SWISS iTMagazine

Nr. 05 | Mai 2019 | Fr. 11.–

Die Stundensätze der Schweizer ICT-Freelancer
Seite 76

Storage Trends 2019

• All-Flash • Cloud
• Machine Learning
• Objektspeicher

CIO-INTERVIEW
Christoph Scholl, BDO Schweiz

Storage Trends

Know-how

Die Art und Weise, wie Unternehmen ihre Daten speichern und abrufen, hat sich in den letzten Jahren grundlegend verändert. Im Schwerpunkt beleuchten wir die wichtigsten und vielversprechendsten Speichertrends der nahen Zukunft.

Die Speicherindustrie entwickelt sich schneller als je zuvor. Marktforscher rechnen mit enormen jährlichen Datenzuwachsraten von bis zu 40 Prozent. Das Gesamtspeichervolumen soll bis 2020 über 50 Zettabyte (ZB) betragen – eine Datenmenge, die vor einigen Jahren noch unvorstellbar war.

Der Erfolg von Unternehmen, sei es eines mit fünf Mitarbeitern oder eines der Global Fortune 500, hängt somit zunehmend mit dessen Speicherstrategie zusammen, denn diese bildet das Fundament, auf dem alles andere aufbaut. Und das muss sicher und felsenfest sein sowie aus den zuverlässigsten Komponenten bestehen.

Die Speicher-Landschaft ist aber auch zunehmend komplexer geworden, neue Technologien, Modelle und Konzepte entern den Markt, und der Wald an möglichen Optionen, sei es bei der Datensicherung, Backup-Strategie oder Datenanalyse, wird immer dichter. Trotzdem lassen sich einige Hauptströme erkennen, wenn es darum geht, zu erkennen, welche Trends in naher Zukunft die Möglichkeit bieten, das Geschäftsmodell von Unternehmen nachhaltig positiv zu beeinflussen.

Automatisierung, Cloud & Backup

Der Bedarf an Automatisierung auf breiter Front ist da. Die Tage der Band- und manuellen Sicherung gehören der Vergangenheit an und das Thema Cloud müsste deutlich auf dem Firmenradar zu erkennen sein. Angesichts der hinter jeder Ecke lauernden potenziellen Sicherheitsverletzungen ist es heute ausserdem wichtiger denn je, kritische Backup-Prozesse zu automatisieren, anstatt es dem Zufall zu überlassen, dass die Mitarbeiter daran denken, das Backup zu aktivieren.

Hierbei geht der Trend in Richtung Appliance-basierten Backups im Zusammenspiel mit geo-redundantem Cloud-Speicher. So können automatische Backups erstellt werden, wobei die Daten dank Speicherung in der Cloud wiederhergestellt werden können, egal was lokal mit ihnen passiert: Etwa durch bösartige Angriffe, wie etwa Ransomware, die alle Dateien im Netzwerk verschlüsseln und somit unbrauchbar machen kann, oder durch unvorsichtige Mitarbeiter, die vielleicht aus Versehen wichtige Dateien löschen. Dank geo-redundanter Speicherung werden sämtliche Daten in mehreren Rechenzentren gesichert und können sogar dann wiederhergestellt werden, wenn einer der Speicherstandorte ausfällt, etwa durch eine Beschädigung der Infrastruktur. Die Cloud erlaubt es Unternehmen einerseits die Kontrolle über kritische Geschäftsdaten zu behalten und gleichzeitig die Skalierbarkeit, Kosteneffizienz und Flexibilität von Software-as-a-Service (Saas)-Lösungen zu nutzen. Diese Art von Backup-Lösung trägt damit im Wesentlichen dazu bei, Datenverlust und Ausfallzeiten zu vermeiden. Ausserdem erlaubt eine Speicherstrategie, die auf der Cloud basiert, Mitarbeitenden auch dann zu arbeiten, wenn die eigene Infrastruktur ausser Betrieb ist, indem diese ganz einfach remote auf die Daten in der Cloud zugreifen. Wenn Backup-Daten in die Cloud verlagert werden, können diese zudem für Migration, Entwicklung und Tests, Daten-Analyse und mehr wiederverwendet werden, wodurch sich wiederum Mehrwert generieren lässt.

Künstliche Intelligenz

Doch auch Rechenzentren entwickeln sich weiter, und Künstliche Intelligenz (KI) spielt zunehmend eine Rolle bei deren Konzeption und Entwicklung. Die Implementierung von KI, im Sinne von lernfähigen Algorithmen und Systemen, birgt zahlreiche Vorteile für den Endanwender. So können KI-gestützte Technologien die Energieeffizienz von Rechenzentren enorm steigern. Google verkündete etwa unlängst, dass durch den Einsatz von KI der Energieverbrauch in den eigenen Datenzentren um bis zu 40 Prozent gesenkt werden konnte.

Andere Vorteile von KI liegen auf der Hand: So birgt die Technologie etwa das Potential, den Geschäftsbetrieb zu modernisieren, indem Daten um ein Vielfaches schneller analysiert werden können oder kann durch die bestmögliche Verteilung von Arbeitslasten die Serverauslastung optimieren und dadurch die Effizienz steigern. Zentral dürfte aber auch der Einsatz als Sicherheitsmechanismus

2019

Von Simon Wegmüller

STORAGE TRENDS 2019

sein. So können Systeme mit Hilfe von Machine-Learning-basierten Systemen rund um die Uhr automatisch überwacht werden, während die Systeme Angriffen und Angriffsvektoren dank Non-Stop-Analyse von Mustern, Daten und -bewegungen stets einen Schritt voraus ist. Ins Detail zum Thema Machine Learning und Sicherheit in der Cloud geht Vesselin Tzvetkov, Senior Security Consultant bei AWS Professional Services, in seinem Fachartikel ab Seite 39.

Flash- & Objekt-Speicher

Durch die kontinuierliche Weiterentwicklung klettern Solid-State-Laufwerke (SSDs) in der Hierarchie von Speichersystemen immer weiter nach oben. Ob vor Ort, in Cloud-Umgebungen oder als Teil einer hybriden Systemarchitektur, Flash-Speicher bietet zahlreiche Vorteile in Bezug auf Geschwindigkeit und Effizienz. Heute kann Flash-Speicher dank seiner wachsenden Komplexität Informationen in Echtzeit (oder nahezu in Echtzeit) liefern und hat deutliche Vorteile gegenüber Festplatten (HDDs) sowohl in Sachen Leistung als auch bei den Betriebskosten. Gleichzeitig sinken die Preise und die Leistung von SSDs verbessert sich von Jahr zu Jahr. All-Flash-Arrays sind so mittlerweile durchaus zu einer ernstzunehmenden Option geworden, um die traditionelle HDD-Infrastruktur zu ersetzten. Und auch im Zusammenspiel mit der Cloud könnte Flash-Speicher eine wichtige Rolle spielen. So stellt die Einführung von Flash neue Leistungserwartungen an Rechenzentren, etwa in Bezug auf ambitionierte Recovery Time Objectives (RTOs), die bisher nur auf kritische Workloads beschränkt waren, nunmehr aber zunehmend auch für nicht-kritische Prozesse und Daten zum neuen Standard werden. Mit Flash-Speicher können die zurzeit leistungsstärksten Backups und Wiederherstellungen implementiert werden, und die Geschwindigkeit der Wiederherstellung von All-Flash-Produktionssystemen ist der von traditionellen Band- oder Harddisk-Lösungen deutlich überlegen. Flash-Backups können zudem auch verwendet werden, um mehr gleichzeitige Server-Backups zu ermöglichen, was wiederum zu einer besseren Auslastung bei gleichem Umfang führt. Dieser Meinung ist auch Markus Grau, Principal Systems Engineer bei Pure Storage, in seinem Fachbeitrag ab Seite 32.

Das Backup-Problem ist damit aber keineswegs gelöst. Denn auch wenn Flash-Speicher für eine schnelle Wiederherstellung verwendet wird, müssen grosse Datenmengen zur Archivierung und Einhaltung gesetzlicher Vorschriften ausserhalb des Unternehmens gespeichert werden. Dazu kommt immer noch in erster Linie Bandspeicher zum Einsatz. Der eigentliche Nachteil der Bandspeicherung besteht darin, dass Daten irgendwo ausserhalb des Netzwerks abgelegt werden und so keinen Wert für das Unternehmen generieren können. Eine mögliche Lösung für dieses Problem heisst Objektspeicher (auch bekannt als Objekt-basierter Speicher). Dabei handelt es sich um eine Datenspeicherarchitektur, die Daten als Objekte verwaltet, im Gegensatz zu anderen Speicherarchitekturen wie Dateisystemen, die Daten als Dateihierarchie verwalten, und Blockspeichern, die Daten als Blöcke innerhalb von Sektoren und Spuren verwalten.

Solche Systeme ermöglichen die Speicherung grosser Mengen unstrukturierter Daten und eignen sich besonders für Daten, auf die zugegriffen werden muss, die aber nicht bearbeitet werden. Objektspeicher kommt etwa zur Speicherung von Fotos auf Facebook, Songs auf Spotify oder Dateien in Online-Speicherdiensten wie Dropbox zum Einsatz, eignet sich aber auch besonders gut für Firmen-Backups. Denn dieser ist praktisch unbegrenzt skalierbar. In einer Welt, in der die Menge der erzeugten Daten exponentiell wächst, ist dies sicher eine gute Voraussetzung. Zu beachten ist jedoch, dass Daten nicht bearbeitet werden können, ohne das gesamte Objekt neu zu schreiben.

Cloud-Objektspeicher ermöglichen heute aber sicher eine kostengünstige, belastbare und sichere Datenhaltung und gehört definitiv zu den Top Speicher-Trends. Was es mit Objektspeicher genau auf sich hat und welches Potential dieser Speicher-Trend entfalten könnte, erfahren Sie im Fachbeitrag ab Seite 46 von Mathias Wenig, Senior Manager TS und Digital Transformation Specialist bei Veritas. ■

All-Flash-Storage im Aufwind

Know-how Innovationen im Storage-Bereich führen zu technologischer Disruption und unterstützen Unternehmen für die datenzentrierte Ära.

Von Markus Grau

Moderne Workloads wie Big Data Analytics, Maschinelles Lernen (ML) und Künstliche Intelligenz (KI) werden immer wichtiger. Das Echtzeit-Design vieler dieser Systeme erfordert einen All-Flash-Speicher, um eine geringe Latenz und einen hohen Durchsatz zu erreichen. Da IT-Abteilungen immer mehr dieser Workloads auf sehr grossen und schnell wachsenden Datensätzen einsetzen, benötigen sie neue, leistungsfähigere Speichertechnologien.

In den letzten Jahren haben sich All-Flash-Arrays im Speichermarkt etabliert. Das Non-volatile-Memory-Express (NVMe)-Protokoll, das von Grund auf für die Parallelverarbeitung entwickelt wurde, gibt All-Flash einen weiteren Schub. NVMe-over Fabrics (NVMe-oF) ermöglicht superschnellen Speichernetzwerken die Konsolidierung mehrerer Workloads in einer Speicherumgebung.

Aktuelle Trends und Potentiale im Storage-Markt

Die fortschreitende Storage-Innovation im Rechenzentrum führt unweigerlich zu Disruption durch den Übergang von alten zu neuen Technologien: von der Festplatte zu Flash, vom Storage Area Network (SAN) oder Direct Attached Storage (DAS) zu Ethernet, von Disk-to-Disk-to-Tape (D2D2T) zu Flash-to-Flash-to-Cloud (F2F2C) und von On-Prem oder Cloud zu Hybrid-Umgebungen. Bereits heute stellt sich die Frage, ob traditionelle SAN- und DAS-Systeme obsolet geworden sind und was an ihre Stelle treten wird.

Vor allem Service Provider bewegen sich auf Ethernet-Netzwerke zu. Die Technologie ist erschwinglich und moderne Scale-Out/Cloud-basierte Anwendungen basieren bereits auf Fast Ethernet Fabrics. Auf diese Weise können die Verfügbarkeits- und Effizienzvorteile eines gemeinsamen Arrays genutzt und gleichzeitig kann maximale Performance erreicht werden. Der Vorteil dabei ist die Konvergenz im Netzwerk. Darüber hinaus hat sich die Geschwindigkeit von Ethernet, derzeit bei 100 Gbit/s, in den letzten Jahren massiv erhöht. Über diese Infrastruktur ist es auch möglich, nicht nur iSCSI- oder NAS-Protokolle, sondern auch Objekt-basierte Protokolle anzusprechen. Ethernet eröffnet auch Möglichkeiten für neue Anwendungen, die über NVMe-oF mit der Storage-Umgebung verbunden werden können.

NVMe als wichtige Storage-Innovation

In den letzten Jahren hat sich NVMe zu einer bedeutenden Innovation im Storage-Umfeld entwickelt. NVMe ist ein Protokoll der nächsten Generation für eine beschleunigte Kommunikation zwischen Prozessor und Flash-Speicher. Der Einsatz von NVMe war zunächst auf den Endverbrauchermarkt, insbesondere Smartphones, beschränkt und wurde auf grosse Enterprise-Storage-Lösungen ausgeweitet. Seitdem hat sich NVMe in den Mainstream-B2B-Markt vorgearbeitet, in Form von Speicherlösungen, die für kleine und mittelständische Unternehmen mit hohen Anforderungen an die Datenverarbeitung attraktiv sind.

Für Flash-Arrays der Enterprise-Klasse bietet NVMe eine weitaus höhere Leistung als die zuvor entwickelten Serial-Attached-SCSI- (SAS)- und Serial-Advanced-Technology-Attachment-(SATA)-Schnittstellen. Diese wurden ursprünglich für Festplatten entwickelt, sind aber immer noch weit verbreitet, selbst in All-Flash-Solid-State-Laufwerken. Der Grund für den Leistungssprung ist, dass NVMe deutlich schneller ist als das herkömmliche Speicherprotokoll SAS. Es unterstützt bis zu 64'000 parallele Warteschlangen mit 64'000 Befehlen pro Warteschlange, womit direkte Übertragungswege zum Flash-Speicher zur Verfügung stehen. Auf diese Weise stehen direkte Übertragungswege zu Solid State Drives (SSDs) bereit. Die daraus resultierende massive Parallelverarbeitung beseitigt die durch serielle Verbindungen verursachten Engpässe. Dies führt zu einer deutlich höheren Performance.

NVMe ermöglicht, was den Datenzugriff betrifft, effizientere und schnellere All-Flash-Systeme im Vergleich zu herkömmlichen Festplatten. Einige der Storage-Anbieter treiben die Transformation zu NVMe voran, mit dem Ziel, NVMe als führendes Schnittstellenprotokoll für Flash zu etablieren.

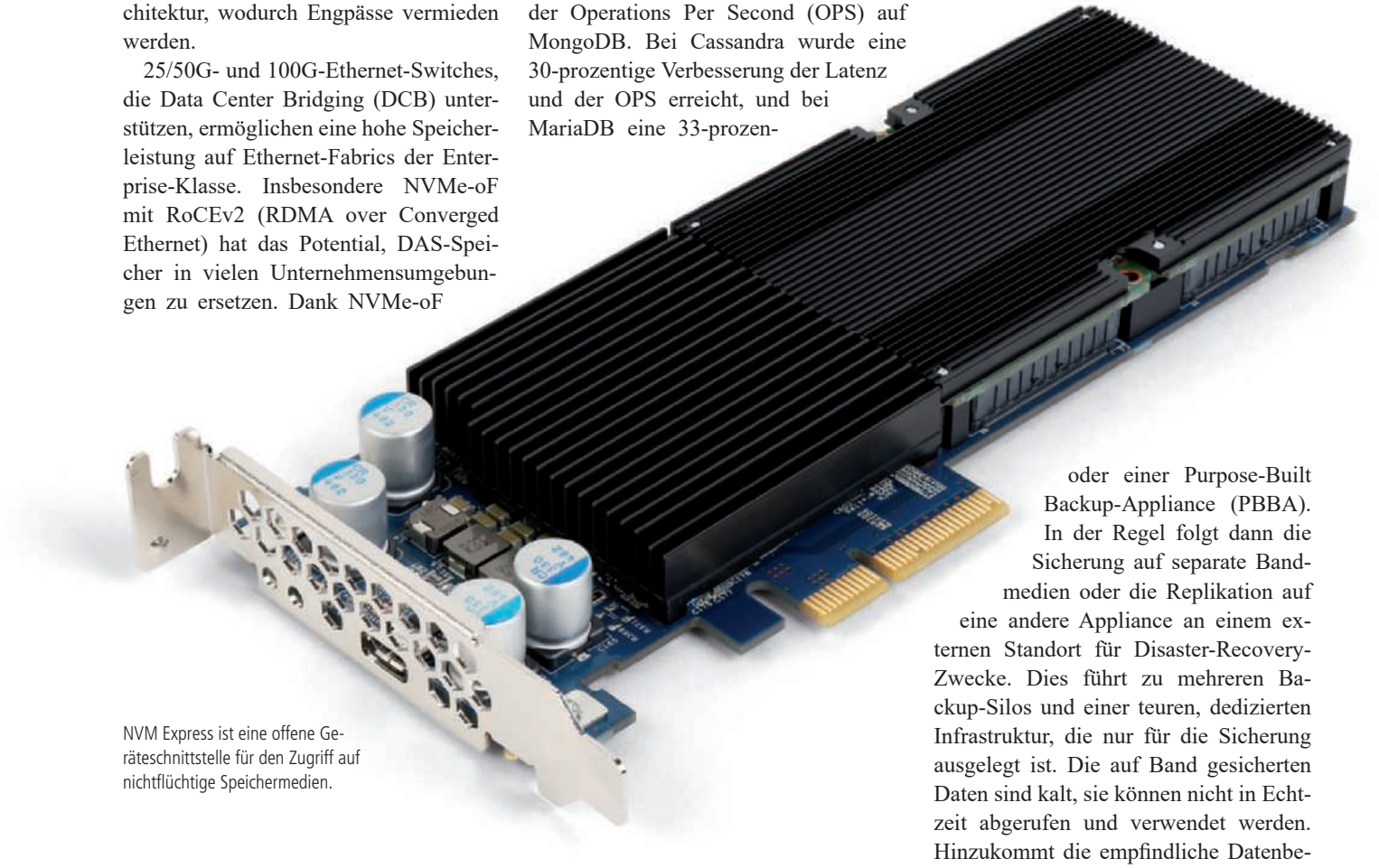
Schnellere Konnektivität mit NVMe-oF

NVMe-oF ist ein zusätzliches neues Protokoll für viel schnellere Verbindungen von Server zu Speicher. NVMe-oF ist eine Erweiterung von NVMe zur Unterstützung von Netzwerkstrukturen wie Ethernet, Fibre Channel, Infiniband und Transmission Control Protocol (TCP). Der Fabric-Ansatz kombiniert die gemeinsame Netzwerkstruktur von Core-, Aggregations- und Edge-Layern in einer Umgebung, zugunsten einer flexiblen Rechenzentrumsinfrastruktur.

NVMe-oF bietet eine schnellere Verbindung zwischen Speicher und Anwendungen auf Servern und eine effizientere

CPU-Auslastung. Dies erlaubt eine weitere Konsolidierung von Rechenzentrum und Netzwerk, da Infrastruktursilos mehrerer Anwendungen eine einzige effiziente Speicherinfrastruktur nutzen können. Dieses gemeinsame Speichernetzwerk beschleunigt den Zugriff und verbessert die Bandbreite. Mit NVMe-oF kann externer Speicher eine Latenz erreichen, die mit DAS vergleichbar ist. NVMe-oF ist bei der Speicher-I/O-Verarbeitung deutlich effizienter als iSCSI und erhöht die Parallelität der Gesamtarchitektur, wodurch Engpässe vermieden werden.

25/50G- und 100G-Ethernet-Switches, die Data Center Bridging (DCB) unterstützen, ermöglichen eine hohe Speicherleistung auf Ethernet-Fabrics der Enterprise-Klasse. Insbesondere NVMe-oF mit RoCEv2 (RDMA over Converged Ethernet) hat das Potential, DAS-Speicher in vielen Unternehmensumgebungen zu ersetzen. Dank NVMe-oF bleibt Fibre Channel eine Option.



NVM Express ist eine offene Geräteschnittstelle für den Zugriff auf nichtflüchtige Speichermedien.

Die direkte Flash-Fabric-Konnektivität ist eine Schlüsselkomponente, die Unternehmen bei der Vereinheitlichung von SAN, DAS und Cloud unterstützt und die Leistung geschäftskritischer Anwendungen und neuer Web-Scale-Anwendungen verbessert. Durch die Unterstützung von NVMe-oF mit RoCE können Unternehmen Flash-Medien näher an Anwendungen heranführen und so den Echtzeit-Zugriff und die Konsolidierung verbessern. Damit ist Ethernet eine erstklassige Rechenzentrumskomponente für Storage mit bis zu 50 Prozent Latenzreduzierung gegenüber iSCSI. NVMe-oF sorgt generell für eine höhere Effizienz im gesamten Netzwerk. Dies gilt insbesondere in Kombination mit Linux und nativen Web-Scale-Anwendungen wie MongoDB, Cassandra und MariaDB, die die Vorteile und die Effizienz von Shared Storage der Enterprise-Klasse nutzen.

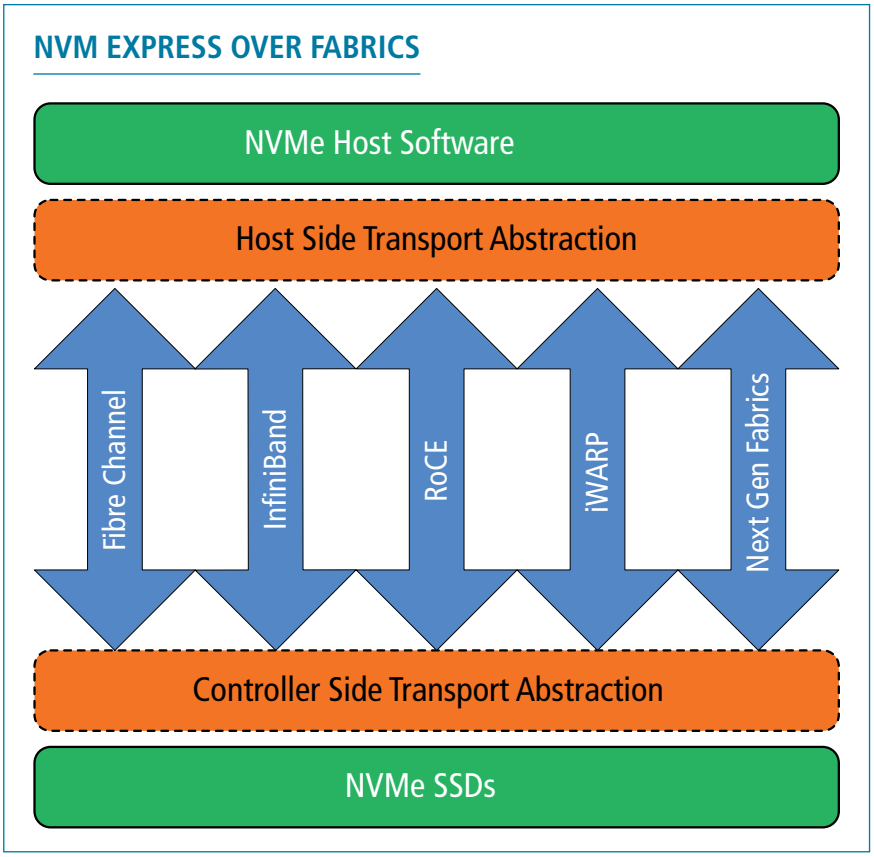
Insbesondere Cloud-native Anwendungen erhalten mit End-to-End NVMe-oF im Vergleich zu SAS-basierten DAS-Lösungen einen deutlichen Leistungsschub. Die eigenen Tests von Pure Storage zeigten eine 50-prozentige Steigerung der Operations Per Second (OPS) auf MongoDB. Bei Cassandra wurde eine 30-prozentige Verbesserung der Latenz und der OPS erreicht, und bei MariaDB eine 33-prozentige Steigerung der maximalen Transaktionen.

Ein weiterer Anwendungsfall wäre zudem sicher auch die Entwicklung einer neuen Test- oder Entwicklungsumgebung auf Basis der aktuellen MongoDB-Daten aus der Produktion. Mit DAS müssten die Daten aus einer Sicherung kopiert oder wiederhergestellt werden. Die direkte Flash-Fabric-Verbindung ermöglicht es derweil, Instanzen sofort aus einem Snapshot heraus zu erstellen, ohne die Produktion zu beeinträchtigen oder zusätzliche Kapazität zu benötigen. All dies kann über eine Rest-API automatisiert werden.

All-Flash als Speicherziel für Backup & Recovery?

Im Zusammenhang mit der Entstehung von Daten als wertvollstem Vermögenswert eines Unternehmens gewinnt die Datensicherung immer mehr an Bedeutung. Das herkömmliche Backup-Modell Disk-to-Disk-to-Tape (D2D2T) entspricht nicht mehr den aktuellen Anforderungen, insbesondere in Bezug auf die schnelle Datenwiederherstellung. Die primäre Festplatte erstellt ein lokales Backup auf der sekundären Festplatte oder einer Purpose-Built Backup-Appliance (PBBA). In der Regel folgt dann die Sicherung auf separate Bandmedien oder die Replikation auf eine andere Appliance an einem externen Standort für Disaster-Recovery-Zwecke. Dies führt zu mehreren Backup-Silos und einer teuren, dedizierten Infrastruktur, die nur für die Sicherung ausgelegt ist. Die auf Band gesicherten Daten sind kalt, sie können nicht in Echtzeit abgerufen und verwendet werden. Hinzukommt die empfindliche Datenbeständigkeit auf Band und die zusätzliche Hardware, die für die Bandsicherung benötigt wird.

Im Gegensatz zum herkömmlichen Ansatz sorgt F2F2C für eine schnellere Wiederherstellung immer grösserer Datensätze und vereinfacht den IT-Betrieb. Das primäre Flash-Speichersystem, beispielsweise mit Oracle oder Vmware, sichert auf Flash-basierten Sekundärspeicher – für schnelle Wiederherstellungen – und die Backup-Daten werden ebenfalls in der Public Cloud gespeichert. Durch Komprimierung und Deduplizierung können Backup-Daten sowohl vor Ort als auch in der Cloud äusserst effizient ge-



Quelle: Wikimedia Commons

NVMe-oF ist eine Erweiterung von NVMe zur Unterstützung von Netzwerkstrukturen wie Ethernet, Fibre Channel, Infiniband und TCP.

speichert werden. Dieser Ansatz zeichnet sich aus durch schnellere und flexiblere Wiederherstellungen, eine sichere langfristige Aufbewahrung von Backup-Daten und eine einfachere Handhabung. Eine schnelle Wiederherstellung findet in der lokalen Umgebung statt, während Backup-Daten in der Public Cloud automatisch zur Unterstützung von Wiederherstellungsvorgängen oder zur Notfallwiederherstellung verwendet werden, wenn lokale Daten nicht verfügbar sind.

Moderne Backup-Lösung: Flash in Kombination mit Cloud

Neue Speicherlösungen bieten ein einheitliches hybrides Cloud-Erlebnis, einheitliche APIs und Automatisierung für Entwickler sowie Backup- und Datensicherungs-Optionen in der Public Cloud. Bei der Interaktion zwischen On-Prem und der Public Cloud ging es darum, eine Lücke zu schliessen: Die Cloud ist nicht speziell für Unternehmensanwendungen konzipiert, und die Unternehmensinfrastruktur ist nicht so einfach zu bedienen wie die Cloud.

Die Datensicherungsarchitektur der nächsten Generation sollte auf Scale-Out-Speichersystemen basieren, die von Grund auf für unstrukturierte Daten entwickelt wurden und eine beispiellose Leistung für eine Vielzahl von Workloads bieten. Schnelle Backups und Wiederherstellungen, aber auch Test/Dev- und Analytik-Anwendungen können auf einer einzigen Speicherplattform zusammengefasst werden. All dies kann nahtlos in einer einheitlichen Hybrid-Cloud-Umgebung erfolgen. Die Storage-Plattform muss daher konsistente Speicherdienste, Ausfallsicherheit und APIs für lokale Umgebungen und mehrere Cloud-Modelle bereitstellen.

Einheitliches Datenmanagement mit Flash-Performance

Die Mobilität von Unternehmensanwendungen in Kombination mit neuen anspruchsvollen Anwendungen hat die strategische Bedeutung der Infrastruktur exponentiell erhöht. Die Antwort ist ein einheitliches Datenmanagement für beide Umgebungen, das durch APIs und Integrationen realisiert wird. Dieser Ansatz erlaubt es, On-Prem-Features wie Hochverfügbarkeit in die Cloud zu bringen und umgekehrt ein Pay-per-Use-Modell wie die Public Cloud in der On-Prem-Infrastruktur anzubieten.

Eine kleine Anzahl von Storage-Anbietern unterstützt ihre Kunden bereits bei der Anbindung an Public Clouds wie Azure und AWS sowie durch Schnittstellen, die es ihnen ermöglichen, Anwendungsfälle wie Backup, Test/Entwicklung oder Disaster Recovery in der Cloud nahtlos umzusetzen. Erfolgreiche Ansätze sind hierbei das Provisioning über eine REST-API oder ein Upgrade-Programm als Abonnementmodell, das Flash-Arrays auf dem neuesten Stand hält.

Neue Datenservices, die seit kurzem verfügbar sind, erleichtern den Umgang mit Anwendungsfällen zwischen On-Prem- und Cloud-Umgebungen. Ein Beispiel wäre die Sicherung von Speicher-Snapshots aus einem Flash-Array auf AWS S3- und Network-File-System-(NFS)-Ziele. Sobald sich die Daten in Amazon S3 befinden, können sie in der Amazon Cloud für Wiederherstellungs-, Disaster-Recovery- oder Test- und Entwicklungs-Zwecke rehydriert werden. Die Portabilität von Snapshots unterstützt somit den Ansatz, die Anforderungen des Multi-Cloud-Modells optimal zu erfüllen. Die richtige Datenstrategie ist entscheidend, denn Daten sind der Schlüssel zu effizienter Entwicklung und Anwendungsmobilität. Heute können Unternehmen ihre Dateninfrastruktur optimal auf ihre Anwendungen abstimmen. Eine datenzentrierte, einheitliche Hybrid-Cloud-Architektur ist ein tragfähiges, zeitgemässes und zukunftsweisendes Modell. Es gibt modernen Unternehmen die nötige Agilität und schafft die Grundlage für die Unterstützung neuer, anspruchsvoller Anwendungen. ■

DER AUTOR

Markus Grau ist Principal Systems Engineer im EMEA CTO Office bei Pure Storage. Seine Laufbahn beim Experten für Flash-Speichersysteme begann er im Frühjahr 2014 als Systems Engineer. Zuvor war Markus Grau rund acht Jahre bei Netapp beschäftigt, wo er vom Systems Engineer zum Solutions Architect aufstieg. Seine Karriere begann Markus Grau bei Case, von wo aus er im Jahr 2000 zu Computerlinks (heute Arrow) wechselte.

Wenn Multi-Cloud zum Standard wird

Know-how Das Mail-System in der einen Cloud, das Personal-Tool beim nächsten Provider und für Telefonie kommt eine dritte Cloud hinzu. Immer mehr Unternehmen setzen auf verschiedene Cloud-Provider. Doch wie gelingt die Transformation hin zu einer Multi-Cloud-Welt?

Von Marco Bösch

Die Digitalisierung aller Geschäftsmodelle und das Internet of Things (IoT), also die Vernetzung aller Maschinen, Gadgets und Sensoren über das Internet, verlangen immer mehr nach dem Einsatz einer Multi-Cloud-Umgebung. Denn gerade das Cloud Computing, also die Haltung aller Daten und Anwendungen in der Internet-Wolke, bietet für die Anforderungen von IoT und die Geschäftsprozessdigitalisierung das ideale Betriebsmodell. Bis 2020, so prognostiziert das IT-Analystenhaus Gartner, sollen rund drei Viertel aller Unternehmen und Organisationen Multi-Cloud- oder Hybrid-Cloud-Modelle einsetzen. Auf Single Clouds, also eine einzige Cloud-Plattform, setzt nur jedes dritte Unternehmen, wie einer Studie des IT-Research- und Beratungsunternehmens Crisp-Research zum Thema Cloud-Orchestrierung zu entnehmen ist.

Hybrid Cloud vs. Multi-Cloud

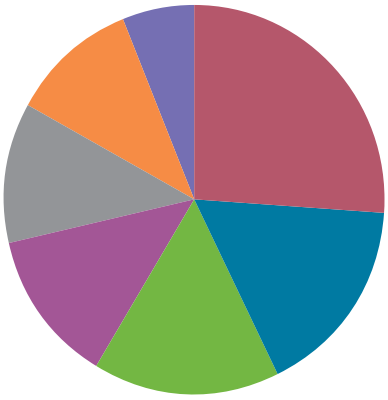
Multi-Cloud ist aber nicht das Gleiche wie Hybrid Cloud. Häufig werden diese Konzepte verwechselt, dabei besteht zwischen beiden ein gravierender Unterschied: Hybrid Cloud bezeichnet die Kombination aus Public und Private Cloud. Das ist zum Beispiel für Unternehmen interessant, die aus Compliance-Gründen nicht sämtliche Daten in der Public Cloud verarbeiten möchten. Viele setzen daher zusätzlich auf Ressourcen aus der Private Cloud, wenn es beispielsweise um die Verarbeitung von Daten geht, die Betriebsgeheimnisse enthalten und deshalb aus Sicht der Unternehmen besonders geschützt werden sollten. Bei der Multi-Cloud hingegen kombinieren Unternehmen nicht nur Ressourcen aus der Public oder der Private Cloud, sondern nutzen darüber hinaus Angebote unterschiedlicher Cloud-Provider. Das kann erforderlich werden, wenn verschiedene Abteilungen im Unternehmen mit unterschiedlichen Ansprüchen entsprechend diversifizierte Anwendungen benötigen – vom File Sharing über die Collaboration-Plattform im Vertrieb und Marketing bis hin zu rechenintensiven Big-Data-Anwendungen oder Testumgebungen.

Warum also Multi-Cloud?

Weg von eigenen Systemen und hin zu IT-as-a-Service – dass Unternehmen darüber nachdenken, ob sie in Zukunft ihre IT ganz oder zumindest teilweise in einer Cloud-Umgebung einrichten wollen, hat viele gute Gründe: einmal die Notwendigkeit zum Kostensparen und zum anderen das Erschliessen verschiedenster Vorteile, die Cloud Services vor allem im Hinblick auf Skalierbarkeit und der sich daraus ergebenden Flexibilität mit sich bringen.

In einer Multi-Cloud-Architektur werden die Cloud-Services von verschiedenen Anbietern zum Einsatz gebracht; insbesondere beliebt ist die Nutzung der Dienste von den Hyperscalern wie Google Cloud, Microsoft Azure, Amazon Web Services und der Lösungen der Enterprise-Anbieter wie beispielsweise der Open Telekom Cloud der Deutschen Telekom. Für jeden Geschäftsprozess wird beurteilt, welche Cloud-Lösung von welchem Anbieter sich dafür am besten eignet und für den jeweiligen Workload die optimalen Bedingungen bietet. Im Zuge der Digitalisierung der Wirtschaft wollen immer mehr Unternehmen Ausgaben von fixen zu variablen Kosten verlagern und nehmen aus diesem Grund Abstand von starren On-Premise-Systemen.

«Warum setzen Sie auf Hybrid- oder Multi-Cloud?»



Quelle: T-Systems

Eine T-Systems-Umfrage an der FH Nordwestschweiz zeigt, warum Firmen auf Hybrid- oder Multi-Cloud setzen.

Von einer Cloud-Umgebung erwarten sie, dass sie all ihre Geschäftsprozesse Ende-zu-Ende unterstützt.

Neben der hohen Flexibilität und den finanziellen Vorteilen gehört auch zu den Vorzügen des Multi-Cloud-Betriebsmodells, dass man sich als Unternehmen ein breites Spektrum an Erfahrung aneignet und dadurch nicht von einem einzigen Anbieter abhängig macht. Das minimiert nebenbei die Unternehmensrisiken und steigert die Resilienz der Unternehmenssysteme. Ausserdem kann sich durch die Nutzung mehrerer Cloud-Plattformen der Zugang zu bestimmten Anwendungen oder Diensten verbessern. Beispielsweise sind einige Produkte und Dienste der Azure Cloud von Microsoft nicht auf AWS verfügbar und umgekehrt.

Global oder lokal?

Was beim Thema Cloud Computing immer wieder zu Diskussionen führt, sind die Fragen nach Datenschutz und Datensicherheit. Wo befinden sich die Cloud-Server und wo sind Cloud-Speicher sowie Cloud-Backup? Generelle Antworten auf diese Fragen gibt es nicht, es kommt immer auf den Einzelfall an. Jemand, der einzig und allein Kosten sparen möchte und der nicht gesetzlich verpflichtet ist, Daten an einem bestimmten Ort vorzuhalten, der wird sich nach einer günstigen Public Cloud umsehen. Ein Unternehmen, bei dem nur ein Teil der Daten sensibel ist, möchte Cloud Services, die ihm sowohl die Kostenvorteile bieten und gleichzeitig die kritischen Daten vor Ort belassen. Und schlussendlich braucht der Kunde, der alles lokal haben muss oder möchte, eine lokale Private-Cloud-Lösung. Der Schlüssel liegt in der gesamtheitlichen Betrachtung der Geschäftsanforderungen und der Integration von Public und Private Cloud wie auch der klassischen IT. Dafür sind vielfältige Integrationskompetenzen gefragt, die die meisten Unternehmen nicht in-house haben.

Treiber für Multi-Cloud-Services

Laut einer Crisp-Research-Umfrage waren noch 2017 die massgeblichen Treiber für den Einsatz eines Hybrid- oder Multi-Cloud-Betriebskonzepts die steigenden Anforderungen durch die voranschreitende Digitalisierung und deren Workloads (54,4%), gefolgt von der Infrastruktur, die den Betrieb nicht alleine gewährleisten kann (38,6%), sowie der Skalierbarkeit (38,1%). Eine Umfrage, durchgeführt von T-Systems im Rahmen eines «Cloud Use Cases Day 2019»-Workshops an der Fachhochschule Nordwestschweiz, zeigt nun, dass sich die Prioritäten für Unternehmen leicht verschoben haben. Neu setzen Unternehmen vor allem auf ein Multi-Cloud-Betriebsmodell, da es mehr Skalierbarkeit bietet, darauf folgen die steigenden Anforderungen durch neue, digitale Workloads, die somit besser gemeistert werden können, sowie an dritter Stelle die unterschiedlichen Business-Applikationen, die als SaaS-Lösung in der Internet-Wolke zur Verfügung gestellt werden.

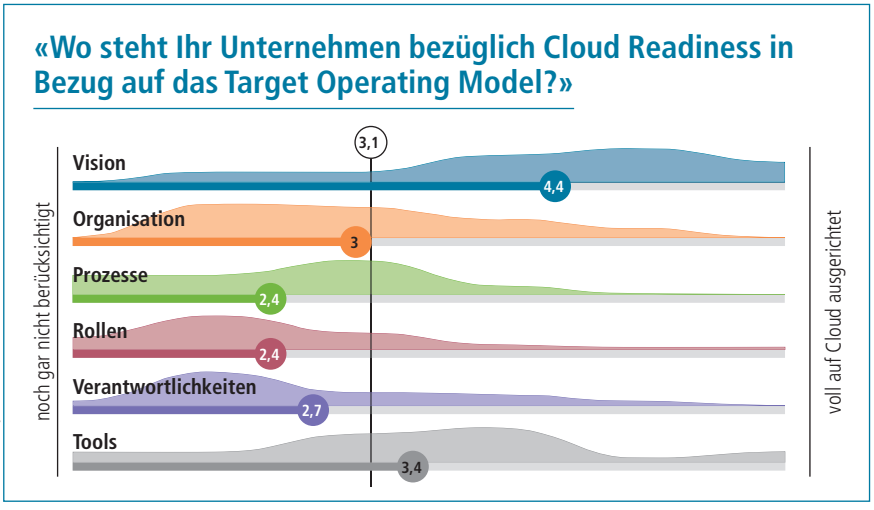
Cloud Computing wird immer geschäftsrelevanter

Der sich abzeichnende Wandel in Bezug auf den Einsatz von einer Multi-Cloud-Architektur verdeutlicht umso mehr, dass Cloud Services in den Kern der Geschäftstätigkeit von Unternehmen vorgedrungen sind. Es drängt sich die Frage auf, wie gut sich Unternehmen ganzheitlich auf Cloud Computing ausgerichtet haben?

Dieser Frage ist das Cloud Research Team um Stella Gatziu Grivas der Fachhochschule Nordwestschweiz (FHNW) nachgegangen. Die Ergebnisse aus der qualitativen CIO-Umfrage von 2017 und der anschliessenden quantitativen Analyse von 2018 haben deutlich gezeigt: Schweizer Unternehmen sind noch nicht am Ziel, wenn es um ihren Reifegrad geht. Die Governance-Maturität, die auch Rollen beziehungsweise Verantwortlichkeiten abdeckt, zeigt noch grossen Entwicklungsbedarf. Es fehlt auch an einer strukturierten Analyse der Cloud-Bedürfnisse. Viele Projekte, die auf Cloud setzen, werden nach wie vor isoliert betrachtet und getrieben durch Fachabteilungen umgesetzt. Damit fehlt es an einer Gesamteinbettung; es entsteht eine Schatten-IT und damit findet keine gesamtheitliche Transformation des Unternehmens statt. Aspekte wie Prozesse, Verantwortlichkeiten und Organisationen werden also nicht nach Cloud-Gesichtspunkten hinterfragt und neu gestaltet.Wie so etwas strukturiert angegangen werden kann, wurde bereits 2012 von Glenfis in Form des Cloud Target Operating Model (TOM) beschrieben.

Cloudreach – ein Unternehmen der ersten Stunde, wenn es um Managed Services auf Basis von Public Clouds geht – bringt es auf den Punkt: «Ein Cloud Operating Model (Betriebsmodell) ist definiert als eine abstrakte Repräsentation (Modell) davon, wie eine Organisation Werte für Kunden schafft unter Verwendung von Cloud Services».

Heutige zentrale IT-Funktionen liefern täglich ihre Services aus Datacentern zu den Geschäftseinheiten. Dieses Betriebsmodell ist seit langem definiert, erprobt und über viele Iterationen optimiert worden. Wenn nun ein Geschäft auf Cloud Services aufsetzen soll, muss das traditionelle Modell komplett hinterfragt werden. Denn wer die Vorteile von Cloud nutzen möchte, muss sich auch darauf einlassen und das heisst, Vision, Governance, Zusammenarbeit, Prozesse, Rollen, Verantwortlichkeiten, Technologien und die Organisationen neu zu durchdenken. Auf



T-Systems befragte Unternehmen auch nach dem Reifegrad in Bezug auf die Cloud Readiness.

dem klassischen Datacenter-Gedanken aufzusetzen, bringt wenig Vorteile oder führt zum Scheitern des Vorhabens.

Anders gesagt: Damit die Vorteile von Cloud Services wie Geschwindigkeit, Agilität und Kosten voll ausgeschöpft werden können, muss sich ein Unternehmen auch auf die Eigenheiten einlassen. Die «Pet vs. Cattle»-Analogie verdeutlicht diese Eigenheiten, die sich aus APIs, Automatisierung, pay-per-use und weiteren Aspekten ergeben. Auch werden heute immer noch häufig IT Business Cases mit Fokus auf Infrastruktur-Kosteneinsparungen erstellt. Diese machen jedoch nur einen kleinen Prozentsatz der Gesamtkosten aus. Viel wichtiger sind die Möglichkeiten, die sich für die Bereiche Effizienz und Mehrwert für das Geschäft ergeben.

Um die Transformation erfolgreich abzuschliessen, dürfen die Menschen und die Prozesse nicht ausser Acht gelassen werden, denn sie sind es, die das Betriebsmodell mit Leben füllen. Die Mitarbeiter benötigten dafür Know-how wie auch den notwendigen Freiraum, um das neue Betriebsmodell entwickeln und umsetzen zu können. Damit spielen sie eine sehr wichtige und zugleich auch herausfordernde Rolle in der Transformation zu einem Cloud-basierten Betriebsmodell.

Das Erarbeiten und Implementieren eines Cloud Operating Model ist somit eine ganzheitliche Angelegenheit. Das Fundament des Cloud Operating Model bilden die Eckpfeiler auf der die Business-Architektur wie auch die System-Architektur aufsetzen. Dies ermöglicht eine beschleunigte Umsetzung der Cloud-Anwendung und damit auch, den höchsten Nutzen aus den Cloud Services zu ziehen.

In einem Workshop des vergangenen Cloud Use Cases Day wurde der Reifegrad der Unternehmen in Bezug auf die Umsetzung eines Target Operating Model abgefragt. Dabei wurde sichtbar, dass Unternehmen zwar ihre Vision stark auf Cloud richten oder zumindest ihre Strategien nach dem Credo «Cloud first» überarbeiten. Gleichzeitig wird jedoch deutlich, dass Mitarbeitende, Prozesse, aber auch die gesamte Organisation und die Rollen sprich Verantwortlichkeiten noch grossen Nachholbedarf in Bezug auf die Transformation hin in die Cloud haben. Als Folge können viele Unternehmen nach wie vor noch nicht das volle Potential von Cloud Services ausschöpfen.

Der Übergang von spontanen Cloud-Implementierungen hin zu einer optimierten Multi-Cloud-Architektur hält für Unternehmen viele Herausforderungen bereit. Ein Cloud Target Operating Model vereinfacht und strukturiert diesen Weg. Unternehmen, die dabei schnell vorankommen wollen, greifen auf kompetente Partner zurück, um diese Herausforderung erfolgreich zu bewältigen. ■

DER AUTOR

Marco Bösch ist Cloud-Experte und Evangelist bei T-Systems Schweiz und als Gastdozent für Cloud-Strategie und Multi-Cloud Management an der Fachhochschule Nordwestschweiz tätig. Er begleitet Kunden auf ihrem Digitalisierungsweg und unterstützt sie sowohl bei technischen als auch wirtschaftlichen und organisatorischen Herausforderungen.

Von Cloud zu Cloud

Fallbeispiel Das Schweizer Unternehmen Aryxe stand vor der Herausforderung, eine Cloud-Speicherlösung zu finden, die hohen Sicherheitsanforderungen entspricht. Eine solide Planung war die Grundlage für eine erfolgreiche Datenmigration.

Von Simon Wegmüller

Das schweizerisch-deutsche Technologieunternehmen Aryxe ist auf digitale Lösungen für KMU spezialisiert. Das Angebot reicht von Research und Consulting bis hin zu Business-Modulen, unter anderem in den Bereichen Social Media, Digital Advertising oder Content Production. Niederlassungen in Bulgarien, Estland, Polen und der Schweiz stellen das Unternehmen vor besondere Herausforderungen, wenn es um den Betrieb einer effizienten IT-Infrastruktur geht.

Um den sicheren Austausch von Daten mit Kunden zu gewährleisten, kam bis vor kurzem die Business-Lösung von Dropbox zum Zug. Vertrauen in die Lösung war aber nur begrenzt vorhanden, da Schweizer und Europäische Sicherheitsstandards von Dropbox nur bedingt eingehalten werden, so Stephan Muehlemann, CEO von Aryxe.

Zwar setzte man mit Dropbox bereits zuvor auf eine Cloud-Speicher-Lösung, die Sicherheitsthematik rückte für Aryxe zunehmend in den Vordergrund. Besonders die Möglichkeit, Daten verschlüsselt ablegen zu können, sowie die Option, die Daten in der Schweiz «und in einem stabilen Umfeld» zu halten, führten zum Entscheid, sich nach anderen Lösungen umzusehen, so Muehlemann.

Hohes Anforderungsprofil

Das letztlich erneut eine Cloud-Lösung das Rennen gemacht hat, ist kein Zufall. «Speziell in der Zusammenarbeit mit Kunden ermöglicht uns ein Cloud-Speicher ein flexibles, aber dennoch siche-

res Teilen von Dokumenten», erklärt CEO Muehlemann. «Aufgrund der hohen Datenmengen sowie dem externen Zugriff von Kunden wäre dies über eine klassische Fileserver-Infrastruktur nicht möglich.» Und auch die Möglichkeit, etwa durch ein flexibles Kostenmodell die Ausgaben möglichst tief zu halten, spielte bei der Entscheidung eine Rolle. Die gewünschte Speicherlösung sollte dabei über API-Integrationen in die bereits bestehenden Systeme eingebettet werden können und hohe Anforderungen bezüglich Verfügbarkeit und Sicherheit erfüllen. Des weiteren standen insbesondere ein solides und flexibles Benutzermanagement, die einfache Integration von Kunden, flexible Wachstumsmöglichkeiten und die Möglichkeit zur Ablage von grossen Datenmengen (was auch die verfügbare Bandbreite miteinschliesst) im Zentrum des Anforderungsprofils. «Wie genau diese Anforderungen gelöst werden, stand für Aryxe an zweiter Stelle», verrät Muehlemann und erklärt: «Hier schätzen wir die Kompetenz unserer Lösungspartner und fokussieren uns auf unsere eigenen Know-how-Bereiche.»

Den richtigen Partner finden

Der Wald bestehend aus Cloud-Speicheranbietern ist zwar dicht, bedingt durch die definierten Anforderungen reduzierte sich die Auswahl für Aryxe jedoch stark. «Besonders die gesamte Verschlüsselung der Daten wurde häufig nicht als Option angeboten», erklärt Muehlemann. Es blieb eine Shortlist mit vier Anbietern übrig, aus welcher Netstream als Gewinner hervorging. «Ausser den technologischen Aspekten war für uns eine Begegnung auf Augenhöhe (KMU/KMU) ebenso wichtig», betont der CEO.

Besonders ins Gewicht fiel für Aryxe dabei auch die Tatsache, dass geschulte Netstream-Mitarbeitende während der Migration, aber auch heute noch, bei Bedarf zur Verfügung stehen. «Als Kunde schätzen wir es, bei Anfragen nicht in einem Call Center zu landen», bringt es Muehlemann auf den Punkt. «Für komplexere Szenarien wurden uns zudem Partnerunternehmen von Netstream genannt, welche uns auch vor Ort hätten unterstützen können, was wir aber intern lösen konnten.»

Migrationsphase

Netstream bietet Kunden diverse Lösungen in den Bereichen Cloud, Internet, Telefonie, Hosting, TV und Wholesale an. Das Unternehmen sieht sich unter anderem als Cloud-Technologielieferanten, der vor allem KMU aber auch grössere Unternehmen mit eigenen Lösungen anspricht. Dabei werden die von Netstream angebotenen Services in bestehende Kunden-Infrastrukturen assimiliert. So bietet das Unternehmen etwa Auslagerungen von Backups in Object Storage oder auch Backup-as-a-Service-Lösungen an.

Nachdem der Entscheid zu Gunsten von Netstream fiel, stellte das Unternehmen Aryxe eine bereits produktive Nextcloud-Umgebung innerhalb eines Tages zur Verfügung. Bei Nextcloud handelt es sich um eine Open-Source-Suite, bestehend aus Client-Server-Software, zur Erstellung und Nutzung von File-Hosting-Diensten. Bereits im Voraus bestand Seitens Aryxe allerdings die Möglichkeit, sich mit der Technologie mittels Testaccount zu befassen. «Im nächsten Schritt wurden erste Workloads, sprich Daten, auf die Nextcloud-Infrastruktur von Netstream migriert und die definierten Testszenarien ein weiteres Mal durchgespielt», so Muehlemann. Nachdem dieser erste Schritt erfolgreich abgeschlossen war, begann man damit, erste Kundendaten zu migrieren, wobei alle Use-Cases zunächst getestet wurden. Nach insgesamt zwei Wochen wurden dann schliesslich final alle Daten auf die neue Lösung migriert. «Durch die Möglichkeit, die technologischen Erfahrungen im Voraus zu sammeln, konnte die eigentliche Migration sehrt strukturiert und zeitlich optimiert umgesetzt werden», fasst Muehlemann zusammen. Insgesamt dauerte die Umsetzung des gesamten Migration-Projekts, inklusive Anbieterauswahl, technischen Tests sowie der eigentlichen Migration, knapp sechs Wochen.

Klare Anforderungen definieren

Vorteile aus der neuen Cloud-Infrastruktur will Aryxe insbesondere durch die Steigerung der Effizienz, die Senkung der Kosten, Erhöhung der Sicherheit und mehr Möglichkeiten im Collaboration-Umfeld mit Kunden erzielen. «Nach den positiven Erfahrungen im abgeschlossenen Projekt denken wir darüber nach, weitere Services von Netstream zu beziehen», verrät Muehlemann.

Anderen Unternehmen, die vor ähnlichen Herausforderungen stehen, rät der CEO besonders bei der Planungsphase nicht zu sparen, so dass klare Anforderungen, sowohl technologisch als auch auf das Business bezogen, formuliert werden können. «Nur so können Überraschungen vermieden werden und der potenzielle Technologieanbieter ist in der Lage, entsprechende Services passend anzubieten», meint Muehlemann. Zudem war für Aryxe der Austausch mit einem bestehenden Kunden von Netstream, welcher den entsprechenden Service bereits bezog, von hohem Stellenwert.

«Nach der Beauftragung empfiehlt es sich, Testszenarien im Gate-Prinzip zu durchlaufen», fährt Muehlemann fort und betont auch die Wichtigkeit einer schrittweisen Migration, um allfällige Herausforderungen früh erkennen und reagieren zu können. «Ist die Migration abgeschlossen, sorgt eine Dokumentation zudem für die nötige Transparenz, reduziert das Risiko eines Know-how-Verlusts und stellt ein strukturiertes Vorgehen im Notfall sicher», rät Muehlemann abschliessend. ■

> «Ausser den technologischen Aspekten war für uns eine Begegnung auf Augenhöhe ebenso wichtig»
>
> **Stephan Muehlemann, CEO, Aryxe**

Machine Learning für mehr Sicherheit

Know-how Daten werden zunehmend zur Herausforderung und auch zum Sicherheitsrisiko für Unternehmen. Machine Learning kann heute jedoch als wirksames Hilfsmittel eingesetzt werden, um Risiken zu minimieren.

Von Vesselin Tzvetkov

Die Flut von unstrukturierten Daten wird zu einer immer grösseren Herausforderung für die IT-Sicherheit. Schliesslich müssen eine Vielzahl an IoT-Geräten, Services, Logs, Videos, Chats, Apps, Fotos und Quellen auf relevante Security-Vorfälle hin untersucht werden. Bislang war es üblich, die Daten durch zentrale Security Proxy, Scanner oder Security-Information-and-Event-Management (SIEM)-Tools zu prüfen. Allerdings können klassische Signaturen in Scannern und SIEM-Tools bereits bei kleinen Modifikationen der Datenmuster nicht mehr erkannt werden. Ausserdem werden in vielen Unternehmen oft nur die Logs geschrieben. Dadurch werden die dahinter liegenden Datenstrukturen von konventionellen Security-Lösungen nicht exakt interpretiert und die relevanten Zusammenhänge bleiben im Dunkeln.

Auch Zugriffsmuster über die API sind ein kritischer Punkt. In diesem Bereich stellt sich die Frage, wie auf die Daten zugegriffen werden kann und was die einzelnen HTTP- oder API-Parameter in einem Log konkret bedeuten. Eine solch einfache und typische Frage bei IT-Sicherheits-Audits können Entwickler häufig nicht vollständig beantworten.

Die Nutzung von Serialisierungs-Frameworks impliziert, dass der Entwickler die Kodierung der übermittelten Werte nicht genau kennt. Soll beispielsweise der Name Max Muster technisch übermittelt und gespeichert werden, ist es notwendig, dass die Parameter und die zugrunde liegenden Kodierungsverfahren exakt bekannt sind. Ein nicht exakt definiertes Interface zu schützen, ist für klassische Systeme sehr schwierig, da sie eine exakte Spezifizierung erfordern. Zusätzlich müssen auch die Überprüfungs- und Update-Zyklen überdacht werden. Es reicht nicht mehr, einmal pro Jahr eine Sicherheitsevaluierung durchzuführen. Schliesslich werden die Applikationen täglich neu aktualisiert und jede neue Codezeile kann eine Sicherheitslücke verursachen. Den Code nicht zu aktualisieren, heisst aber im Gegenzug, längst bekannte Schwachstellen offenzulassen. Eine manuelle Evaluierung oder gar vollabdeckende Security-Tests bei grösseren Anwendungen können aber nicht bei jeder Code-Änderung durchgeführt werden. Die Zeit für diese Tests blockiert die Veröffentlichung, sodass kritische Sicherheitsänderungen schnell und automatisiert erkannt werden müssen.

Von einer intelligenteren Erkennung profitiert auch die Analyse von Kommunikationsmustern von Datenbanken. Ein Beispiel: Eine Datenbank wird jede Minute von einer Anwendung kontaktiert und lädt 100 Kilobyte an Daten. Nach einem Update werden plötzlich alle zwei Minuten 1 Megabyte an Daten geladen. Ist das normal oder steckt dahinter ein gezielter Angriff auf Kundendaten? Die Definition, was ein normales Kommunikationsmuster ist, kann nur selten manuell erfolgen, weil die Komplexität der Anwendungen in den meisten Fällen zu hoch ist. Ein solches Muster präzise zu identifizieren, ist jedoch entscheidend für die Sicherheit.

Das gleiche Prinzip gilt auch beim Nutzerverhalten. Hat ein Anwender ein neues Smartphone, erweitert er seinen Freundeskreis oder geht er einem neuen Hobby nach, so kann dies sehr schnell zu einem komplett neuen Benutzerverhalten führen. Aus Sicht der Analysesoftware kann dahinter aber auch ein Identitätsdiebstahl stecken. Das Problem: Wie genau ein Nutzer eine Anwendung konkret einsetzt, lässt sich nur schwer antizipieren. Bei einer klassischen Sicherheitslösung ist es jedoch erforderlich, das bereits von vornherein zu definieren, da sonst abnormales Verhalten nicht festgestellt werden kann.

Höhere Exposition kritischer Services und Daten

Ausserdem erfolgt in vielen Fällen die Inventarisierung von möglichen Schwachstellen der IT-Sicherheit nur mangelhaft. So lässt sich oft nur schwer feststellen, welche Kunden- und Unternehmensdaten tatsächlich online verfügbar sind. Da in Unternehmen heute viele Projekte in kurzen Abständen starten, ist eine lückenlose Dokumentation und Überprüfung schwierig. Ohne die Daten zu kennen, lässt sich aber kein effektiver Schutz gewährleisten.

Zu den klassischerweise am häufigsten auftretenden Sicherheitsvorfällen gehören vergessene Datenbank-Backups im Internet, Schlüssel von Entwicklern direkt in den Code-Repository eingebettet, sowie das Publizieren unternehmensinterner Daten auf öffentlichen Websites. Unbedachte Handlungen und Fehlverhalten von Mitarbeitern werden so zu einem Risiko. IT-Sicherheitsrichtlinien, also Policies, können die ungewollte Herausgabe oder versehentliche Veröffentlichung von Daten verhindern. Allerdings handelt es sich bei diesen nur um administrative Massnahmen – eine technische Kontrolle können sie nicht ersetzen.

Ob wirklich eine Sicherheitslücke besteht, wird in vielen Firmen durch ein Se-

curity Operation Center (SOC) überprüft. Dort werden alle Ereignisse analysiert und von geschultem Personal entweder eskaliert oder als falsche Alarme identifiziert. Können weder eine Anwendung noch das entsprechende Kommunikationsmuster identifiziert werden, gibt es in der Folge zwei Optionen: entweder eine sehr hohe Anzahl an Falschmeldungen oder aber unerkannte Angriffe. Durch die nicht bekannten Kommunikationsmuster und normale API-Anfragen entstehen sehr viele falsche Alarme, die manuell bearbeitet werden müssen. Dabei handelt es sich um eine repetitive und ressourcenintensive Aufgabe. Letztlich investieren Mitarbeiter viel Zeit in einfache, wenig strategische Aufgaben, die nicht notwendigerweise händisch erledigt werden müssten.

All diese Punkte sprechen für ein Security-Konzept, das Machine Learning aus der Cloud beinhaltet. Dafür spricht unter anderem, dass grosse Datenmengen eine nach Bedarf skalierbare Lösung verlangen. Sind kurzfristig mehrere Terabyte an Daten zu evaluieren, so müssen die Ressourcen dafür nicht dauerhaft vorgehalten werden. Bezahlt wird pro Stunde oder bezogen auf die jeweilige Datenmenge. Cloud Provider bieten dabei Algorithmen, die sich innerhalb von Minuten einsetzen lassen, quasi im Baukastensystem an. Passt eine bestimmte Architektur oder ein Algorithmus nicht zu den eigenen Anforderungen, so lässt er sich schnell und unkompliziert anpassen.

Machine Learning im Sicherheitskontext

Regel- und Signatur-basierte Sicherheitssysteme erkennen Sicherheitsverletzungen anhand von vordefinierten Mustern. Allerdings kann jeder potentielle Angreifer mit Grundkenntnissen in Machine Learning (ML) ohne viel Aufwand ein Modell trainieren, das ein Reverse Engineering der Verteidigungsregeln durchführt und so das Sicherheitssystem überwindet. Adaptive ML-Systeme dagegen können auch solche Angriffe erkennen.

Algorithmen zur Anomalie-Erkennung sind etwa die Unterscheidung von Ausreissern aus einem gleitenden Durchschnitt oder anderen Statistiken, K-Means-Clustering, in denen das Verhalten auf K-Gruppen-Cluster verteilt wird oder K-Nearest-Neighbours, mit denen die Entfernung zu den K-Nearest-Neighbours-Punkten kalkuliert wird. Wenn die Entfernung zu gross ist, wird der Punkt als Ausreisser definiert. Eine weitere Variante sind Autoencoders, wobei es sich um ein Neuronales Netz (NN) zur Dimensionsreduktion handelt. Nachdem die Daten in einer niedrigeren Domäne kodiert wurden, kristallisiert sich in der Regel heraus, was anormal ist.

Überwachte ML-Systeme sind so konzipiert, dass sie zuerst Muster in klassifizierten Daten erkennen, wie zum Beispiel Sicherheitsverletzungen und anormales Verhalten. Das überwachte ML-System wird auf den Datensatz geschult und verwendet ihn als Ausgangslage. Nachdem das ML-Modell trainiert wurde, kann es auf einen neuen, nicht klassifizierten Datensatz angewendet werden, von dem nicht bekannt ist, ob er ein Angriff ist. Im Idealfall kann das trainierte ML-Modell die abnormalen Verhaltensweisen und dadurch potenzielle Angriffe erkennen. Die Anwendungen können sowohl gemäss den Klassifizierungsmerkmalen als auch gemäss den Dateninhalten variieren. Wenn die Daten boolescher Art klassifiziert sind, etwa als Angriff/nicht, ist es möglich, Algorithmen wie Logistic Regression, Decision Trees oder in ihren fortgeschrittenen Formen Random Cut Forest und Gradient Boosting anzuwenden. Neuronale Netze können bei einer booleschen Klassifizierung angewendet werden, aber auch auf jede andere Art von Datenstruktur. So ist es durch NN möglich, Muster in Texten zu erkennen, etwa Kreditkartendaten oder personenbezogene Informationen. Wiederkehrende neuronale Netze (RNN) sind eine gängige Technik zur Identifizierung solcher Muster.

ML im praktischen Beispiel

Es existiert eine breite Palette von ML-Algorithmen. Einer davon ist beispielsweise Amazon Macie von Amazon Web Services (AWS). Dabei kommt Machine Learning zum Einsatz, um Daten automatisch zu erkennen, zu klassifizieren und anormale Benutzerzugriffe oder Verhalten zu identifizieren. Dazu werden zuerst Daten durch Natural Language Processing (NLP) klassifiziert. Die Informationen werden nach Gruppen von Personen, Daten, Geschäftswert, Schlüsseln/Zertifikaten, Source Code und weiteren Parametern klassifiziert. Mit Hilfe von NN findet die Lösung Anomalien bei den Zugriffen auf diese Daten. Tritt eine Anomalie auf, wird ein Alarm generiert. Ein Dashboard gibt dem Administrator alle notwendigen Informationen.

Die Konten (User) und Instances (Virtuelle Maschinen) werden fortlaufend auf böswillige oder unbefugte Verhaltensweisen untersucht. Die Lösung erkennt verdächtige Angreifer mithilfe integrierter Feeds mit Informationen zu den jeweiligen Bedrohungen und nutzt maschinelles Lernen zur Erkennung von Angriffen beim Benutzerverhalten und bestimmten Workloads. Wenn der Service eine potentielle Bedrohung erkennt, wird eine ausführliche Sicherheitswarnung bereitgestellt. Das können zum Beispiel Bitcoin-Mining, Malware, Port-Scans oder der Zugriff von einem potentiellen Malware-Server sein.

Für die Analyse mit Machine Learning werden folgende Quellen verwendet: Netzwerk-Logs (wie TCP-Aktivitäten), Benutzer-API-Aufrufe (Starten und Stoppen von EC2-Instanzen), DNS-Auflösung (Wohin kommuniziert eine Instance im Internet?) und Thread-Intelligence-Quellen (Welche Malware ist gerade im Umlauf?). Der Vorteil dabei ist, dass keine Agent Software auf dem Rechner notwendig ist. Der Anwender hat dadurch keinerlei Performance-Einbussen oder Anwendungsprobleme, wie beim Virenscanner.

Machine-Learning-Algorithmen, Cloud-Elastizität und Visibilität sind wichtige Hilfsmittel der Sicherheitsmitarbeiter, um mit der Flut von Daten und Komplexität umgehen zu können. Die neuen Möglichkeiten durch Machine Learning kommen Unternehmen bestimmt entgegen. Für Mitarbeitende heisst es nun, sich weiterzubilden, um die Prinzipien von Maschine Learning und ML-Algorithmen zu verstehen. ■

DER AUTOR

Vesselin Tzvetkov ist Senior Security Consultant bei AWS Professional Services und beschäftigt sich mit Sicherheitsarchitektur und der Entwicklung innovativer Lösungen. Er hat an der TU-Darmstadt in Sicherheit promoviert und an der Universität Bochum in Deutschland einen M.S. in Elektrotechnik erworben.

Cloud-Speicher für Unternehmen

Marktübersicht Das Speichern von Daten in der Cloud bietet viele Vorteile: Skalierbarkeit, Flexibilität und vor allem Kosteneinsparungen. «Swiss IT Magazine» präsentiert 23 Angebote für Schweizer Unternehmen im Überblick.

Von Simon Wegmüller

Storage bedeutete früher: Ein ständig wachsender Haufen von Festplatten, irgendwo im Keller gelagert, damit einhergehender stetiger Platzmangel, Hardwareausfälle und vergessen gegangene Backups. Zugegeben, dabei handelt es sich sicher um ein etwas gar negatives Szenario, doch steckt darin zumindest ein Funke Wahrheit – Datenhaltung konnte und kann auch heute noch dem dafür zuständigen IT-Profi in einem Unternehmen regelmässig den Schlaf rauben.

Doch dann trat die Cloud auf den Plan, und damit skalierbarer Speicher zu einem günstigen Preis. Cloud-Speicher bietet auf den ersten Blick eine Reihe von Vorteilen gegenüber herkömmlicher Datenspeicherung. So kann von überall her, einen Internetzugang vorausgesetzt, auf die in der Cloud gespeicherten Daten zugegriffen werden. Es müssen keine physischen Speichermedien mehr gelagert werden, oder, in Zeiten des mobilen Arbeitens, gar mit sich herumgetragen werden. Auch die Wahl des Clients zum Arbeiten wird unwichtig, da die Daten direkt in der Cloud gespeichert und abgerufen werden können. Und auch in Sachen Kollaboration bietet die Cloud viele neue Möglichkeiten. So können Teammitglieder etwa gemeinsam an einem Projekt arbeiten und Dateien können mit Personen auf der ganzen Welt und in Sekundenschnelle geteilt werden.

Für KMU, so die Anbieter, bieten sich Cloud-Speicher-Angebote geradezu an, da dadurch die Komplexität der eigenen IT-Infrastruktur reduziert werden kann. «Es gibt meiner Meinung nach drei gute Gründe für KMU, die Daten in einer Schweizer Cloud zu lagern: Höhere Sicherheit, niedrigere Kosten und erhöhte Produktivität im Team», bringt es Florin Gruber, Chief Information Security Officer bei Filesync, auf den Punkt.

Häufige Anwendungsfälle für Enterprise Cloud Storage sind Archivierung, die primäre Speicherung von Anwendungsdaten sowie Backup und (Disaster) Recovery. Unternehmen sollten zudem besonders dann Cloud-Speicher in Betracht ziehen, wenn das Bedürfnis besteht, hohe Speicherkosten vor Ort zu minimieren, das komplexe Daten-Management zu Externalisieren und die Notwendigkeit, die Infrastruktur vor Ort zu aktualisieren, aus der Welt zu schaffen.

Grosse Angebotsvielfalt

Heute existieren hunderte verschiedener Cloud-Speicher-Lösungen. Während sich einige davon auf sehr spezifische Anwendungsfälle fokussieren, zum Beispiel das Speichern von E-Mails oder Bildern, steht auch zur Speicherung digitaler Daten aller Art eine Vielzahl von Angeboten zur Verfügung. In der Regel besteht die Infrastruktur solcher Systeme aus hunderten von Datenservern, die in Rechenzentren platziert sind. Dabei ist es essenziell, dass Daten immer auf mehreren Maschinen, und, wenn möglich, in verschiedenen geographischen Zonen abgelegt werden. Dies wird als Redundanz bezeichnet und garantiert Kunden, auch dann auf ihre Daten zugreifen zu können, wenn einzelne Server oder gar Rechenzentren ausfallen. Als weiteren Sicherheitsmechanismus besitzen zur Datenhaltung verwendete Server ausserdem jeweils mehrere Netzteile, um die Stromzufuhr auch bei Ausfall einer Stromversorgung zu gewährleisten.

Während die Anforderung an eine Cloud-Speicher-Lösung seitens Kunden zwar sehr unterschiedlich sein können, erwähnt doch eine grosse Anzahl der von «Swiss IT Magazine» befragten Anbieter deren Wunsch, dass die Daten in der Schweiz aufbewahrt werden und der Datenschutz gewährleistet ist. «Unsere Kunden wünschen sich eine sichere Umgebung für die Firmendaten und einen zentralen Ort – Datenspeicherung in der Schweiz –, an dem die Benutzer Dateien bearbeiten und austauschen können», verrät etwa Tobias Christen, CEO von Dswiss, und erwähnt damit auch gleich den wohl am zweitmeisten genannten Feature-Wunsch der Kunden: Kollaborationsmöglichkeiten. Dies bestätigt zum Beispiel auch Andre Salzmann, Produktmanager bei Axians Ruf: «Kunden wünschen sich einen Cloud-Speicher, der ihnen die Zusammenarbeit und die gemeinsame Dateiennutzung mit internen und externen Benutzern erleichtert.»

Zuverlässigkeit & Sicherheit

Die beiden grössten Bedenken bezüglich Cloud Storage sind derweil die Zuverlässigkeit und Sicherheit. Kunden werden ihre Daten wahrscheinlich nicht einem anderen Unternehmen anvertrauen, ohne sicher zu sein, dass sie jederzeit auf ihre Informationen zugreifen können und niemand sonst Zugriff darauf erhält. Um Daten dahingehend zu schützen, verwenden die meisten Systeme eine Kombination von Technologien.

Besonders die Möglichkeit, Daten verschlüsselt abzulegen, indem komplexe mathematische Algorithmen zur Kodierung von Information verwendet werden, hilft Anbietern dabei, bei Kunden das ➤

nötige Vertrauen zu gewinnen. Des weiteren sind auch Authentifizierungsprozesse hier wie dort Pflicht und nicht selten werden diese zusätzlich durch Multi-Faktor-Authentifizierung unterstützt, wobei mehrere voneinander unabhängige Komponenten für den Zugriff auf die Daten benötigt werden. Ein Beispiele wäre etwa nach dem Login die Übermittlung eines Sicherheitscodes via Smartphone. Letztlich empfiehlt sich auch die Implementierung von verschiedenen Autorisierungsebenen, so dass nicht alle Mitarbeiter Zugriff auf alle Daten erhalten. So kann beispielsweise ein Front-Desk-Mitarbeiter nur sehr eingeschränkt auf Daten zugreifen, die auf einem Cloud-System gespeichert sind, während der Leiter der Personalabteilung umfangreichen Zugriff auf Dateien hat.

Doch selbst mit diesen Schutzmassnahmen benötigt es immer noch einen gewissen Grad an Vertrauen gegenüber dem Anbieter. Um dieses zu gewinnen, setzen Anbieter einerseits auf Zertifizierungen, andererseits auf moderne (Rechenzentrums-)Infrastrukturen, die sie teils selber

23 CLOUD-STORAGE-ANGEBOTE FÜR UNTERNEHMEN

ANBIETER	ACRONIS	AGIBA IT SERVICES	AXIANS	BECHTLE STEFFEN	DSWISS	ECLIPSO
Name des Angebots	Acronis Backup Cloud	MySwissCloud.ch	FA Sync & Share	360° Sharefile	Securesafe	eclipso Business
Allgemeine Angaben zum Anbieter						
Anzahl Kunden in der Schweiz	> 4000	> 100	> 1000	>250	> 1000 KMU	k.A.
Server-Standort(e)	Schweiz, Deutschland u.a.	Schweiz	Schweiz	Schweiz	Schweiz	ausschliesslich Deutschland
Zugriff auf Cloud-Speicher via						
Web Interface	■	■	■	■	■	■
Client Software für PC	■	■	■	■	■	■
Mobile App	■	■	■	■	■	■
Unterstützte Plattformen (Software / App)						
Windows / MacOS / Linux	■ / ■ / ■	■ / ■ / ■	■ / ■ / ❑	■ / ■ / ■	■ / ■ / ❑	■ / ■ / ❑
iOS / Android	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■
Protokolle						
WebDAV	❑	■	❑	■	❑	■
FTP	❑	■	❑	■	❑	❑
SMB / CIFS	■ / ■	■	■	❑	❑	❑
Rsync	❑	❑	❑	❑	❑	❑
Sicherheit						
Verschlüsselte Übertragung	SSL 256-Bit AES	SSL 256-Bit AES	SSL 256-Bit AES	SSL 256-Bit AES	TLS 256-Bit, RSA-2048, 256-Bit AES	■
Verschlüsselte Lagerung	256-Bit AES	256-Bit AES	256-Bit AES	SSL 256-Bit AES	256-Bit AES	❑
Datenschutzstandards	ISO 27001, ISO 50001	ISO 27001, FISMA, FIPS	FIPS 140-2	k.A.	ISO 27001	DSGVO, BDSG
Georedundante Sicherung (Anzahl)	■ (k.A.)	■ (2)	❑	■ (1)	■ (3)	❑
Umfang / Beschränkungen						
Speicherplatzlimit (insgesamt)	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimiert	50 GB
Limit Dateigrösse	unlimitiert	unlimitiert	100 GB	100 GB	2 GB	100 MB
Limit Transfervolumen (pro Tag)	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimiert	2000 GB/Monat
Min. / Max. Nutzeranzahl	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimiert	k.A.
Kosten und Vertrag						
Einmalige Einrichtungskosten	keine	je nach Dienst untersch.	■	1500 Franken	keine	keine
Pay as you use	■	■	❑	■	■	k.A.
Preise pro Monat (nur Speicherplatz, ohne zusätzliche Nutzer)	kein MSRP für Endkunden, da Vertrieb durch Service Provider	je nach Dienst unterschiedlich	50 GB zu Fr. 10.–	10 GB zu Fr. 10.–	100 GB zu Fr. 12.– 1000 GB zu Fr. 108.–	€ 7.90
Kostenlose Demoversion	■	■	Nach Vereinbarung	■	10 GB für 1 Monat	■
Mindestvertragsdauer	1 Jahr	1 Jahr	1 Jahr	6 Monate	3 Monate	12 Monate
Kündigungsfrist	3 Monate	3 Monate	monatlich	6 Monate	keine	keine
SLAs	■	■	■	■	■	k.A.
Sonstiges						
Benutzerkonten-/Rechteverwaltung	■	■	■	■	■	❑
Collaboration-Tools	■	■	■	■	■	■
Backup-Funktionalität	■	■	■	■	❑	❑
Datenarchivierungs-Funktionalität	❑	■	❑	❑	■	❑
Automatische Synchronisation	❑	■	■	■	■	■
Virenschutz auf Server	■	■	❑	■	❑	■
Info	www.acronis.com	www.myswisscloud.ch	www.axians-ruf.ch	www.bechtle-steffen.ch	www.securesafe.com	www.eclipso.ch

■ = ja, ❑ = nein; k.A = keine Angaben; 1) COS stellt eine S3 Schnittstelle zur Verfügung; 2) über Partnerfirma

betreiben. «Netstream betreibt ein hochsicheres Rechenzentrum in der Schweiz», so Björn Westra, Cloud Solution Sales bei Netstream, und ergänzt: «Alle unsere Services und Angebote unterliegen dem Schweizer Recht und orientieren sich am Schweizer Datenschutzgesetz.»

Doch es besteht immer die Möglichkeit, dass ein Hacker eine elektronische Hintertür und Zugangsdaten findet oder dass ein verärgerter Mitarbeiter mit seinem Benutzernamen und Passwort Daten ändert oder gar vernichtet. Cloud-Speicher-Anbieter investieren deshalb viel Geld in Sicherheitsmassnahmen, um die Möglichkeit von Datendiebstahl oder Korruption zu begrenzen und das Vertrauen ihrer Kunde zu gewinnen.

Das andere grosse Anliegen seitens Kunden, die Zuverlässigkeit, ist derweil genauso wichtig wie die Sicherheit. Ein instabiles Cloud-Storage-System kann zu schwerwiegenden Verlusten, nicht nur in Bezug auf Daten, sondern auch finanziell führen. Niemand will Daten in einem ausfallgefährdeten System speichern, noch einem Unternehmen vertrauen, das

EQIPE	FILESYNC	FIRST FRAME NETWORKERS	GOOGLE	GREEN.CH	IBM	INFONIQA
Nextcloud	**Filesync für Teams**	**First 365 Box**	**Google Cloud Storage**	**Nextcloud**	**IBM Cloud Object Storage**	**Swiss3cloud**
> 300	>10'000	150	k.A.	> 100'000	> 50	> 30
Schweiz	Schweiz	Schweiz	Schweiz, USA	Schweiz	On-Prem (beim Kunden) / Cloud (weltweit)	Schweiz
■	■	■	■	■	■	■
■	■	■	■	■	3rd Party	❑
■	■	■	■	■	3rd Party	❑
■ / ■ / ■	■ / ■ / ■	■ / ■ / ❑	■ / ■ / ■	■ / ■ / ■	■ / ■ / ■ [1]	■ / ■ / ■
■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■ [1]	❑ / ❑
■	❑	■	k.A.	■	❑	❑
■	❑	❑	■	■	❑	❑
■	❑	❑	k.A.	■	■ für Archive Use-Cases	❑
❑	❑	■	■	❑ (Csync)	❑	❑
SSL/TLS 256-Bit	SSL 2048 Bit HTTPS	TLS SHA-256	SSL 256-Bit AES	256-Bit SSL Encryption	SSL 256-Bit AES	SSL 256-Bit AES
256-Bit AES	256-Bit AES	256-Bit AES	256-Bit AES	❑	256-Bit AES	256-Bit AES
ISO 27001	ISO 27001, Tier-IV RZ, SQS	DSGVO	ISO 27001, FISMA, FIPS	Rechenzentrum ISO 27001	ISO 27001, ISO 27017, ISO 27018, FISMA, FIPS	ISO27001
❑	■ (4)	■ (k.A.)	■ (2)	❑	■ (frei wählbar)	❑
unlimitiert	unlimitiert	unlimitiert	unlimitiert	bis 250 GB	unlimitiert	unlimitiert
unlimitiert	unlimitiert	unlimitiert	5 TB	individuell	unlimitiert	5 GB
unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
unlimitiert	unlimitiert	unlimitiert	unlimitiert	bis zu 200	unlimitiert	unlimitiert
keine	keine	keine	keine	494 Franken	keine auf der Cloud	keine
■	❑	■	■	❑	■	■
100 GB zu Fr. 20.–	200 GB zu Fr. 49.90; Je weiterer Nutzer (+100GB): Fr. 15.–	50 GB zu Fr. 11.90.–	50 GB zu $ 1.30 100 GB zu $ 2.60	Ab Fr. 20.– pro 100 GB	Standard $ 0.02/GB, Vault $ 0.01/GB, Cold Vault $ 0.006/GB, Flex $ 0.029/GB, Archive $ 0.002/GB	1 GB zu Fr. 0.03
unlimitiert für 14 Tage	10 GB dauerhaft	■ (Demo-User)	k.A.	❑	30 Tage / 25GB	100 GB für 30 Tage
3 Monate	1 Jahr	12 Monate	keine	6–36 Monate	keine	❑
1 Monat	3 Monate	1 Monat	keine	3 Monate	keine	❑
❑	■	■	■	■	■	■
■	■	■	■	■	■	■
■	■	■	■	■	3rd party	❑
■	■	■	■	■	■	❑
❑	■ [2]	❑	❑	❑	■	❑
■	■	■	■	■	■	❑
■	■	■	❑	❑	❑	❑
www.eqipe.ch	www.filesync.ch	www.firstframe.net	cloud.google.com	www.green.ch	www.ibm.com	www.infoniqa.ch

finanziell instabil ist. Während die meisten Cloud-Speicher-Anbieter versuchen, dieses Problem durch Redundanztechniken zu lösen, besteht immer noch die Möglichkeit, dass ein ganzes System abstürzt und Clients keinen Zugriff auf ihre gespeicherten Daten haben.

Cloud-Storage-Anbieter leben und sterben durch ihren Ruf. Daher liegt es im Interesse jedes Unternehmens, einen sicheren und zuverlässigen Service zu bieten. Wenn ein Unternehmen diese grundlegenden Kundenerwartungen nicht erfüllen kann, hat es keine grosse Chance.

Preise, Migration & Support

Die Kosten für Cloud-Speicher variieren derweil je nach Datenmenge, Datenschutzanforderungen und manchmal auch der Art der Daten. So kann beispielsweise der Abruf von Daten aus der Cloud mit zusätzlichen Kosten verbunden sein. Die Preismodelle können zudem von Anbieter zu Anbieter unterschiedlich sein, so dass Unternehmen sich nach dem für ihre Bedürfnisse am besten geeigneten Cloud Hoster umsehen müssen.

Der Weg der Daten von der lokalen Haltung in die Hände eines Cloud-Speicher-Anbieters ist ein bedeutendes Unterfangen und sollte nicht unterschätzt werden. Dateien müssen migriert, Benutzer geschult und die korrekte Anwendung

23 CLOUD-STORAGE-ANGEBOTE FÜR UNTERNEHMEN (Fortsetzung)

ANBIETER	ITPOINT SYSTEMS	IWAY	MTF	NETSTREAM	ORIENTED.NET
Name des Angebots	**Swiss Dataspace**	**Iway Sync&Share**	**MTF File Cloud**	**Object Storage**	**Wölkli Cloudspeicher**
Allgemeine Angaben zum Anbieter					
Anzahl Kunden in der Schweiz	> 300	30'000	> 1000	30'000	> 1000
Server-Standort(e)	Schweiz	Schweiz	Schweiz	Schweiz	Schweiz
Zugriff auf Cloud-Speicher via					
Web Interface	■	■	■	■	■
Client Software für PC	■	■	■	❑	■
Mobile App	■	■	■	❑	■
Unterstützte Plattformen (Software / App)					
Windows / MacOS / Linux	■ / ■ / ■	■ / ■ / ■	■ / ■ / ■	■ / ■ / ■	■ / ■ / ■
iOS / Android	■ / ■	■ / ■	■ / ■	❑ / ❑	■ / ■
Protokolle					
WebDAV	■	■	❑	❑	■
FTP	❑	❑	❑	❑	■
SMB / CIFS	❑	❑ / ❑	❑	❑	■
Rsync	❑	❑	❑	❑	❑
Sicherheit					
Verschlüsselte Übertragung	256-BIT AES	SSL 256-Bit AES	SSL 256-Bit AES	SSL 256-Bit AES	SSL 256-Bit AES
Verschlüsselte Lagerung	256-Bit AES	256-Bit AES	256-Bit AES	SSE Encryption	256-Bit AES
Datenschutzstandards	ISO 27001, Europrise, ULD	ISO 27001, FISMA, Tier IV	ISO 27001, FIPS, FINMA Konform, GDPR	keine	ISO 27001, DSGVO
Georedundante Sicherung (Anzahl)	Ja (2)	■ (k.A.)	■ (2)	❑	■ (2)
Umfang / Beschränkungen					
Speicherplatzlimit (insgesamt)	unlimitiert	je Abo	unlimitiert	unlimitiert	unlimitiert
Limit Dateigrösse	60 GB	2 TB	5 TB	unlimitiert	1 TB
Limit Transfervolumen (pro Tag)	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
Min. / Max. Nutzeranzahl	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
Kosten und Vertrag					
Einmalige Einrichtungskosten	keine	ab 0.- je nach Abo	250 Franken	keine	keine
Pay as you use	■	❑	❑	■ (oder Bundle Prizing)	❑
Preise pro Monat (nur Speicherplatz, ohne zusätzliche Nutzer)	1 GB zu Fr. 0.80 50 GB zu Fr. 37.50 100 GB zu Fr. 70.–	25 GB zu Fr. 5.– 50 GB zu fr. 25.– 100 GB zu Fr. 60.–	50 GB zu Fr. 19.– 100 GB zu Fr. 38.–	0–4999 GB zu Fr. 0.048/GB 5000–14'999 GB zu Fr. 0.047/GB 15'000–499'999 GB zu Fr. 0.046/GB > 500'000 GB zu Fr. 0.045/GB	10 GB zu Fr. 7.50 50 GB zu Fr. 15.– 200 GB zu Fr. 32.50 500 GB zu Fr. 57.50
Kostenlose Demoversion	30 Tage	Auf Anfrage	■	1 Monat unlimitiert	2 GB für immer
Mindestvertragsdauer	12 Monate	keine	■	keine	1 Jahr
Kündigungsfrist	1 Monat	1 Monat	■	keine	2 Monate
SLAs	■	■	■	■	■
Sonstiges					
Benutzerkonten-/Rechteverwaltung	■	■	■	■ (via Support)	■
Collaboration-Tools	■	■	■	❑	■
Backup-Funktionalität	■	■	■	■	■
Datenarchivierungs-Funktionalität	❑	■ (Versionierung)	■	❑	■
Automatische Synchronisation	■	■	■	❑	■
Virenschutz auf Server	❑	❑	❑	❑ (kein Server existent)	■
Info	www.swissdataspace.com	www.iway.ch	www.mtf.ch	www.netstream.ch	www.woelkli.com

■ = ja, ❑ = nein; k.A = keine Angaben

durch die Mitarbeiter muss überwacht und kontrolliert werden.

Nur logisch also, dass die Anbieter den engen Kundenkontakt und das Supportangebot als zentral betrachten. Andreas Schneebeli, CEO von Agiba IT Services: «Wir als KMU kennen die Bedürfnisse unserer Kunden sehr genau und achten deshalb darauf, auch bei einem Wechsel in die Cloud den vollen Support zu gewährleisten.» Dazu gehören bei vielen Anbieter auch regelmässige Wartungsüberprüfungen und individuelle Schulungs-Angebote für Kunden. So können Kunden bei T-Systems beispielsweise über zusätzliche Service-Vereinbarungen erweiterte Leistungen beziehen, die vom Consulting- und Administrationsservice, der IT-Architekturberatung bis hin zu einem Manager-on-Duty-Service reichen, so Cami Brichet, Solutions Experte Cloud Services bei T-Systems Schweiz. Einige Cloud-Services konzentrieren sich auf grosse Unternehmen, andere auf einzelne oder wenige Benutzer. Und auch die Benutzerfreundlichkeit variiert je nach Angebot. Es muss also auch sichergestellt werden, dass die Endbenutzer mit dem Dienst, für den man sich entscheidet, problemlos arbeiten können. Deshalb spielt auch hier das Support- und Schulungs-Angebot seitens Anbieter eine wichtige Rolle. ■

PROCLOUD	SIMPLYFIND	SPEICHERBOX.CH	SWISSCOM	T-SYSTEMS SCHWEIZ
Business Drive	**Data Safe**	**Home, Business**	**File Service NFS Elastic (via Dynamic Computing Services DCS)**	**Open Telekom Cloud – Object Storage Service**
> 100	k.A.	k.A.	> 2000	> 200
Schweiz	Schweiz	Schweiz	Schweiz	Deutschland
■	■	■	■	■
■	■	■	■	■
■	■	■	❑	❑
■ / ■ / ❑	■ / ■ / ❑	■	■ / ■ / ■	■ / ■ / ■
■ / ■	■ / ■	■ / ■	❑ / ❑	■ / ■
❑	❑	❑	❑	■
❑	❑	❑	❑	■
❑	❑	❑	❑	■
❑	❑	❑	❑	■
SSL/TLS 2048-Bit	SSL 256-Bit AES	SSL 256-Bit AES	❑	SSL 256-Bit AES
256-Bit AES	256-Bit AES, RSA-2048	256-Bit AES, End to End Verschlüsselung	256-Bit AES	256-Bit AES
ISO 27001 (Rechenzentren)	ISO 9001, ISO 27001	❑	ISO 27000, 27001, ISAE 3402	alle üblichen
■ (2)	■ (2)	■ (k.A.)	■ (2)	■ (2)
unlimitiert	1000 GB	unlimitiert	unlimitiert	unlimitiert
unlimitiert	2 GB	5 TB	16 TB	48,8 TB pro Objekt auf Object Storage
unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
keine	keine	keine	keine	keine
❑	■	❑	■	■
500 GB, 5 User zu Fr. 39.– 1 TB, 10 User zu Fr. 69.–	50 GB, Fr. 4.50 200 GB,Fr. 9.00 1000 GB, Fr. 15.00	100 GB zu Fr. 59.– 500GB zu Fr. 130.– 1TB zu Fr. 250.– 500GB pro Benutzer zu Fr. 11.–	1 GB zu Fr. 0.24.–	EUR 0.022/GB
100 GB, 2 User für 30 Tage	50 GB, 2 User für 30 Tage	alle Angebote für 30 Tage	❑	❑
1 Monat	12 Monate	1 Jahr	keine	keine
keine	keine	1 Monat	keine	keine
❑	❑	■	■	■
■	■	■	■	■
■	■	■	❑	■
❑	■	■	■	■
❑	■	■	■	■
■	■	■	■	❑ (kann zugeschaltet werden)
❑	■	❑	❑	❑
www.business-drive.ch	www.simplyfind.com	www.speicherbox.ch	www.swisscom.ch	open-telekom-cloud.com

Quelle: «Swiss IT Magazine»

Daten an der Quelle schützen und veredeln

Know-how Die Menge an Daten nimmt immens zu – und die Datenflut muss auch sinnvoll verarbeitet werden. Der richtige Objektspeicher im Zentrum hilft dabei.

Von Mathias Wenig

Durch Konzepte wie das Internet der Dinge entstehen nicht nur immense Mengen an Daten – sie müssen auch sinnvoll verarbeitet werden. Dabei sind Unternehmen im Vorteil, die aus den Datenmassen schnell logische Schlüsse ziehen können. Der Einsatz von Objektspeicher im Zentrum kann dabei helfen.

Immer mehr Hersteller pflanzen in ihre Alltags- und Gebrauchsgeräte Sensoren, Prozessoren und Software ein. Selbst Toaster, Kaffeeautomaten oder Mixer kommunizieren mit ihrer Umgebung. Das Ziel der Hersteller ist dabei meist, den gesamten Lebenszyklus des Produktes begleiten zu können. Auch die Produktion wird entsprechend aufgerüstet und immer mehr Daten werden erfasst.

Die Anbieter versuchen damit zu verstehen, wann und warum ihr Produkt den Geist aufgibt und was der Kunde wünscht. Die Menge der Daten, die dafür zu verarbeiten und auszuwerten sind, wird rasant zunehmen. Einen Mehrwert haben dann nur diejenigen Unternehmen, die ihre Daten schnell und richtig interpretieren.

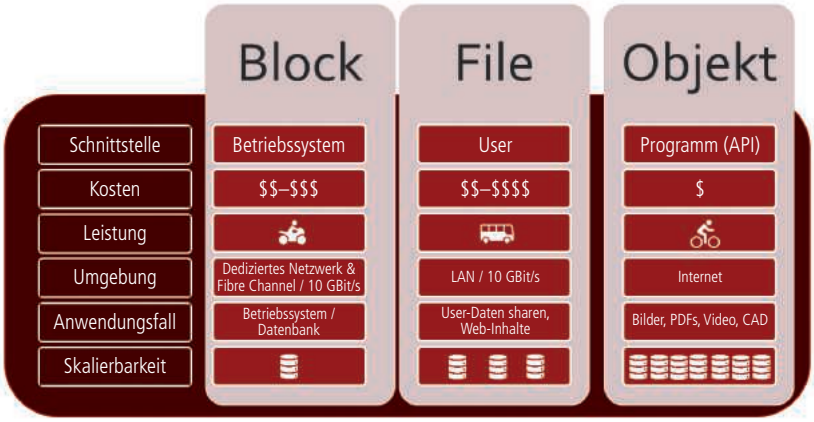
Dafür müssen zwei Voraussetzungen erfüllt werden. Zum einen gilt es, Plattformen aufzusetzen, die die zunehmende Flut an unstrukturierten Daten extrem skalierbar bewältigen können. Zum anderen müssen die Daten im zweiten Schritt «veredelt» werden. Damit ist gemeint, dass ihre Inhalte verständlich und die richtigen Informationen über passende Prozesse automatisch weiterverarbeitet werden. Das kann in eigenen Cloud-basierenden Micro-Services oder bei Partnern geschehen, die mit ihren Diensten die Daten zusätzlich anreichern oder ihre Leistungen an bestimmte gesammelte Datenkriterien koppeln. Ein typisches Beispiel dafür sind Sonderleistungen, etwa ein Premiumsupport durch einen externen Dienstleister.

Datenpakete schnüren für bessere Skalierbarkeit

Durch IoT-Anwendungen werden bereits heute Unmengen an Daten generiert und Experten schätzen, dass die gesamte Datenmenge aus IoT-Applikationen schon bald auf mehrere Zettabytes ansteigen wird. So wird alleine ein Connected Car mit all seinen Komponenten täglich ein Terabyte generieren.

All diesen Daten gemeinsam ist ihre grösstenteils statische Natur. Meist werden Momentaufnahmen erfasst und archiviert – mit dem Ziel, sie später auszuwerten. Ein Beispiel dafür ist der Online-Handel. Dort werden seit Langem die Interessen des Käufers, seine Kaufhistorie und die letzten Zugriffe auf Produkte als Metadaten zusätzlich archiviert. Auch Plattformen wie Sky, Netflix oder Facebook agieren wie grosse Archive. Und jeder, der auf einem Social-Media-Portal einzelne Bilder oder Videos hochgeladen, Kommentare abgegeben oder andere Inhalte aufgerufen hat, geniert Daten, die schlussendlich statischer Art sind.

DATENSPEICHERARCHITEKTUREN



Quelle: Veritas

Objektspeicher verwaltet Daten als Objekte, im Gegensatz zu anderen Speicherarchitekturen wie Dateisystemen oder Blockspeicher. Dies bietet verschiedene Vorteile, gerade wenn es sich um unstrukturierte Daten handelt.

Die Anbieter dieser Dienste setzen zum Speichern und Organisieren dieser Daten meist auf sogenannte Objektspeicher. So laufen aktuelle Workloads wie S3, Facebook oder Spotify alle auf dieser Art von Speicherarchitektur. Aber auch in Software-defined Architekturen und Opensource-Projekten wie OpenStack, Swift, Redhat und Ceph sind entsprechende Objektspeicher verbreitet. Entwickler moderner Applikationen und Dienste erwarten deshalb zurecht, dass ihre Cloud-basierenden Systeme auf solche Strukturen zurückgreifen können. Schliesslich garantieren sie relative einfache Skalierbarkeit, auch in einem globalen Kontext.

Objekt Store

Der Vorteil eines Objektspeichers sind seine Struktur und die Organisationsweise, also die Art und Weise, wie er Daten als Objekt ablegt und auffindbar macht. Dabei kommen drei Elemente zum Tragen: die eigentlichen Daten – ob Urlaubsbild, Musikstück oder eine Konstruktionszeichnung; weitere Attribute als Metadaten, die einen zusätzlichen Kontext liefern; und ein global einzigartiger Identifier, der das Objekt in einem verteilten System auffindbar macht.

Im Objekt Store ist jedes Objekt mit all seinen Zusatzparametern wie den Metadaten als Ganzes abgelegt. Dabei entfallen komplexe Hierarchien, mit denen die Daten sonst kategorisiert werden. Schliesslich darf der User konzeptionell direkt auf das gesamte Objekt mit all seinen Zusatzdaten im Objekt Store zugreifen. Sollen später einzelne Teile des Objekts modifiziert werden, so muss über den Objekt Store das ganze Objekt geöffnet, aktualisiert, umgeschrieben und dann wieder gespeichert werden. Das kostet Systemressourcen, weshalb Objektspeicher sich eher für unstrukturierte Daten und Workloads eignen, die häufig Read-, aber selten Write-Anfragen stellen.

Müssen häufig Daten geschrieben werden, so sind Block-basierende Speicher die bessere Wahl. Ein Beispiel für sich schnell ändernde Daten sind transaktionale Einträge in Datenbanken, die in Echtzeit geschehen. Auch für geteilte Daten, die von vielen Usern gleichzeitig bearbeitet und überschrieben werden, sind blockbasierende NAS-Systeme besser geeignet.

Der Vorteil des Objektspeichers ist seine simple und massive Skalierung. Wird mehr Platz für Webinhalte, Backup-Daten oder Archive benötigt, muss der Objektspeicher einfach nur um neue Nodes erweitert werden. Dabei kann der Speicher sehr schnell und flexibel an den Bedarf angepasst werden und der Anwender kann alte und neue Hardware miteinander mischen. Ein teures Upgrade der kompletten Infrastruktur – mit langen Ausfall- und komplexen Projektzeiten – entfällt.

Die technische Grundlage dabei ist der so genannte flache Namespace. In ihm sind die Daten standortübergreifend als Objekte organisiert. Das so genannte Erasure Coding, kurz EC, schützt dabei die Daten im Namespace vor Fehlern und Verlust. Die Grundlage dafür ist ein mathematisches Verfahren zum Datenschutz, das Daten in Fragmente aufteilt, erweitert und neu mit redundanten Teilen codiert, die dann auf physikalisch getrennten Orten gespeichert werden. Im Schnitt passiert das an mindestens drei Orten. Selbst beim Ausfall einer Node sind die Daten also immer noch an zwei anderen Orten präsent. Der laufende Betrieb wird dadurch nicht eingeschränkt und es kann mit günstigen Commodity-Hardwareelementen gearbeitet werden, da die Objektarchitektur Ausfälle robust und schnell selbst kompensiert.

Daten – das wichtigste digitale Gut

Daten sind ein wertvoller Rohstoff, dessen Kontrolle Unternehmen in der eigenen Hand halten wollen. Mit Blick auf die Cloud werden jedoch auch andere Dienste, Partner, Provider und ihre Algorithmen auf Teile der Firmendaten zugreifen, um diese zu veredeln. Beispiele dafür sind die Artificial Business Intelligence Engine von Google, der Finanzdienst eines Partners oder die Software des Logistikpartners. Umso wichtiger ist die Kontrolle der Daten.

Die Datenhoheit ist jedoch nur gewährleistet, wenn der Datenschutz gewahrt bleibt und nur derjenige auf Metadaten im Objekt zugreifen darf, der dazu berechtigt ist. Angesichts der grossen Menge von Objekten pro Namespace und Datenvolumina in Zettabyte-Dimensionen muss der Objektspeicher selbst eine Reihe von Aufgaben direkt an der Quelle ausführen. Dazu gehört das selbstständige Klassifizieren der Daten, damit stets eindeutig geklärt ist, um was für Inhalte es sich überhaupt handelt. Der Versuch, dies über externe Zusatzmodule zu erledigen ist zum Scheitern verurteilt, denn das Datenwachstum wird ständige Erweiterungen erfordern und Flaschenhälse sind vorprogrammiert. Effizienter ist es also, dass der Objektspeicher diese Aufgabe im Speicher selbst durchführt, bevor er Anfragen zu einem bestimmten Objekt beantwortet.

Eine grosse Rolle spielt dieser Aspekt im Zusammenhang mit Vorschriften rund um Compliance und Datenschutz. Per Software-Richtlinie lässt sich dann klar steuern, an welche angekoppelten Dienste das Objekt weitergegeben werden darf und an welche nicht.

Da der Objektspeicher im Zentrum der Architektur steht, muss dieser selbstverständlich alle gängigen Protokolle und Plattformen im Cloud-Segment von sich aus unterstützen. Dazu gehören Dienste wie S3, eine Rest API, MQTT genauso wie Java, JDBC, Thrift, Kafka oder HDFS. Dadurch können die Entwickler flexibel aus einer Vielzahl an Schnittstellen wählen.

Mit dem Objektspeicher wandelt sich also ein einfaches Datenarchiv hin zu der Steuerungs- und Säuberungszentrale, mit denen Firmen die Datenmassen auch in Zukunft bewältigen, die im Zuge von Digitalisierung und IoT entstehen. Das geschieht, indem sie die Inhalte der Datenmassen einsehen und klassifizieren, darauf basierend Workflows anstossen und somit die Daten veredeln. Genau das ist die Grundlage für moderne Cloud-basierende Dienste, die auf globaler Ebene skalierbar sind. ■

DER AUTOR

Mathias Wenig ist Senior Manager TS und Digital Transformation Specialist bei Veritas und leitet ein Team technischer Vertriebsingenieure in Deutschland, Österreich und der Schweiz. Er und sein Team sind dafür verantwortlich, Kunden jeder Grösse in diesen Ländern dabei zu helfen, ihre Cloud-Strategie weiterzuentwickeln und ihre Rechenzentren zu modernisieren. Dabei orientiert er sich an der Multi-Cloud-Data-Protection-Strategie von Veritas, um gemeinsam mit seinem Team Kunden gezielt zu beraten.

Altdaten – der blinde Fleck

Digitale Transformation: Die richtige Strategie sieht eine systemunabhängige Plattform für Informationsmanagement vor.

Daten sind der Treibstoff der digitalen Wirtschaft – sagt man. Und das zurecht. Wer sie im Kontext, am besten in Echtzeit und unabhängig von der anfallenden Datenmenge analysieren kann, reagiert schneller auf Marktveränderungen, passt sein Angebot besser als die Konkurrenten an Konsumentenwünsche an und ist in der Lage, neue Geschäftsmodelle, Produkte und Services zu entwickeln. Doch dafür ist es notwendig, alle Daten – die in den operativen Systemen benötigten wie die nicht mehr aktiv benötigten – zu berücksichtigen.

Aktuelle wie Altdaten müssen vor Cyberangriffen geschützt werden und ihre Verarbeitung, Aufbewahrung und Analyse hat den Vorgaben der verschiedenen Regularien zum Datenschutz genügen – und zwar vor wie nach einer Datenmigration. Zu diesen Regularien zählt insbesondere seit dem vergangenen Jahr die europäische Datenschutz-Grundverordnung (EU-DSGVO), die von den Unternehmen die Fähigkeit verlangt, Informationen auf der Ebene des einzelnen Datensatzes gezielt zu löschen. Für die Aussagekraft der Analysen ist es zudem unerlässlich, dass auch bei den Altdaten die Qualität optimiert wird, bevor sie ausgewertet werden. Denn schlechte Daten bringen schlechte Analyseergebnisse.

Datensicherheit, Datenschutz, Datenmigration, Big Data – all diese Aspekte sind umso wichtiger, als die meisten Unternehmen im Rahmen von Digitalisierungsinitiativen ihre Anwendungslandschaften modernisieren und dabei neue Softwaregenerationen implementieren. Illustres Beispiel sind die 50.000 SAP-Bestandskunden weltweit, die bis 2025 auf SAP S/4HANA migrieren müssen. Sie verfolgen mit dieser Migration das Ziel einer agilen Applikationslandschaft, mit deren Hilfe sie die digitale Transformation meistern können.

Das ist Herausforderung wie Chance zugleich. Chance, weil sich die Qualität der Daten optimieren lässt und diese sich besser als auf Legacy- oder Archivsystemen gegen Angriffe und Datenschutzverletzungen sichern lassen. Herausforderung, weil sich nicht eins zu eins auf die Ebene der Daten übertragen lässt, was als Ziel auf der Ebene der Anwendungen völlig richtig und erstrebenswert ist.

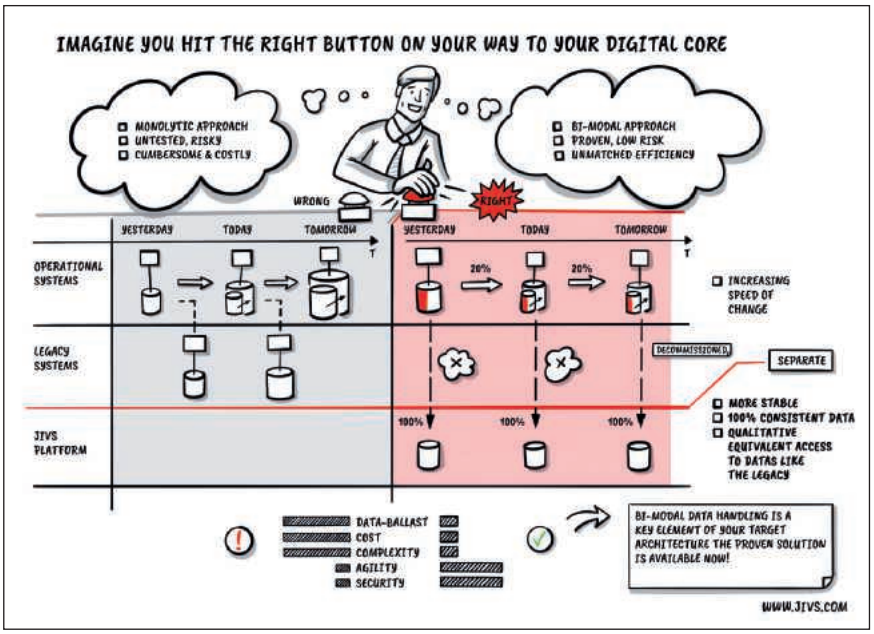
Denn auf der Ebene der Daten geht es also weniger um Agilität als um Stabilität. So darf die Datenstruktur, die auch den geschäftlichen Kontext ihrer Entstehung und Verarbeitung abbildet, über den gesamten gesetzlich vorgeschriebenen Zeitraum nicht verändert werden.

Der richtige Ansatz – eine Frage der Architektur

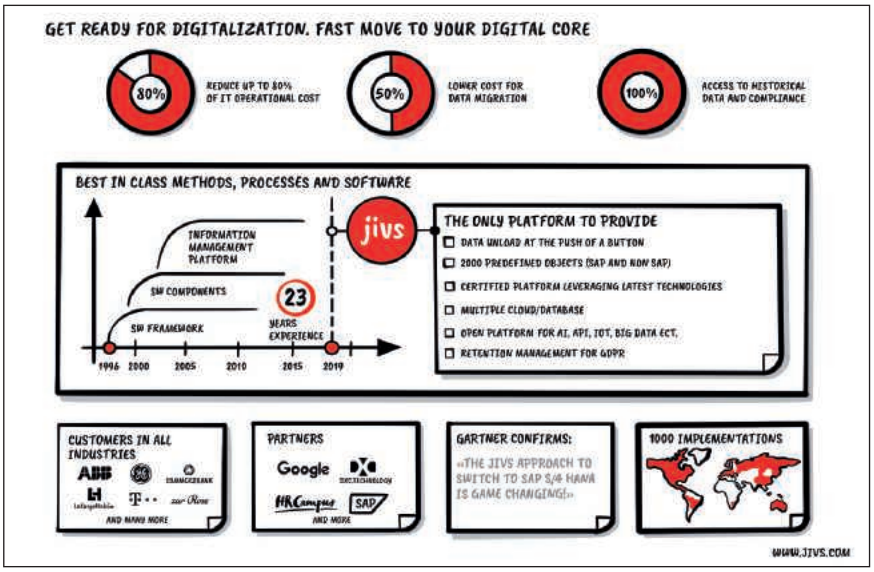
Die alles entscheidende Frage lautet daher: Wie lassen sich die entgegengesetzten Ziele Agilität und Stabilität miteinander in Einklang bringen? Mit Hilfe eines neuen Ansatzes: einer anderen Architektur der Applikationslandschaft, die Altdaten und -dokumente von den agilen Apps der Zukunft trennt. Altsysteme lassen sich dadurch abschalten, neue Softwaregenerationen dauerhaft schlank und agil halten.

Schlüsselelement dieser neuen Architektur ist eine eigene systemunabhängige Umgebung für Daten, Dokumente und ihren Geschäftskontext, die nicht mehr in den operativen Systemen benötigt werden. Eine solche Umgebung sorgt für die gebotene Stabilität auf der Datenebene. Gleichzeitig erhöht sie die Rechts- und IT-Sicherheit. Denn sie lässt sich anders als viele Altsysteme weiter patchen und absichern. Zudem erlaubt sie, mittels Funktionalitäten für Retention Management den gesamten Lebenszyklus von Altdaten und -dokumenten auf der Ebene der einzelnen Datensätze und Dokumente lückenlos zu managen. Dies schliesst ausdrücklich das gezielte Löschen von Daten und Dokumenten im Sinne der EU-DSGVO mit ein.

Die Folge: Die Altapplikationen können abgeschaltet werden, was zu operativen Einsparungen gegenüber ihrem Weiterbetrieb von bis zu 80 Prozent führt. Ausserdem reduziert sich der Aufwand für Migrationen auf neue Softwaregenerationen in der Regel um die Hälfte.



Der richtige Weg: Altsysteme abschalten und Altdaten auf JiVS auslagern



JiVS bringt massive Vorteile: Über 1000 Implementierungen weltweit sind der Beweis

Zeit gewinnen, Geld sparen, agil werden

Mit einer systemunabhängigen und rechtssicheren Plattform für Informationsmanagement wird die Unternehmens-IT insgesamt deutlich agiler und kann verschiedenste Geschäftsszenarien mit weit geringerem Aufwand unterstützen:

Beispiel Konsolidierung von Applikationslandschaften: Bei der Konsolidierung heterogener IT-Umgebungen handelt es sich nicht um ein rein technisches Projekt. Vielmehr verbinden die Unternehmen damit betriebswirtschaftliche und strategische Ziele. Dadurch sollen die Komplexität reduziert, der entsprechende Wartungs-, Administrations- und Kostenaufwand gesenkt, und Innovationen beschleunigt werden. So bietet die Konsolidierung weltweit verteilter Anwendungslandschaften die Möglichkeit, Änderungen und Weiterentwicklungen schneller zu implementieren und global bereitzustellen. Diese Ziele lassen sich jedoch nur erreichen, wenn die Altsysteme stillgelegt werden.

Beispiel Datenqualität: Ein Kunde, viele Datensätze und dazu noch unterschiedliche, so dass die Unternehmen von verschiedenen Kunden ausgehen statt von einem einzigen. Denn sie können bei Auswertungen keine Beziehung zwischen den Datensätzen feststellen. Das ist der heutige Stand in vielen Unternehmen. Daten im Detail zu analysieren ist aber geradezu die Voraussetzung für optimierte digitale Prozesse, neue digitale Produkte und Services. Wer keinen korrekten Überblick über die Kaufhistorie eines Kunden hat, wird ihn nicht mit den richtigen Angeboten und mit dem richtigen Mass an Personalisierung ansprechen. Kurz: Die Grundlage für digitale Geschäftsmodelle fehlt.

Beispiel Big Data: Neben der Datenqualität ist es das schiere Volumen, das bei Big-Data-Projekten eine Herausforderung darstellt. Reichen für die Überwachung von Parametern etwa aktuelle Sensordaten aus der Produktion aus, so lassen sich qualitative Erkenntnisse am besten dann gewinnen, wenn auch die Altdaten in die Analyse mit einbezogen werden. Dafür müssen sie aber vollumfänglich und einfach im Zugriff bleiben. Darüber hinaus setzen regelmässige Analysen voraus, dass selbst bei einem sehr hohen Datenvolumen aus operativen Daten historische werden. Folglich muss die Möglichkeit bestehen, dass für die Echtzeitüberwachung benötigte Daten nicht gelöscht, sondern aufbewahrt und Teil des Altdatenbestands werden – ohne die operativen Systeme zu belasten. Solche umfassenden Big-Data-Szenarien sind aber nur möglich, wenn die Altdaten in einer system- und applikationsunabhängigen sowie zentralen Umgebung aufbewahrt und vorgehalten werden.

Für die Zeit vor wie nach Migrationen: Systeme wachsen. Schon nach kurzer Zeit müssen die Speicherkapazität erweitert und die Rechenressourcen vergrössert werden, damit Anfragen von Fachanwendern gegen das System nicht spürbar zu Lasten der Performance gehen. Speziell für SAP-Bestandskunden kommt eine weitere Herausforderung hinzu. Denn ihre Bestandssysteme laufen in der Regel noch nicht auf der neuen Datenbank SAP HANA, sondern auf einem der gängigen relationalen DBMS-Systeme. In Zukunft aber müssen sie Lizenzen für SAP HANA erwerben, die zudem volumenabhängig sind. SAP-Bestandskunden haben daher ein starkes Interesse daran, ihre Datenbestände zu reduzieren, bevor sie auf die HANA-Datenbank migrieren.

Eine Plattform für den richtigen Ansatz

Agile Unternehmen brauchen eine agile Applikationslandschaft. Diese muss aber von den Stabilitätsanforderungen der Daten befreit sein. Genau dafür wurde die Java-basierende Plattform für Informationsmanagement JiVS entwickelt. Sie zeichnet sich dadurch aus, Daten aus abgeschalteten Altsystemen, aber auch die zugehörigen Dokumente in ihrem Geschäftskontext weiter rechtssicher vorzuhalten.

Die Kosten für den Betrieb von JiVS liegen dabei in der Regel um 80 Prozent unter denen für den Weiterbetrieb der Altsysteme. Zudem zeigt die Erfahrung aus über 1000 erfolgreichen JiVS-Projekten weltweit, dass sich das zu migrierende Datenvolumen im Allgemeinen um bis zu 80 Prozent senken lässt. Insgesamt können die Unternehmen ihren Aufwand für die Migration auf neue Softwaregenerationen in der Regel um 50 Prozent reduzieren, während sie 100-prozentigen Zugriff auf ihre Altdaten und -dokumente behalten – und das bei voller Rechtssicherheit.

JiVS ist damit das Kernelement einer agilen Applikationslandschaft in den Unternehmen: So sieht der richtige Ansatz aus, um den blinden Fleck in traditionellen IT-Umgebungen zu beseitigen.

Die inhaltliche Verantwortung für den Artikel liegt bei Data Migration Services AG.

WEITERE INFORMATIONEN

DATA MIGRATION SERVICES
Data Migration Services AG
Kontakt: Tobias Eberle
Tel.: 071 686 91 39
E-Mail: tobias.eberle@dms-global.com

In 3 Schritten zu sicheren Daten

So vermeidet Freeletics Datenlecks aus Public Clouds

Ihr Unternehmen kann es sich nicht leisten die Kontrolle zu verlieren – insbesondere, wenn es sich um sensible Daten handelt. Das Risiko von Datenlecks und Sicherungsausfällen erkannten auch die Geschäftsführer der Freeletics GmbH, die durch ihre Fitnessapp über grosse Mengen an hochsensiblen Kundeninformationen verfügen. Eine umfangreiche IT-Strategie musste her, um die Sicherheit der Kundendaten zu wahren. Mit den Lösungen von Synology funktionierte das in drei Schritten.

Schritt 1: Ein eigener Server für Handlungsfreiheit

Eine wichtige Vorgabe der Freeletics GmbH war, immer Herr über die eigenen Daten zu sein. Bei der Recherche nach einer eigenen All-in-One-Server-Lösung überzeugten sie die Synology Network Attached Storages (NAS) in punkto Sicherheit z. B. wegen der Ausfallsicherheit durch mehrere Festplatten im RAID, dem umfassenden Zugriffsrechtesystem, der unkomplizierten Wartung und Skalierbarkeit dank erweiterbarer Speicherkapazität ganz nach Unternehmens-, und Datenwachstum sowie wegen der strukturierten Datenverwaltung über ein einfaches Interface. Alltägliche Arbeitsabläufe laufen nun über die Synology RackStation RS3617xs+. So bestimmt das junge Unternehmen selbst über seine IT-Infrastruktur und agiert unabhängig von externen Hosts und fortlaufenden Lizenzkosten. Dabei widmet Freeletics der langfristigen Sicherung der Daten besondere Aufmerksamkeit. Ganz nach dem Motto «doppelt hält besser», zeigen Schritt 2 und 3, wie eine gute Backup-Strategie für die meisten Unternehmen aussieht.

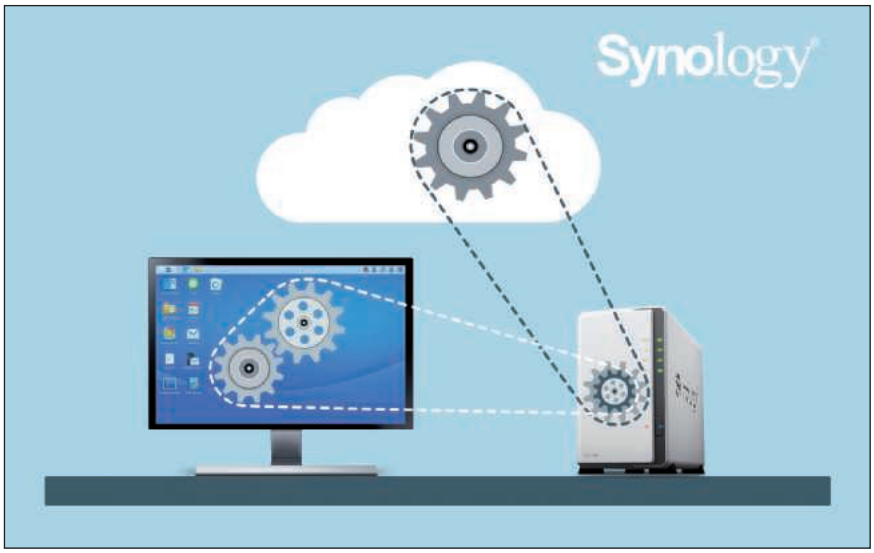
Schritt 2: Backup vor Ort

Automatisierte Datensicherungen laufen auf ein weiteres Synology NAS im Unternehmen. Da die kompletten Daten nun auch auf dem Backup-Server liegen, sind sie gegen einen eventuellen Ausfall des Hauptservers geschützt. So können auch Daten, die versehentlich gelöscht wurden, wiederhergestellt werden.

Schritt 3: Backup in die Cloud

Doch was passiert bei Feuer, Hochwasser oder bei einem Einbruch in die Serverräume? Für diese nicht ganz auszuschliessenden Fälle hat sich Freeletics für ein weiteres Backup ihrer Daten entschieden – und zwar standortunabhängig in eine Cloud.

An Cloud-Anbieter setzte Freeletics hohe Massstäbe: DSGVO Konformität, Speicher in deutschen Rechenzentren, Datenverschlüsselung, spezifische Zeitpläne für Sicherungen und eine grosse Speicherkapazität. Die meisten Cloud-Speicher-Lösungen erfüllen diese Anforderungen nicht vollständig. Doch gerade bei der Sicherung von Kundendaten wollte das Start-Up keine Kompromisse eingehen. Die passende Lösung fand das Unternehmen dann in der Synology C2. Die flexiblen C2 Backup-Lizenzmodelle bieten auch bei grossen Datenmengen, wie den über 35 TB von Freeletics, Lösungen an und verursachen bei der Wiederherstellung keine zusätzlichen Kosten. Für die Erstsicherung nutzte Freeletics den kostenlosen Synology Dienst, bei dem die Datenmengen auf einem Service-NAS verschlüsselt abgelegt, zum C2-Rechenzentrum in Frankfurt transportiert und eingespielt werden. So konnte die sonst langwierige und bandbreitenintensive Erstsicherung ganz unkompliziert vorgenommen werden.



Gegen Datenlecks aus Public Clouds: Auf Nummer sicher mit der Hybrid-Lösung

Public Clouds sind gängige, von Privatpersonen und Unternehmen eingesetzte, öffentlich zugängliche Dienste, um Daten standortunabhängig zu verwalten. Die Verfechter dieser Cloud-Dienste argumentieren oft mit der einfachen Handhabung und den niedrigen Kosten, doch ist das wirklich so?

Die häufig zunächst kostenlosen Clouds können schnell teuer werden, wenn mehr Speicherplatz benötigt wird. Ausserdem ist das Thema Datenschutz und IT-Sicherheit ein grosser Unsicherheitsfaktor. Da sich das Datenschutzrecht immer auf das Land bezieht, in dem sich das Rechenzentrum der Cloud befindet (oftmals in den USA), können Datenlecks in Form von fremden Zugriffen auftreten.

Um die Hoheit über Ihre Daten zu erlangen, bieten sich Private und Hybrid-Clouds, wie die Synology C2 an. So werden Ihre Daten verschlüsselt und DSGVO konform in einer Cloud mit Rechenzentrum in Deutschland abgelegt. Insbesondere die Anbindung an ein NAS ermöglicht, dass Sie auch ohne Internetverbindung immer auf Ihre Daten zugreifen können.

Die inhaltliche Verantwortung für den Artikel liegt bei Synology GmbH.

DER AUTOR

Dennis Schellhase ist seit 2011 Teil der Synology GmbH (Standort Düsseldorf) und seit 2016 in der leitenden Funktion als Head of DACH Market tätig