann auch hier den Anwendern niemand abnehmen. Die Bedienfunktionen sind meist über eine Browseroberfläche zugänglich, deren Benutzung im Vergleich zu den früheren Bedienschnittstellen der Backup-Anwendungen in der Regel wesentlich einfacher ist.

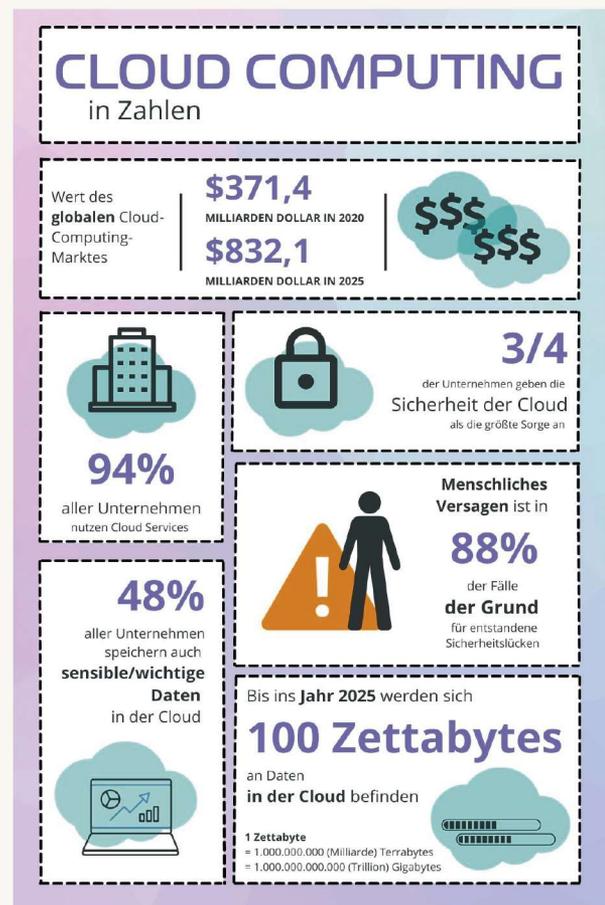
Cloud-Backup-Angebote gibt es in den unterschiedlichsten Größenordnungen – wer nur einen einzigen Computer sichern muss, bekommt schon für einen einstelligen Eurobetrag monatlich einen anständigen Service. Wer alle möglichen Systeme und große Speichervolumina zu sichern hat, muss notwendigerweise mehr berappen. Anbieter können Hyperscaler oder traditionelle Backup-Software-Spezialisten sein, aber auch kleinere Cloud-Provider, die sich an eine regionale oder branchenspezifische Zielgruppe wenden. Letztere kooperieren oft mit Backup-Software-Spezialisten wie Acronis oder Veeam, die spezielle Programme für Managed-Service-Provider auflegen. Diese bieten dann ihren Kunden Backup as a Service auf Basis der betreffenden Software an.

Ein Testbetrieb empfiehlt sich

Der Einstieg in die Nutzung von BaaS ist in der Regel einfach: Man legt

einen Account bei einem Provider an, macht die nötigen Eingaben, legt zum Beispiel die zu sichernden Laufwerke, Dateien oder Ordner fest, den Backup-Rhythmus und andere Feinheiten und kann loslegen. Anders sieht es aus, falls auf den zu sichernden Clients, Servern oder mobilen Endgeräten Agenten zu installieren sind. Hier ist etwas Vorarbeit erforderlich; aber solche Angebote kommen auch eher nicht als BaaS, sondern als konventionelle Backup-Software mit der Cloud als einem der möglichen Speicherorte daher und sind hier nicht Gegenstand. Die Marktübersicht liefert Informationen zu in Deutschland verfügbaren BaaS-Angeboten. Zugrunde liegen die bei einer Webrecherche zugänglichen Informationen. Aufgrund der zahlreichen Anbieter ist die Liste nicht vollständig.

Empfehlenswert ist auf jeden Fall ein vorüberiger Testbetrieb. Wer die Funktionsfähigkeit und -vielfalt, die Benutzeroberfläche und den Bedienkomfort eines Backup-Service aus der Cloud testen will, sollte auf jeden Fall erst einmal mit einem oder wenigen Rechnern anfangen. Möglicherweise stellt der Provider Unternehmenskunden auch eine



Nicht nur immer mehr, sondern auch immer sensiblere Daten landen in der Cloud, und das, obwohl die Sicherheit der Daten in der Cloud drei Viertel aller Firmen Kopfschmerzen bereitet (Abb. 1).

EINFACHE DATENSICHERUNG MIT DER StarWind Backup Appliance

Moderne Unternehmen können sich Ausfallzeiten schlicht nicht leisten. Sie müssen gewährleisten, dass ihre Daten zuverlässig geschützt sind und bei Bedarf schnellstmöglich wiederhergestellt werden können. Mit herkömmlichen, festplattenbasierten Backup-Systemen ist jedoch nicht nur die Sicherung von Daten, sondern auch ihre Wiederherstellung mit erheblichem Zeitaufwand verbunden.

Darüber hinaus sind die Ressourcen in kleinen bis mittleren Unternehmen sowie in den Außen- und Zweigstellen (Remote Office/Branch Office, ROBO) großer Unternehmen oft beschränkt. IT-Abteilungen sind deshalb gezwungen, diese Ressourcen möglichst effizient zu nutzen. Da der Backup-Server in solchen Umgebungen in der Regel erst nachträglich implementiert wird, kann es passieren, dass er zum Storage-Engpass wird.

Mit der StarWind Backup Appliance lassen sich die meist zeitaufwendigen Prozesse für Datensicherung und Wiederherstellung erheblich beschleunigen. Sie kombiniert Technologien, die bislang nicht kompatibel waren, und stellt somit eine Komplettlösung für die Datensicherung bereit, die sich die Performance von vollständig NVMe-basiertem Storage zunutze macht.

Die StarWind Backup Appliance ermöglicht eine deutlich längere Nutzung Ihrer Backup-Infrastruktur und bietet leistungsstarke Funktionen für die Datensicherung und Wiederherstellung. Sie ist damit eine intelligente Lösung für Unternehmen, die ihre Backup-Strategie optimieren möchten.



Die Appliance kombiniert modernste Hardware (NVMe, CPUs der neuesten Generation) und Software (StarWind SAN & NAS, Veeam Backup & Replication) in einem kompakten Gehäuse, das mit 1 HE nur wenig Platz benötigt. Durch den Einsatz neuester Technologien ist sie auf ein lange Nutzungsdauer, einfache Skalierbarkeit, ein optimiertes Management und Ransomware-Schutz auf mehreren Ebenen (lokal, VTL und Cloud) ausgelegt.

Die Appliance kombiniert modernste Hardware (NVMe, CPUs der neuesten Generation) und Software (StarWind SAN & NAS, Veeam Backup & Replication) in einem kompakten Gehäuse, das mit 1 HE nur wenig Platz benötigt. Durch den Einsatz neuester Technologien ist sie auf ein lange Nutzungsdauer, einfache Skalierbarkeit, ein optimiertes Management und Ransomware-Schutz auf mehreren Ebenen (lokal, VTL und Cloud) ausgelegt.

Dank ihrer transparenten Architektur lässt sich die StarWind Backup Appliance einfach verwalten und ermöglicht eine unkomplizierte Überwachung Ihrer Backups. Die Lösung wird nach Ihren individuellen Anforderungen vorkonfiguriert. Die Experten von StarWind unterstützen Sie ohne Aufpreis bei der Integration und Migration von Backups.

Die StarWind Backup Appliance ist die ideale Lösung für KMU und die ROBO- Umgebungen großer Unternehmen, die die Verwaltung ihrer Backup-Prozesse vereinfachen, Engpässe bei der Datensicherung vermeiden und im Katastrophenfall eine schnelle Wiederherstellung ihrer Daten gewährleisten möchten.

intel

Intel® NVMe SSDs

derzeit schnellster
verfügbarer Speicher



Intel® Xeon® Ice
Lake CPUs

die neueste Generation von
Intel-Prozessoren



GRAID
SupremeRAID™

die weltweit erste
NVMe-oF-RAID-Karte

StarWind
HYPERCONVERGENCE

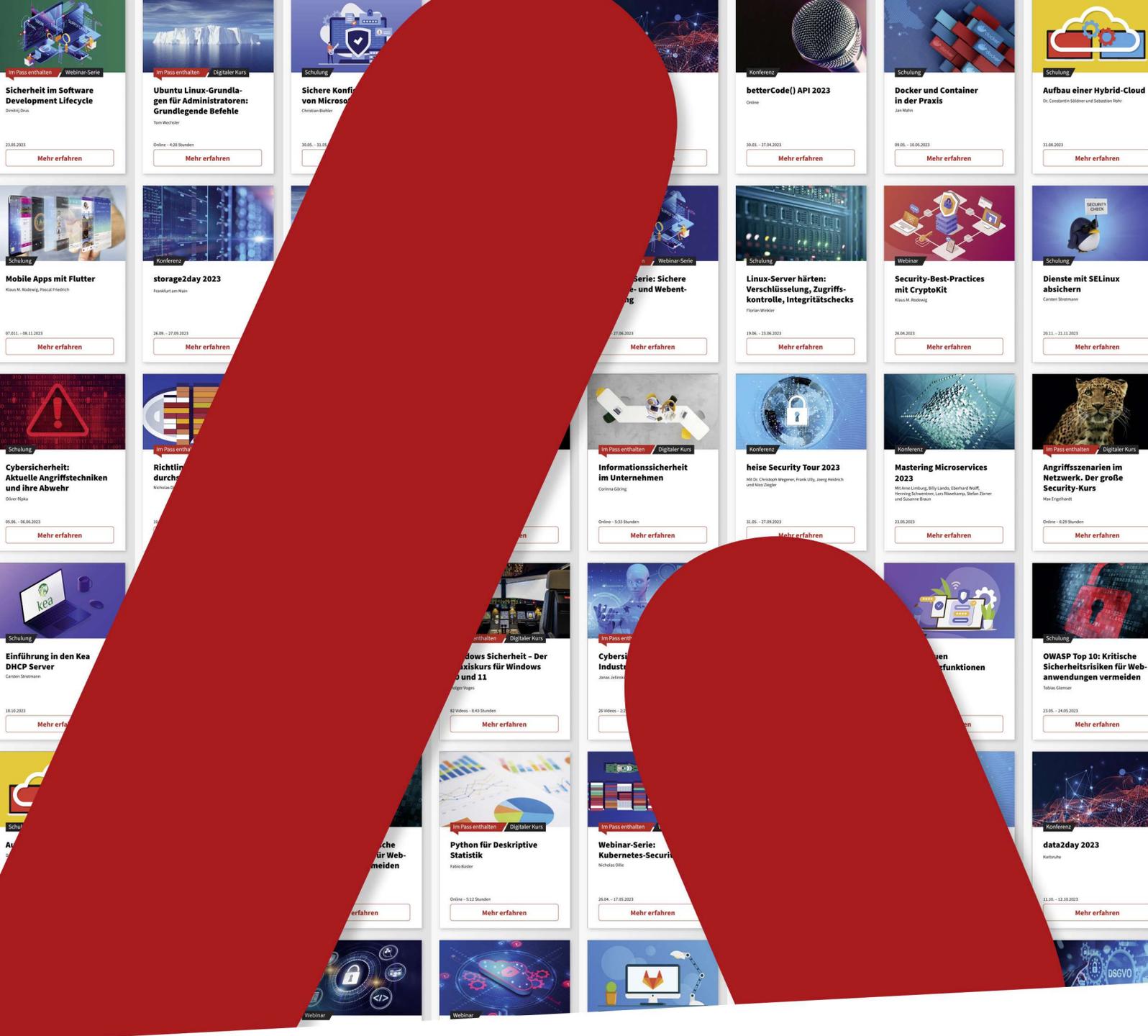
StarWind SDS

unübertroffene
Speichervirtualisierung



Für weitere Informationen:
starwindsoftware.com

Für Anfragen und Fragen:
sales@starwind.com



Wissenslücken? Nicht mit uns!

Wir helfen Ihnen dabei, die IT-Themen zu lernen, die heute – und morgen – wichtig sind.

Die Zukunft des Lernens ist digital:

Die heise Academy bietet Ihren IT-Teams die Weiterbildungslösungen an, die Sie benötigen. Lassen Sie Ihre Fachkräfte nach Bedarf und direkt am Arbeitsplatz lernen.

Intensivieren Sie diese Lernerfahrung mit relevanten, topaktuellen Schulungen und Webinaren. Sichern Sie sich das IT-Wissen, das Ihr Unternehmen heute – und morgen – braucht: bei **heise Academy, dem Zuhause Ihrer professionellen IT-Weiterbildung.**



Storage

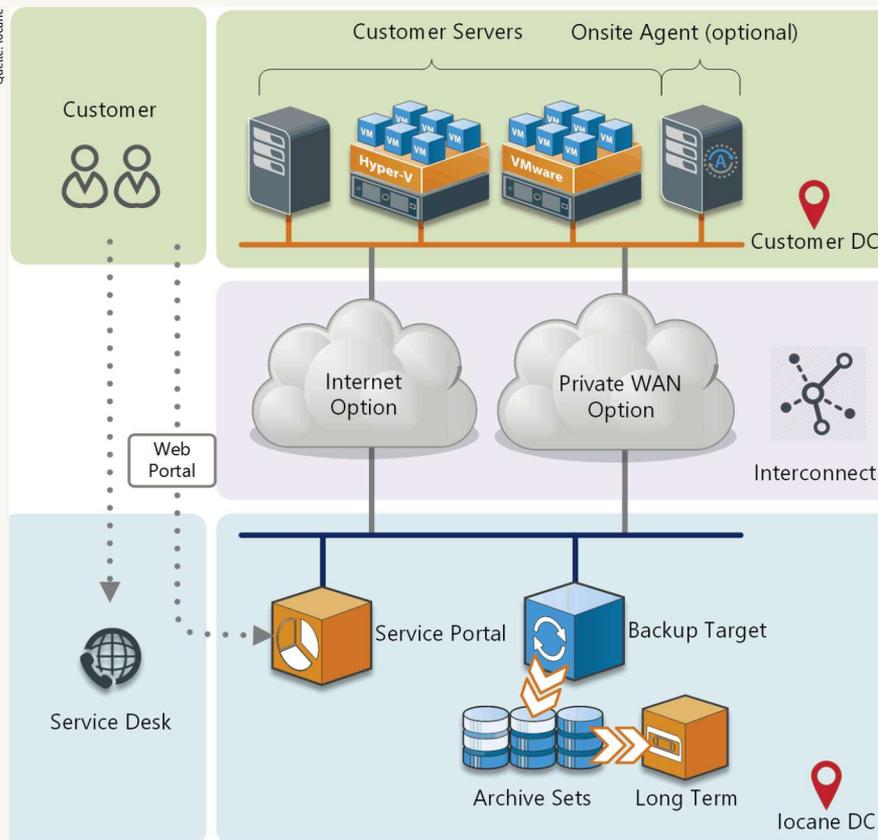
Virtuelle und physische Server samt Daten werden mit oder ohne Agent über öffentliche oder private Leitungen in die Rechenzentren der BaaS-Provider gesichert, daneben haben Kunden Zugriff auf das webbasierte Serviceportal und den Service Desk (Abb. 2).

Quelle: locane

Testversion zur Verfügung oder erlaubt die kostenlose testweise Nutzung des vollen Funktionsumfangs über eine gewisse Zeitspanne und mit begrenzter Kapazität.

Bei Tests ist auch darauf zu achten, wie sehr die Backups die CPU und die I/O- und Netzwerkpfade der Systeme belasten. Gerade bei der CPU-Belastung können sich die Angebote sehr stark unterscheiden. Das liegt vor allem an der unterschiedlichen Priorisierung der Backup-Jobs. Eine hohe Belastung der CPU ist auf jeden Fall ein Minuspunkt.

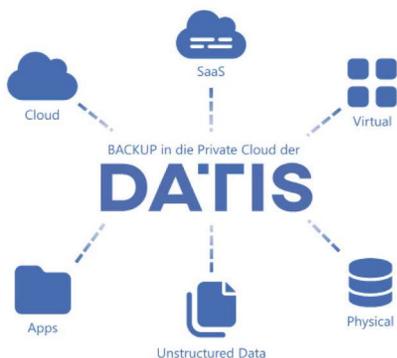
Genauso wichtig sind die Up- und Downloadzeiten. Profis sollten sie messen, bevor sie ein längerfristiges Engagement eingehen. Natürlich sind schnelle Up- und Downloads besser als langsame, solange die Geschwin-



ANZEIGE

Mit Backup as a Service von DATIS auf der sicheren Seite

Viele Unternehmen vernachlässigen das Backup ihrer Daten. Die Gründe dafür: Ihr Tagesgeschäft beansprucht sie derart, dass kaum noch Zeit für anderes bleibt oder sie verfügen vor dem Hintergrund des Fachkräftemangels gar nicht mehr über die Ressourcen. In solchen Fällen hilft Backup as a Service (BaaS). Die zeitintensive Datensicherungsroutine wird über einen gesicherten Zugriff durch einen Dienstleister übernommen. Denn eine professionelle Datensicherung wird immer aufwendiger, nicht zuletzt, weil Cyberbedrohungen zunehmen und der Digitalisierungsgrad steigt.



Datensicherung von DATIS auf höchstem Niveau

Die Rechenzentrums-Experten der DATIS bieten Unternehmen flexibel skalierbare BaaS-Lösungen für ihre IT-Systeme an. Dabei erfolgt die Datensicherung in eine Private Cloud von DATIS nach der goldenen 3-2-1-1-0-Regel und erfüllt damit höchste Sicherheitsstandards. Dazu zählen Backup und Restore an sieben Tagen die Woche, rund um die Uhr, eine verschlüsselte Ablage der Daten sowie eine dezidierte Überwachung der angelegten Repositories. DATIS setzt dabei auf den-Technologiemarktführer Veeam. Damit werden sämtliche Multi-Cloud-Ansätze der Unternehmen abgedeckt, denn Veeam unterstützt u.a. Cloud-Plattformen wie AWS, Microsoft Azure oder Google Cloud.

Bei Cloud-Anwendungen immer an Backups denken

Viele Unternehmen setzen Microsoft 365 ein und bedenken dabei oftmals nicht, dass Microsoft lediglich die Infrastruktur der Cloud-Anwendungen liefert. Ein regelmäßiges Backup und damit die Sicherung der dort abgelegten Daten werden in diesem Kontext oftmals vernachlässigt. Auch hier schafft BaaS von DATIS Abhilfe: Die IT-Experten leisten die Sicherung von Exchange, SharePoint, OneDrive und Teams. Durch die Ablage der Backups in der Private Cloud von DATIS lassen sich problemlos einzelne Objekte und auch mehr wiederherstellen.

Im worst case: Ausfallzeiten mit Disaster Recovery von DATIS minimieren

Abgerundet wird das BaaS-Portfolio der DATIS durch ausgefeilte Disaster-Recovery-Services (DRaaS). Diese sorgen dafür, dass Unternehmen etwa nach einem Betriebsausfall oder Cyberangriff über sichere VPN-Tunnels schnellstmöglich Zugriff auf ihre IT-Infrastruktur bekommen und die Funktionsfähigkeit ihrer Systeme wiederherstellen können. Die Anforderungen hierbei sind vielfältig, sodass die IT-Experten der DATIS diese gemeinsam mit den Unternehmen individuell konzeptionieren.

Sie haben Fragen? Dann rufen Sie uns gerne an oder schreiben Sie uns! In unseren Rechenzentren sind Ihre Daten ganz sicher in den besten Händen.

Maximilian Münch
DATIS Business Development
+4962172703528
maximilian.muench@datis.de

Anbieter von Backup as a Service (BaaS)

Anbieter	Produktname	Preis	Zielgruppe
Acronis	Acronis Cyber Protect für Unternehmen	ab 70,99 Euro/Monat	Unternehmen aller Größen
Adestis	Backup as a Service	Managed Service, Preis auf Anfrage	KMU
Advanced UniByte	Backup as a Service	Managed Service, Preis auf Anfrage	KMU
Alfahosting	Cloud-Backup	sechs Tarifmodelle für 1 oder 3 Computer, Preise von 14,99 Euro/Monat (1 Computer, 12 Monate, 300 GByte) bis 30,99 Euro/Monat (3 Computer, 1 Monat, 600 GByte)	KMU
B2B Backup	Managed Backup Service	Preiskalkulator im Web; Preisbeispiel: 10 VM, 2 physische Server, 20 PCs/Notebooks, 20 MS-365-User, 24/7-Support: 371,60 Euro/Monat	KMU
Backblaze	Backup	Business-Veeam-Backup: 5 US-Dollar/TByte im Monat, Downloads 0,01 US-Dollar/TByte im Monat oder 1520 US-Dollar/10 TByte im Jahr; Computer-Backup: 7 US-Dollar/Monat pro Rechner; Server-Backup: 5 US-Dollar/Monat pro Server; Laufzeiten: 1 Monat, 1 Jahr, 24 Monate	Unternehmen aller Größen
Bechtle	Backup as a Service	auf Anfrage	Mittelstand
bestserv	BaaS	3 Euro/Monat pro MS-Office-365-Lizenz	KMU
Cancom	Backup as a Service	Managed Service, Preis richtet sich nach gesicherten VMs, gebuchtem Repository-Volumen und Datenverkehr	KMU
Carbonite (Open Text)	Cloud-to-Cloud-Backup	Laufzeit 1–12 Monate; von 6 US-Dollar/Monat (69 US-Dollar jährlich) bis 150 GByte; in vier Stufen bis 29 US-Dollar/Monat (320 US-Dollar jährlich) bei 5 TByte	Nutzer der Onlineanwendungen
Clumio	Protect	nutzungsbasierte Preise je nach Servicelevel des Backups; mehrere Preiskomponenten; Beispiel: inkrementelle Standard-S3-Backups 0,025 US-Dollar gesicherte Daten (pro GByte und Monat), 0,040 US-Dollar Wiederherstellung (pro GByte und Monat), 0,025 frühzeitige Löschung (pro GByte und Monat), 1,50 US-Dollar pro Million gemanagter Objekte im Monat	Nutzer von AWS-Services
Commvault	Metallic	unterschiedliche Module zu unterschiedlichen Preisen; Beispiel: Modul Kubernetes/VMs: Preisstaffel von 84,78 Euro/Monat (für bis zu 49 × 10 VMs) bis 63,77 Euro/Monat (für bis zu 999 × 10 VMs)	mittlere und größere Unternehmen
CrashPlan	Cloud Data Backup	Enterprise: Preis auf Anfrage, ab 100 User; SMB (bis 100 User): 9,99 US-Dollar pro Endgerät	Unternehmen aller Größen
DARZ	BackupaaS	Managed Service, Preis auf Anfrage	KMU
Datis	Online Backup made in Germany	Managed Service, Preis auf Anfrage	KMU, unter 50 TByte Volumen/Monat
Druva	Data Resiliency Cloud	RZ-Backup: ab 210 US-Dollar/TByte und Monat; SaaS: ab 2,50 US-Dollar/User und Monat; Endpunkte ab 8 US-Dollar/User und Monat; AWS-Server ab 7 US-Dollar/User und Monat	größere Unternehmen
dogado	Online-Backup	Vertragslaufzeit 1 Jahr; MS 365: 4,90 Euro/Monat für 1 Gerät, (150 GByte); Clients: 14,90 Euro/Monat, für 1 Gerät, (300 GByte); Server: 89,90 Euro/Monat für ein Gerät (1 TByte)	KMU
fks-IT	Smart Backup Server	Managed Service, Preis auf Anfrage	KMU, NetApp-Anwender, Hamburg und Umgebung
Fritz ManagedIT	Managed Backup / Online-Backup / Cloud Backup	Fritz Managed Standard: 39 Euro/Monat pro virt. Server, 1 TByte; FritzBackup Advanced 49 Euro/Monat pro virt./phys. Server, 2,5 TByte; FritzBackup Disaster Recovery 89 Euro/Monat pro virt./phys. Server, 1 TByte	KMU
IDrive	Cloud-Backup	diverse Abos (ab 1,25 TByte: Monat / 1 Jahr / 2 Jahre): von 250 GByte: 74,62 US-Dollar/Jahr, 149,25 US-Dollar / 2 Jahre bis 12,5 TByte: 299,95 US-Dollar/Monat, 2249,62 US-Dollar/Jahr; 4499,25 US-Dollar / 2 Jahre	KMU
Inneo	Safe Protect -S3	Managed Service, Preis auf Anfrage	KMU
INS	Backup as a Service	Managed Service, Preis auf Anfrage	KMU
Ionos	MyDefender	ab 2,50 Euro/Monat (für 100 GByte)	KMU
Ionos	Cloud Backup by Acronis	ab 7 Euro/Monat (für 100 GByte)	größere Unternehmen

digkeit nicht zulasten anderer Anwendungen geht. Die fehlerfreie Übermittlung der zum Backup vorgesehenen Daten sollte bei Backup-Services sowieso selbstverständlich sein.

Gebühren und Laufzeiten vergleichen

Gebühren erheben die Anbieter in den Abomodellen üblicherweise monatlich, aber

auch jährlich. Sie berechnen sich meist durch die Zahl der zu sichernden Geräte. Dabei unterscheiden die Anbieter in der Regel zwischen Clientcomputern respektive Endgeräten und Servern. Angebote, die Server sichern, sind teurer. Manchmal gibt es Zusatzgebühren beispielsweise für Mobilsysteme oder zusätzliche Leistungen.

Ein wichtiges Kriterium ist auch die Vertragslaufzeit: Kann man den Dienst monatlich oder noch kurzfristiger kündigen? Oder

ist eine langfristige Bindung notwendig? Falls beide Modelle verfügbar sind, sollte man sich die Preisstruktur genau ansehen. Denn oft bezahlt der Anwender die höhere Flexibilität durch die kürzere Vertragslaufzeit mit höheren Gebühren. Deshalb sollte man sich auch genau ansehen, was passiert, wenn die vorgesehene Kapazität überschritten wird: Ist es möglich, sofort und unkompliziert mehr zu beanspruchen – zu den dann fälligen höheren Tarifen natürlich –

Besonderheiten	URL
integrierte Sicherheitsfunktionen, sichert physische, virtuelle, Cloud- und Mobilgeräte, Ransomware-Schutz, Bare-Metal-Recovery, CDP, Any-to-any-Migration, Deduplizierung	www.acronis.com
Speicherung in Deutschland	www.adeptis.com
Kooperationspartner: NetApp; Speicherung in deutschem Tier-III+-RZ, auditfähige DR, mobile Speichermedien für den Notfall	www.au.de
begrenzte Gerätezahl (1 oder 3 Computer), Speicherung in Deutschland, sichert Windows und macOS, Monatsrate mit Einrichtungsgebühr (4,99 Euro), Verschlüsselung, keine Sicherung von Mobilsystemen	alfahosting.de/online-backup
georedundante Speicherung in Deutschland (Berlin/Hamburg), zwei- bis vierstufiges Backup, Ende-zu-Ende-Verschlüsselung, alle Datenquellen, Testrückversicherungen, auf Wunsch Bandsicherung, erweitertes Reporting, Kalkulator im Web	www.b2b-backup.de
Kooperationspartner beim Server-Backup: MSP360; sichert Computer und Server, Veeam-Backups (zusätzlicher Cloud-Tier) und NAS (Integration mit Synology, QNAP, TrueNAS), Zwei-Faktor-Authentisierung, Speicherung in den USA und Europa, Ransomware-Schutz, eigener Cloud-S3-Storage (kostengünstiger als AWS)	www.backblaze.com
Kooperationspartner: Veeam (Cloud Connect, WAN-Accelerator: 50-mal beschleunigter Transport, verbindet sich mit Veeam-Backup-Jobs in Bechtle-Cloud), NetApp (AltaVault, Snap Mirror: Datenreduzierung bis 30:1, kompatibel mit den meisten Backup-Lösungen); Speicherung in deutschen Tier-3-Rechenzentren	www.bechtle.com
sichert nur MS Office 365, Speicherung in Deutschland, Recovery bis zu 90 Tagen rollierend	www.bestserv.de
Kooperationspartner: Veeam; Georedundanz, Selbstbedienungsportal, Hochsicherheits-RZ, im Notfall Lieferung physischer Speichermedien, nutzungsbasierte Abrechnung, maximales Änderungsvolumen: täglich 300 GByte/Repository	www.cancom.de
unterstützt Salesforce, Windows 365 (gesamte Office-Suite), Google Workspace, Box und Dropbox, bis zu vier automatische Backups täglich, Ransomware-Schutz	www.carbonite.com
schützt AWS-Cloud-Services: EC2-Datenbanken, EBS, S3, DynamoDB, MySQL, PostgreSQL, Oracle, Microsoft SQL Server, MariaDB und NoSQL, automatisiertes Data Lifecycle Management, granulare Wiederherstellung	clumio.com/platform/protect
separate Sicherungsmodule für Kubernetes/VMs, Datenbanken, Files und Objekte, Office 365, Dynamics 365, Salesforce; Zusatzmodule für Ransomware-Schutz, DR, Government Cloud, übersichtlicher Onlinepreiskalkulator	www.commvault.com/metallic
unbegrenzte Gerätezahl, unbegrenzter Speicherplatz, Ransomware-Schutz, Migrationsunterstützung (MS USMT), sichert ausschließlich Files, Windows/macOS/Linux, keine Mobilgeräte, Anwender kann Speicherort konfigurieren (RZ in Irland und Kontinentaleuropa), Multi-Faktor-Authentisierung möglich	www.crashplan.com
Kooperationspartner: Veeam; verfügbar über DE-CIX, Sicherung in Deutschland, keine Up-/Downloadkosten, Option: DR	da-rz.de/backup-aas
Kooperationspartner: Veeam; Speicherung in Deutschland	www.datis.de
Services für RZ-Backup, SaaS-Backup (MS 365, Google Workspace, Salesforce), Endpunkt-Backup und AWS-Backup, Cloud-DR, Ransomware-Schutz	www.druva.com
Speicherung in Deutschland; Plattformen: Windows/macOS; Speicherung lokal oder in der Cloud, Serverversion sichert Active Directory, MySQL, MS Exchange, MS SharePoint, Recovery von VMs, Bare Metal Recovery	www.dogado.de/digitales-buero/online-backup
Kooperationspartner: NetApp, auch DR; Speicherung in Deutschland (Hamburg-Cloud)	www.fks-it.de/baas
inkludierte Antivirus-/Anti-Malware-Software, bei Advanced darüber hinaus CDP, Cluster, SAP-HANA- und Oracle-DB-Unterstützung; bei DR darüber hinaus: Cloud-DR, Site2Site-VPN; Speicherung in Deutschland	www.fritz.gmbh
unbegrenzte Gerätezahl, sichert Server (MS SQL, MS Exchange, Hyper-V, MS SharePoint, Oracle, Linux), Clients, Mobilgeräte und angeschlossene Laufwerke, Einrichtung von Subaccounts möglich, Kompression, CDP, sichert auch Cloud/SaaS, Speicherort unklar, Lieferung eines Offlinespeichermediums ins Haus, geräteübergreifende Onlinesynchronisation	www.idrive.com/de/small-business
Kooperationspartner: NetApp; Speicherung in Deutschland, nur unstrukturierte Daten	www.inneo.de
Kooperationspartner: Veeam, Acronis, S3-Storage-Provider; lokale und Cloud-Sicherung	www.ins-online.ne
RZ in Deutschland, sichert vielfältige Systeme; optional: MS-365-Backup	www.ionos.com
sichert alle Geräte, virtuelle Server, Browserschnittstelle, integrierter Cyberschutz, Update-Management, 1-Click-Recovery	www.ionos.com

oder müssen erst umständliche Prozesse absolviert werden, ehe der nötige zusätzliche Speicherraum verfügbar ist?

Plattformvielfalt wünschenswert

Wichtig ist es, bei der Auswahl auf die unterstützten Betriebssysteme und Endgeräte zu achten. Was nützt der schönste Backup-Schutz für den Computer auf dem Schreibtisch, wenn die Hauptarbeit an mobilen Ge-

räten außerhalb der Firmenräume stattfindet und diese nicht gesichert werden können? Zwar decken die meisten Angebote für Firmenkunden ein breites Spektrum unterstützter Betriebssysteme ab, dennoch sollte man genau hinsehen. Carbonite beispielsweise sichert lediglich Windows und Mac, nicht aber Tablets, Smartphones oder Linux-Systeme.

Zu den Plattformen gehören heute selbstverständlich auch die diversen Hypervisor-

ren – schließlich weicht die dedizierte IT schon seit 20 Jahren virtualisierten und jetzt auch cloudifizierten Infrastrukturen. Je länger die Liste der unterstützten Hypervisoren, desto flexibler ist der Service einsetzbar. Wer allerdings eine Umgebung fährt, die konsequent nur einen Hypervisor verwendet, kommt auch mit einem Dienstleister hin, der seine Backup-Services nur dafür anbietet. Unternehmen, die schnell und oft auch durch Aufkäufe wachsen, sollten die gewünschte

Anbieter von Backup as a Service (BaaS)

Anbieter	Produktname	Preis	Zielgruppe
IS4IT	Backup as a Service @ IS4IT	Managed Service, Preis auf Anfrage	KMU
IT-Haus	Backup as a Service by IT-Haus	Managed Service; Veeam Backup for MS 365: 3,50 Euro/Monat pro User + 15 Euro/500 GByte; Veeam Cloud Connect (VM) ab 10 Euro/Monat pro VM + 40 Euro/500 GByte; Virtual Tape Out (S3) ab 15 Euro/500 GByte	KMU
Kyndryl	Backup as a Service	Managed Service, Preis auf Anfrage	große Unternehmen
Mivitec	Backup as a Service	Managed Service, Preis auf Anfrage	KMU
MXP	MXP Cloud Backup	Managed Service, Preis auf Anfrage	KMU
net.de	Veeam Backup as a Service	Managed Service, Preis auf Anfrage	KMU
nlx.cloud	Backup as a Service	Managed Service, Preis auf Anfrage	KMU
Real Cloud	Backup in der Cloud	Managed Service, Preis auf Anfrage	Mittelstand
Operational Services	Cloud Backup as a Service	Managed Service, Preis auf Anfrage	KMU
OVH Cloud	Veeam Managed Backup	neun Tarifvarianten/Servicelevels; Standard, Advanced, Premium; Beispiele: Standard, VM mit 250 GByte: 7,14 Euro inkl. MwSt. monatlich pro VM; Premium, VM bis 2 GByte: 356 Euro inkl. MwSt. monatlich pro VM	KMU
PlusServer	plusbackup	Speicherplatz: ab 0,035 Euro/GByte; Lizenzen: ab 2 Euro/Client bei vorhandener Veeam-Lizenz, ohne Veeam-Lizenz: 14,65 Euro/Client	KMU
Spider Oak	One Backup	Laufzeit 1–12 Monate; von 6 US-Dollar/Monat (69 US-Dollar jährlich) bei bis zu 150 GByte in vier Stufen bis 29 US-Dollar/Monat (320 US-Dollar jährlich) bei 5 TByte	KMU
sc synergy	Backup as a Service	Managed Service, Paketpreise auf Anfrage	KMU
SHD	Cloud Backup	Managed Service, Preis auf Anfrage	KMU
SkySystems IT	Backup as a Service	Basic: 100 GByte, 49 Euro/Monat; Standard: 250 GByte, 99 Euro/Monat; Premium: 500 GByte, 149 Euro/Monat; Platinum: 1 TByte, 229 Euro/Monat	KMU
SVA	Backup as a Service	Managed Service, Preis auf Anfrage	Unternehmen aller Größen
Synology	C2 für Unternehmen	Business: 49,95 Euro/Monat (5 TByte, 250 Benutzer); Enterprise: 499,75 Euro/Monat (25 TByte)	Unternehmen aller Größen
Telekom	Managed Backup to Cloud / Managed Backup to Hybrid Cloud	Backup to Cloud: ab 20 Euro/Monat; Backup to Hybrid Cloud: Endgeräte: ab 1478 Euro; NAS-Anbindung ab 19,90 Euro	KMU
ucs	uBundle Backup & Replica	Managed Service, Preise pro TByte und lizenzierter VM	KMU
Windcloud	Backup as a Service	Preiskalkulator im Web; Preisbeispiel: 10 VM, 10 TByte: ab 355 Euro/Monat	KMU

Flexibilität eher höher gewichten, um auch die Infrastruktur einer Akquise sichern zu können, ohne sich einen neuen Backup-Provider suchen zu müssen.

Sicherung von Cloud-Softwarediensten

Unterstützt ein Service alle Plattformen, ist noch immer nicht sicher, dass er alle benötigten Daten auch tatsächlich wie gewünscht sichert. Häufig in separate Services ausgelagert und damit extra zu bezahlen ist etwa das Cloud-to-Cloud-Backup von Anwendungen wie Windows 365, Salesforce, Google Workspace oder Datenaustauschplattformen wie Dropbox oder Box.

Einen genauen Blick verdient Windows 365, auch aufgrund seiner Verbreitung. Hier ist zu klären, ob dessen Daten ebenfalls vom Backup-Service abgedeckt werden oder ob man dafür eventuell einen Zusatzservice braucht. Einige BaaS-Provider bieten

solche Dienste an. Cloud-Provider wie Microsoft Azure – oder wer auch immer Kundenanwendungen hostet – sind jedenfalls ohne Zubuchung entsprechender Sonderoptionen nicht für den Datenbestand der Kunden zuständig, sondern lediglich für die Systemumgebung. Bei einem Datenverlust in der Azure-Cloud etwa ist Microsoft ohne zusätzliche Vereinbarungen nicht haftbar zu machen.

Die Frage des Speicherorts

Darüber hinaus ist auch die Frage zu klären, ob die Daten ausschließlich in der Cloud oder auch auf Speichermedien on Premises landen dürfen oder sollen. Hier gibt es sehr unterschiedliche Konstellationen. Wer auch eine Inhouse-Kopie der Backup-Daten möchte, etwa um vom Anwender versehentlich gelöschte Daten auch bei einem temporären Ausfall des Providers zurückspielen zu können oder um Offlinekopien für den Fall einer

Ransomware-Attacke im Tresor zu haben, ist jedenfalls bei einem Cloud-only-Produkt an der falschen Adresse.

Sind vermehrt sensible Daten zu speichern, ist es wichtig zu wissen, wo genau sie liegen. Manche Provider geben nur vage an, ihre Daten lägen in eigenen Cloud-Rechenzentren ohne Ortsangabe oder irgendwo in den Rechenzentren der Hyperscaler. Das ist ein Ausschlusskriterium, wenn die gesicherten Daten der DSGVO oder anderen Schutzbestimmungen unterliegen, die das Speichern im nationalen oder zumindest europäischen Rechtsraum vorschreiben.

Verschlüsselung sollte sein

Wer seine Daten sicher speichern will, wird auch auf eine Verschlüsselung Wert legen. Zu achten ist auf den gewählten Algorithmus. 256 Bit lange Schlüssel sind heute State of the Art. Eine geringere Schlüssellänge ist demgemäß ein Minus.

Besonderheiten	URL
Varianten: BaaS Target: Einrichtung eines zweiten Backup-Target in der IS4IT-Cloud; BaaS All Remote: Neueinführung eines Managed BaaS; BaaS Local & Remote: lokaler und Cloud-Backup, Einführung der Managed-BaaS-Lösung, hochperformanter Restore; BaaS as Required: Individual-Backup-Lösung (z.B. VPN, Multi-Cloud-Replikation, lokale Hardware); Speicherung in Deutschland	www.is4it.de/backup-as-a-service
Kooperationspartner: Veeam (MS 365, Cloud Connect); S3-Tape-out, Datenspeicherung in Deutschland, Selbstbedienungsportal	www.it-haus.com/?s=baas
Speicherort und weitere Details unklar	www.kyndryl.com
Kooperationspartner: Arrow, Veeam; Speicherort München, Düsseldorf, auch Cloud-Backup, Server, physische/virtuelle Umgebungen, DR, redundante Speicherung	www.mivitec.de
Kooperationspartner: Acronis; Speicherung in Deutschland, Sicherung im Generationenprinzip (Tag/Woche/Monat)	www.mxp.de/hosting/cloud-backup
Kooperationspartner: Veeam; USB-Rescue-Stick, sichert PCs, Notebooks, Server	www.net.de/backup
Kooperationspartner: Veeam; integrierte WAN-Beschleunigung, redundante Speicherung in Deutschland (mehrere Brandabschnitte), unveränderlicher Speicher (Ransomware-Schutz), Langzeitaufbewahrung, sichert physische/virtuelle Server und Workstations	nlx.cloud
Kooperationspartner: DELL/EMC; Speicherung in Deutschland, Sicherung vor Ort und in der Cloud, bis zu 250 PByte Storage-Volumen, unterstützt viele Hypervisoren, sehr leistungsfähige Deduplizierung	realcloud.de/backup
Kooperationspartner: Veeam; Sicherung in Deutschland, Datenverschlüsselung optional, WAN-Beschleunigung optional	www.operational-services.de
Kooperationspartner: Veeam; Funktionen und Backup-Häufigkeit je nach Servicelevel, Langzeitspeicherung und Backup-Proxy pro Host nur bei Premium	www.ovhcloud.com
Kooperationspartner: Veeam (für Server, virtuelle Server, Clients on Premises, File Storage); Clientsoftwareinstallation und Backup-Agent erforderlich, Speicherung in Deutschland	www.plusserver.com/produkte/baas
unbegrenzte Gerätezahl, Point-in-Time-Recovery, keine Unterstützung von Mobilgeräten, Filesharing-Raum, Anwender übernimmt Schlüsselverwaltung, keine Angaben zum Speicherort	crossclave.com/one
Kooperationspartner: Commvault; Speicherung in mehreren deutschen Rechenzentren, interaktives Webinterface	scsnynergy.com
Kooperationspartner: NetApp; Speicherort Berlin, Tier-III-RZ; optional: DRaaS, On-Demand-Personal bei Wiederherstellung	www.shd-online.de
Kooperationspartner: Acronis; Speicherort Acronis-RZ, Verfügbarkeit 99,9 Prozent, monatlich kündbar, unbegrenzte Gerätezahl, sichert physische Server, VMs, MS 365, Mobilsysteme	www.sfc-software.de
individuelles Sicherungskonzept, schlüsselfertige Lösung, 30 Tage kostenloser Test, Speicherort nach Wahl, Garantie für individuell festgelegte Wiederherstellungszeit	www.sva.de/de/services/backup-as-a-service
granulare Recovery, beliebig viele Sicherungskopien, Rollenkonzept, E-Mail-Warnungen, auch MS-365-Backup	www.synology.com
sichert Server und Workstations, Sicherung in Private Telekom Cloud, Selbstbedienungsportal, Hybridlösung mit lokalem Backup on Premises	geschaeftskunden.telekom.de
Kooperationspartner: Veeam; Anbindung mit bis zu 10 GBit/s, Replizierungsressourcen mit 2,4 bis 2,7 GHz Taktrate	ww.ucs.cloud/backup-as-a-service
Kooperationspartner: Veeam, VMware; kohlendioxidfreie Datensicherung dank Windstrom, Speicherung in Deutschland	windcloud.de/produkte/cloud-backup

Zweitens ist die Schlüsselverwaltung wichtig. Oft wird angeboten, den Schlüssel selbst zu verwalten oder dies dem Provider zu überlassen. Wer dem Provider nicht wirklich traut, sollte die Schlüsselsebstverwaltung wählen. Dabei gilt es aber zu bedenken, dass, falls der Schlüssel beim Kunden verloren geht, jeder Zugang zu den Backups ebenfalls verwehrt ist. Denn der Provider hat in diesem Fall garantiert keinen Zugriff auf Schlüssel oder Daten.

Platzsparende Deduplizierung darf sein

Wer größere Datenmengen in der Cloud speichert, schätzt Deduplizierungsmechanismen, denn sie sparen Platz und damit Geld. Besonders wirksam ist die Deduplizierung mit variabler Blockgröße. Mit den vom Provider eingezogenen Egress-Gebühren haben die Anwender von Backup as a Service wenig zu schaffen. Mit ihnen lassen sich die

Provider den Datentransfer von der Cloud zurück zum Kunden entlohnen.

Sinnvoll sind außerdem inkrementelle Sicherungen, bei denen nur die Veränderungen zum letzten Backup weggeschrieben werden. Auch dieses Verfahren reduziert nicht nur das Backup-Volumen erheblich, sondern vor allem den Datenverkehr und entlastet damit die Netze.

Ein anderes Thema ist jedoch der Zeitbedarf beim Zurückspielen der Daten, denn er hängt maßgeblich vom Durchsatz, aber auch von der Software ab. Da bei Unternehmen oft genug etliche TByte wiederherzustellen sind, kann das das Zeitbudget empfindlich strapazieren. Unter ungünstigen Bedingungen ist es daher schön, wenn Anbieter – gern auch gegen Aufpreis – bereit sind, eine Festplatte per Express an den durch den Datenverlust ohnehin gebeutelten Kunden zurückzuschicken.

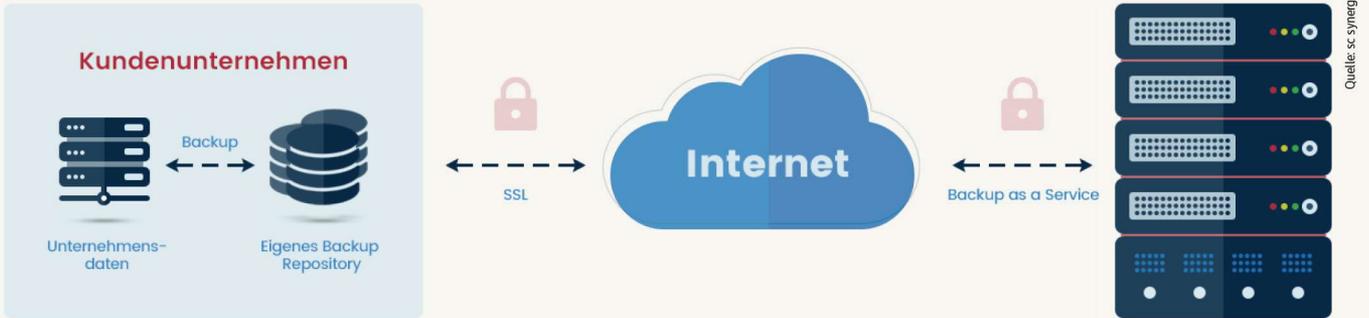
Handelt es sich um sehr veränderungs-trächtige Daten, beispielsweise Bestell- oder

Lagersysteme, ist ein kontinuierliches Backup oder eine CDP (Continuous Data Protection) wichtig. Sie schreibt jede Veränderung der Daten sofort weg und konsolidiert sie später in das Backup. Das ermöglicht im Fall des Falles die Wiederherstellung des aktuellen Stands der Systeme.

Sicherheitsorientierte Zusatzfunktionen

Auch lohnt es sich, auf sicherheitsorientierte Zusatzfunktionen wie integrierten Ransomware-Schutz oder Malware-Scans zu achten. Denn bei Ransomware-Angriffen sind oft genug auch die Backups infiziert. Wer dann das Backup zurückspielt und hofft, seine Systeme so schnell wieder in Betrieb nehmen zu können, endet da, wo er angefangen hat: bei verschlüsselten Daten.

Sinnvoll sind daher Funktionen, die Malware auch in Backups aufspüren, Snapshot-



Alternativ zum Cloud-only-Backup wird das Backup beim Kunden erzeugt und eine Kopie ins BaaS-Rechenzentrum übertragen (Abb. 3).



Funktionen, die es erlauben, bis exakt zur letzten Malware-freien Minute zurückzugehen, und Ähnliches. Einige professionelle Tools bieten Derartiges bereits an. Malware- und insbesondere Ransomware-Schutz des Backups ist auf jeden Fall ein gewichtiges Plus bei der Produktauswahl. Acronis bringt sogar Forensikfunktionen mit, die es ermöglichen, Vorfälle nachträglich durch Speicher-Dumps oder Prozessaufzeichnungen nachzuvollziehen. Eine weitere interessante Zusatzfunktion ist es, die Systeme aus Backup-Images in der Cloud direkt wieder hochzufahren. Dies bieten die Provider häufig unter dem Stichwort „Disaster Recovery“ als Teil oder optionale Zusatzfunktion des Backup-Dienstes an. Wer sich sicher sein möchte, dass die Systeme schnellstmöglich ihre Arbeit wieder aufnehmen, ist damit möglicherweise gut bedient.

Nach der Erhebung von NordLocker gehören deutsche Firmen und Einrichtungen zu den gefährdetsten Opfern von Ransomware-Angriffen (Abb. 4).

Ransomware, die allgegenwärtige Bedrohung

Das Bundesamt für Sicherheit in der Informationstechnik stufte die Ransomware-Bedrohungslage im Jahr 2022 in seinem einschlägigen Bericht zum Thema als hoch ein – daran dürfte sich im laufenden Jahr nichts ändern (siehe ix.de/z481). Angriffsvektoren gibt es viele: Spam, die Ausnutzung von Exploits und schlecht konfigurierter Servern oder ungeschützte Zugänge zu Systemen über externe Netze.

Viele Angreifer verstehen ihre Aktivitäten als Geschäftsmodell und sind oft als international agierende Unternehmen organisiert. Darüber hinaus sind zunehmend auch politisch motivierte Täter unterwegs, die versuchen, in den digitalen Assets als gegenständig eingestuft Staaten Chaos zu stiften oder Geld für Aktivitäten zu verdienen, die ihrem Land politisch nützen. Der Ukrai-

nekrieg hat die Intensität politisch motivierter Cyberangriffe deutlich erhöht.

Zu den entstehenden Schäden zählen finanzielle Verluste, eine verschlechterte Reputation, die zum Verlust von Kunden und Partnern führen kann, und rechtliche Folgen, falls durch die DSGVO, KRITIS oder anderweitige Bestimmungen geschützte Daten verloren gegangen sind und sich der Betreiber der IT eine (Mit-)Verantwortung zurechnen lassen muss.

Deutschland gehört zu den Ländern, die besonders im Fokus der Angreifer stehen. In der statistischen Erhebung „Ransomware statistics: Who is targeted the most?“ von NordLocker, einem Anbieter von sicherem Cloud-Storage, gehörte Deutschland im Durchschnitt der Jahre 2020 bis 2022 zu

den zehn Ländern mit den weltweit meisten Ransomware-Angriffen (siehe ix.de/z481). Maßstab war die Zahl der Ransomware-Angriffe pro Mitarbeiter der an der Umfrage teilnehmenden Firmen. Angegriffen werden vor allem kleinere Unternehmen, aber auch der gehobene Mittelstand bis zu einem Umsatzvolumen von einer halben Milliarde Dollar.

Die bevorzugten Branchen, gegen die sich Ransomware-Attacken richten, sind produzierendes Gewerbe, Baugewerbe, Transport und Logistik, die Hightechbranche, das Gesundheitswesen, Finanzen und Versicherungen sowie der öffentliche Sektor. Allerdings sind alle Branchen signifikant von Erpressungsversuchen betroffen. Die Gruppen Lockbit und Conti sind bei Weitem die aktivsten Ransomware-Täter.

In iX extra 7/2023: Cloud: Identity and Access Management – IAM-Fähigkeiten von Cloud-Anbietern

Viele Unternehmen befinden sich in einer grundlegenden Transformation auf dem Weg in die Cloud. Das Nutzen verschiedenartiger Cloud-Formen wie Public, Private oder Hybrid und Bereitstellungsmodelle wie IaaS, PaaS oder SaaS verspricht Kostenminimierung, unbegrenzte und schnelle Ressourcenverfügbarkeit sowie eine softwarebasierte Administration per Infrastructure as Code. Beim Weg in die Public Cloud müssen verschiedene Akteure dem Sicherheitsbedürfnis der Anwender Rechnung tragen. Firmen vertrau-

en einerseits den Cloud-Anbietern ihre wichtigen Daten an und werden andererseits mit einer angespannten Cybersicherheitslage konfrontiert.

Ein durchdachtes Identity and Access Management bietet hier grundlegende Sicherheitsfeatures für Anwendungen und IT-Infrastrukturen. Dafür stellen die Cloud-Anbieter ein buntes Potpourri an Funktionen in ihrem Sortiment bereit.

Erscheinungsdatum: 29. Juni 2023

Fazit

Anwender sollten, bevor sie einen BaaS-Dienst ordern, ihre Bedürfnisse genau evaluieren und am besten anhand einer Checkliste überprüfen. Nicht immer helfen die im Internet gelieferten Informationen weiter. Gerade wer mit den Managed Services eines kleineren Serviceproviders mit lokaler oder nationaler Reichweite liebäugelt, muss meistens das persönliche Gespräch suchen.

Insgesamt ist aber das Backup in und aus der Cloud gerade für kleinere Unternehmen ohne umfassende IT-Ressourcen sicher eine erwägenswerte und zukunftssträchtige Option, die Fixkosten senkt und die Sicherheit steigern dürfte. (sun@ix.de)

Quellen

Alle zitierten Statistiken und Berichte sowie die Direktlinks der aufgeführten BaaS-Anbieter siehe ix.de/z481

Die weiteren iX extras

10/2023	Security: Neues rund um die it-sa	erscheint am 21.09.2023
11/2023	Hosting: Hochverfügbarkeit auf Bestellung	erscheint am 19.10.2023
12/2023	Storage: Objekt-Storage	erscheint am 23.11.2023

ARIANE RÜDIGER

arbeitet als freie IT-Journalistin.



Rechtssichere E-Mail-Archivierung made in Germany

Einfach. Zuverlässig. Weltweit erprobt.

MailStore Server

- ▶ E-Mail-Archivierung für KMU

MailStore Service Provider Edition

- ▶ E-Mail-Archivierungslösung für Service Provider



Schon über **80.000 Kunden** und über **1.000 Service Provider** in mehr als 100 Ländern vertrauen auf MailStore. Setzen auch Sie auf die **Experten für E-Mail-Archivierung**.

MailStore Software GmbH · Clörather Str. 1-3 · 41748 Viersen, Deutschland
Telefon: +49 (0)2162 - 502990 · E-Mail: sales@mailstore.com · www.mailstore.com

Die Experten für E-Mail Archivierung

**MAIL
STORE**
by opentext™