Cloud-Backup: Vor- und Nachteile im Überblick

Es gibt zahlreiche Vorteile, die sich durch ein Cloud-Backup erreichen lassen. Doch geht es bei der Wahl des geeigneten Cloud-Backups auch darum, die Nachteile zu berücksichtigen.

von

- Paul Kirvan
- Dave Raffo, Senior Analyst

Zuletzt aktualisiert: 06 Dez. 2024

Fast jedes Unternehmen nutzt Cloud-Services für unterschiedliche IT-Prozesse, darunter auch für Backup und Recovery. Da das Datenwachstum nach wie vor anhält, ist eine umfassende und zuverlässige Backup-Technologie wichtig, um eine optimale Sicherungsstrategie zu gewährleisten. Aufgrund günstiger Bandbreiten- und Skalierbarkeitstechnologien hat das Cloud-Backup in den vergangenen Jahren an Bedeutung gewonnen und kommt ebenso häufig zum Einsatz wie Festplatten, SSDs oder Tapes.

Das Backup geschäftskritischer Informationen wie Daten, Datenbanken, Anwendungen oder Dateien ist ein wichtiger Teil einer Disaster-Recovery-Strategie. Diese sorgt dafür, dass bei einem Störfall essenzielle Daten und Systeme schnell wiederhergestellt werden können, sei es auf den gleichen Primärsystemen oder auf anderen Umgebungen wie der Cloud.

Es gibt zahlreiche Cloud Service Provider, die entsprechende Dienste für das Backup anbieten. Meist wird dafür eine Public-Cloud-Umgebung genutzt, in einigen Fällen auch eine Hybrid Cloud. Zudem lässt sich mithilfe der Cloud-Anbieter auch eine Private Cloud am eigenen Standort einrichten. Zu den bekanntesten Cloud-Dienstleistern gehören AWS, Microsoft Azure, Google Cloud oder IBM Cloud. Darüber hinaus kann ein Cloud-Backup mithilfe von Drittanbietern für das Hosting und Management des Backups in dessen Cloud-Umgebung genutzt werden. Für Daten, die in SaaS-Anwendungen wie Salesforce und Microsoft 365 erstellt wurden, kommen zudem Cloud-to-Cloud-Backup in Frage.

Baclup-Services – wie auch generelles Cloud Computing – kann aus einer Kombination von internen und externen Ressourcen sein. Ein Szenario ist zum Beispiel die Verwendung eigener Soft- und Hardware am eigenen Standort, die dann durch Cloud-Ressourcen erweitert wird: ein Backup wird am eigenen Standort erstellt und vorgehalten, ein zweites in der Cloud.

Eine andere Möglichkeit ist die Nutzung der eigenen Software, um Daten direkt vom standorteigenen Server/Produktivsystem in einem Backup-Server in der Cloud zu sichern.

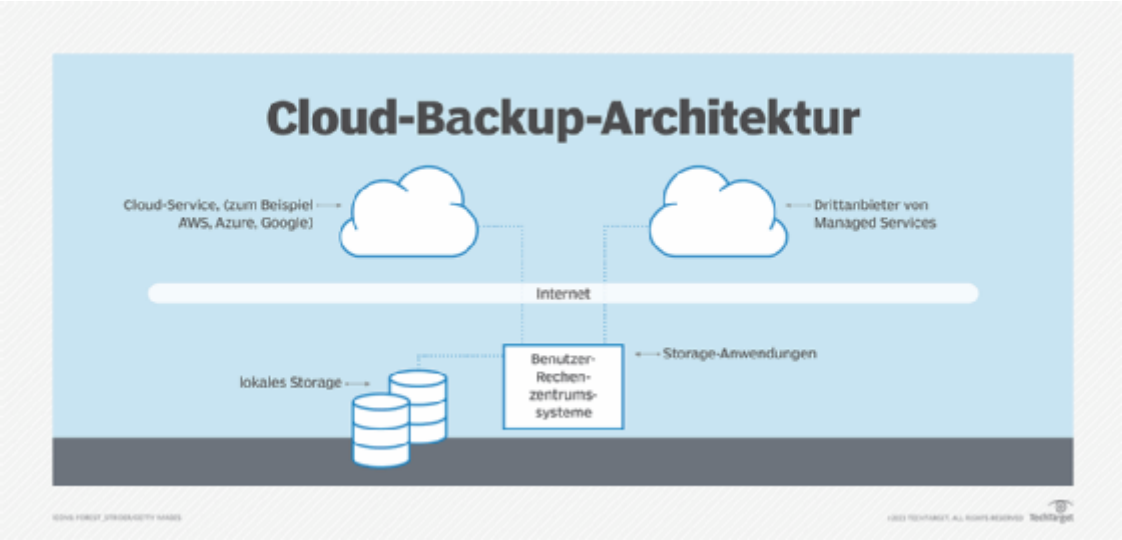


Abbildung 1: Es gibt verschiedene Architekturen für das Cloud-Backup, aus denen der IT-Verantwortliche wählen kann.

Die Abrechnung der Cloud-Backups basiert oft auf der real genutzen Speicherkapazität, wobei häufig ein Pay-As-You-Grow-Modell damit einhergeht, also die Option, automatisch den Speicherplatz zu skalieren und dementsprechend abgerechnet zu werden. Weitere Kostenfaktoren können der geografische Standort, Redundanzanforderungen, Datenvorhaltungszeiten, Netzwerkbandbreite und Anzahl der Nutzer sein. Oft fallen auch höhere beziehungsweise zusätzliche Kosten für das Zurückholen der Daten aus der Cloud an.

Vorteile des Cloud-Backups

Das Backup in der Cloud bietet mehrere Vorteile, darunter die folgenden:

- **Effizienz und Zuverlässigkeit.** Cloud-Anbieter nutzen modernste Technologien wie festplattenbasierte Sicherung, Datenkomprimierung, Verschlüsselung, Datendeduplizierung, Servervirtualisierung, Speichervirtualisierung und anwendungsspezifischen Schutz, die in SSAE-16-zertifizierten Rechenzentren nachgewiesen werden können. Zusätzlich zu der Sorgfaltspflicht, die mit ihrer Zertifizierung einhergeht, bieten viele Cloud-Anbieter eine 24/7-Überwachung, Verwaltung, Datensicherheit in vielen Formen, Data Protection, Berichterstattung und Unterstützung bei Disaster-Recovery-Aktivitäten. Darüber hinaus müssen sich die Nutzer keine Gedanken über Technologie-Upgrades, gespeicherte Datenmengen, Migrationen oder Veralterung machen, da sich der Dienstanbieter um alle Infrastrukturfragen kümmert.
- **Skalierbarkeit mit Kapitaleinsparungen.** Cloud-Backups können kostengünstig sein, insbesondere für Verbraucher und kleine Unternehmen, die keine großen Datenmengen zu schützen haben. Bei Public Clouds gibt es auch keine Probleme mit der Skalierbarkeit, so dass eine ausreichende Speicherkapazität selten ein Problem darstellt. Die Verwaltung von Cloud-Backups über einen Dienstanbieter ist einfacher, da der Anbieter die Verwaltung übernimmt. Die Verlagerung von Backups in die Cloud kann ein Air-Gap-Arrangement bieten, das geschäftskritische Daten und Systeme vor Cyberangriffen wie Phishing und Ransomware schützt, da die Dateien außerhalb des Unternehmens liegen.
- **Verbesserte Wiederherstellungszeit für kleine Datensätze.** Bei einer Wiederherstellung von einem Band müsste ein IT-Verantwortlicher das Band abrufen, laden, die Daten lokalisieren

und wiederherstellen. Die Wiederherstellung von Dateien aus einem Cloud-Speicher ist dagegen schneller; sie erfordert keinen physischen Transport vom externen Standort, keine Bandbearbeitung und keine Suchzeit. Die wiederherzustellenden Dateien können schnell lokalisiert und über eine Netzwerkverbindung heruntergeladen werden. Dies trägt dazu bei, die für die Wiederherstellung wichtiger Daten und Systeme benötigte Zeit zu verkürzen. Außerdem entfällt die Notwendigkeit eines lokalen Bandspeicher-Arrays. Der Erfolg dieser Methode hängt weitgehend davon ab, wie viel Bandbreite über eine WAN- oder Internetverbindung verfügbar ist.

- **Zugänglichkeit.** Cloud-Backup kann für Unternehmen attraktiv sein, die sich die Investition und Wartung einer separaten DR-Infrastruktur nicht leisten können. Sie kann auch für diejenigen interessant sein, die sich einen vollständigen DR-Standort leisten können, aber die größere Effizienz und die Kosteneinsparungen erkennen, die durch die Auslagerung von Datenressourcen erzielt werden können. Auf Datenkopien außerhalb des Standorts kann von praktisch jedem Gerät oder Standort mit Internetanschluss aus zugegriffen werden. Solche Ressourcen bieten zusätzliche Sicherheit und Data Protection im Falle einer Störung, beispielsweise bei einer regionalen Katastrophe.
- **Umfassenderer Schutz.** Auf der Grundlage der ermittelten Sicherungsanforderungen und der Häufigkeit der Datenabrufe können Cloud-Backups Edge-Geräte wie Laptops oder Tablets schützen, die nicht Teil einer standortspezifischen Backup-Installation sind. Cloud-Repositories können auf der Grundlage einer Kostenanalyse auch den Bedarf an Bandspeichern ersetzen oder ergänzen.
- **Verhinderung von Unterbrechungen durch Ausfälle des lokalen Speichers.** Bei einem Ausfall lokaler Speicher-Arrays können die in der Cloud gespeicherten Daten abgerufen werden, sobald die Geräte vor Ort wieder in Betrieb genommen wurden.
- **Datenkonsolidierung.** Dank der riesigen Speicherkapazitäten, die von Cloud-Anbietern zur Verfügung gestellt werden, können Nutzer ihre Speicherressourcen von mehreren Standorten aus lokal und global konsolidieren und so sicherstellen, dass eine Störung an einem beliebigen Ort nicht zum Stillstand des Unternehmens führt.

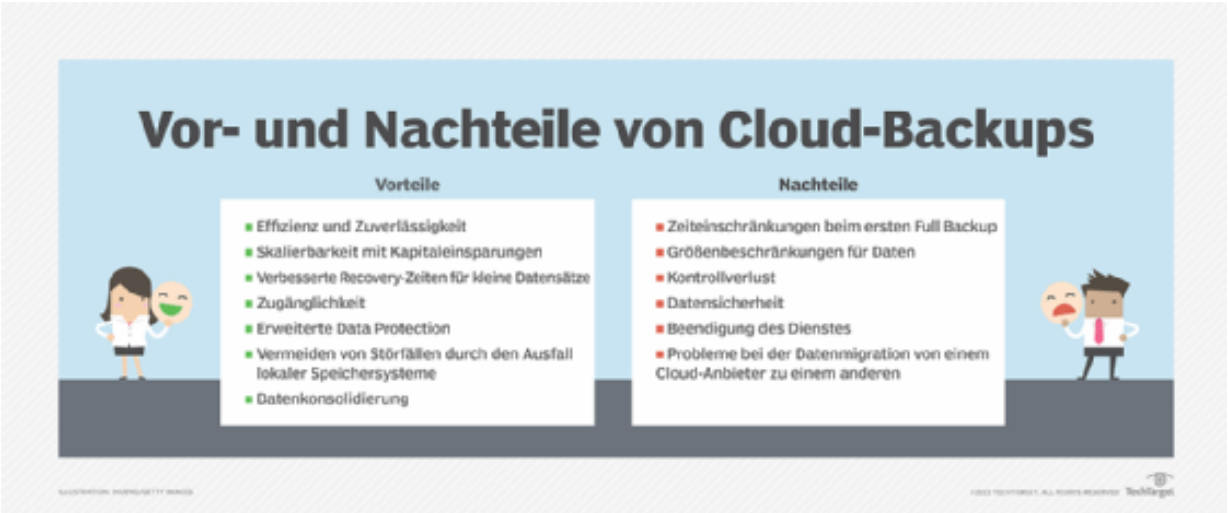


Abbildung 2: Die verschiedenen Vor- und Nachteile einer Cloud-Sicherung im Kurzüberblick.

Nachteile der Cloud-Sicherung

Es gibt auch Nachteile der Cloud-Sicherung, darunter die folgenden:

- **Zeitbeschränkungen bei der ersten vollständigen Sicherung.** Je nach der Gesamtkapazität der zu sichernden Daten könnte sich die erste vollständige Sicherung (Full Backup) und/oder vollständige Wiederherstellung von Daten am lokalen Standort als zu zeitaufwändig erweisen und Auswirkungen auf die Produktionssysteme haben. Es könnte notwendig sein, Erst- oder Vollsicherungen nach Feierabend oder an Wochenenden zu planen.
- **Größenbeschränkungen.** Je nach Bandbreitenverfügbarkeit haben Unternehmen möglicherweise einen Schwellenwert für die Datenmenge, die täglich in die Cloud gesendet werden kann. Diese Beschränkungen können sich auf Backup-Strategien auswirken, bei denen Daten und Anwendungen schnell abgerufen werden müssen. Die für Backups benötigte Bandbreite ist für große IT-Abteilungen oft ein großes Problem. Die Menge der zu sichernden Daten kann mit verschiedenen Methoden wie der Datendeduplizierung reduziert werden. Backup-Teams könnten sich dafür entscheiden, nur bestimmte Datensätze in ein Cloud-Repository zu verschieben, um Bandbreitenbeschränkungen zu kompensieren und Kosten zu senken.
- **Kontrollverlust.** Die Benutzer haben wenig bis gar keine Kontrolle über ihre Datenbestände, sobald diese in einen Cloud-Dienst verschoben wurden. Service Level Agreements (SLAs) sind ein geeignetes Mittel, um sicherzustellen, dass die Daten bei Bedarf verfügbar sind.
- **Datensicherheit.** Sobald die Daten ein Unternehmen verlassen und in einen Cloud-Dienst übertragen werden, hat der Benutzer keine Echtzeitkontrolle mehr über die Daten. Es ist Aufgabe des Benutzers, dafür zu sorgen, dass SLAs und andere Bestimmungen festgelegt und durchgesetzt werden, um sicherzustellen, dass der Cloud-Anbieter die Daten des Benutzers schützt.
- **Beendigung des Dienstes.** Genauso wichtig wie der Vergleich spezifischer Funktionen ist es, die beste Ausstiegsoptionen für einen Cloud-Dienst zu verstehen. Gebühren für die Beendigung oder den vorzeitigen Austritt, Kündigungsbenachrichtigung und Datenextraktion sind nur einige der Faktoren, die zu berücksichtigen sind. Bei großen Public-Cloud-Anbietern wie AWS, Azure und Google ist dies wahrscheinlich weniger ein Problem, bei kleineren MSPs und regionalen Cloud-Diensten hingegen schon.
- **Schwierige Migration zu einem anderen Anbieter.** Ähnlich wie bei der Beendigung einer Dienstvereinbarung können die Gebühren für die Datenübertragung von einem Cloud-Backup-Anbieter zu einem anderen die Gesamtkosten des Dienstes erhöhen.

Zusätzliche Erwägungen zur Cloud-Sicherung

Cloud-Sicherung bringt zusätzliche Überlegungen mit sich, die Unternehmen bei der Wahl ihrer Backup-Strategie berücksichtigen sollten. Wenn Unternehmen einen Vertrag für Cloud-Backup abschließen, entscheiden sie sich in der Regel für Backup as a Service (BaaS). Dieser Service beinhaltet die Migration von Daten zwischen dem Standort des Nutzers und dem Rechenzentrum des Cloud-Service-Anbieters (CSP). Um die Netzwerkbandbreite zu optimieren und Latenzzeiten zu reduzieren, werden die Sicherungsdaten vor der Übertragung an den CSP üblicherweise dedupliziert und komprimiert. Obwohl dies generell ein effizienter Prozess ist, können sich Herausforderungen ergeben, wenn die Daten abgerufen und wiederhergestellt werden müssen.

Eine der Hauptschwierigkeiten besteht darin, dass die deduplizierten Sicherungsdaten vor der Wiederherstellung für eine Anwendung rehydriert, also in ihr ursprüngliches Format und ihre ursprüngliche Dateistruktur zurückgeführt werden müssen. Dieser Prozess kann zeitaufwendig sein. Noch bedeutsamer ist jedoch die Zeit, die für das Herunterladen großer Datenmengen vom CSP zum

Anwender benötigt wird. Bei umfangreichen Datensätzen wie virtuellen Maschinen, Datenbanken oder Anwendungen kann dies erhebliche Zeit in Anspruch nehmen und möglicherweise mit den zuvor festgelegten Recovery Time Objectives (RTO) in Konflikt geraten.

Um diese Herausforderung zu bewältigen, bieten viele Anbieter Disaster Recovery as a Service (DRaaS) an. Eine Option im Rahmen dieses Angebots ist die Möglichkeit, kritische Geschäftsanwendungen als VM-Instanzen direkt in der Cloud des Anbieters auszuführen. Dies kann wertvolle Produktionszeit einsparen, erfordert jedoch vom Administrator sicherzustellen, dass die Anwendung in der Cloud-Umgebung des Anbieters ordnungsgemäß funktioniert.

In Disaster-Recovery-Situationen, in denen eine cloudbasierte Interims-Produktionsumgebung geschaffen wird, können zusätzliche Kosten entstehen. Diese können sich aus dem Bedarf an Hochgeschwindigkeits-Speicherressourcen oder ausreichender Netzwerkbandbreite ergeben, um Hunderte oder sogar Tausende gleichzeitiger Benutzersitzungen zu ermöglichen. In solchen Szenarien, in denen die Nutzer plötzlich stark vom CSP abhängig sind, können bisher unbekannte Variablen auftreten, die möglicherweise die Dienstqualität beeinträchtigen.

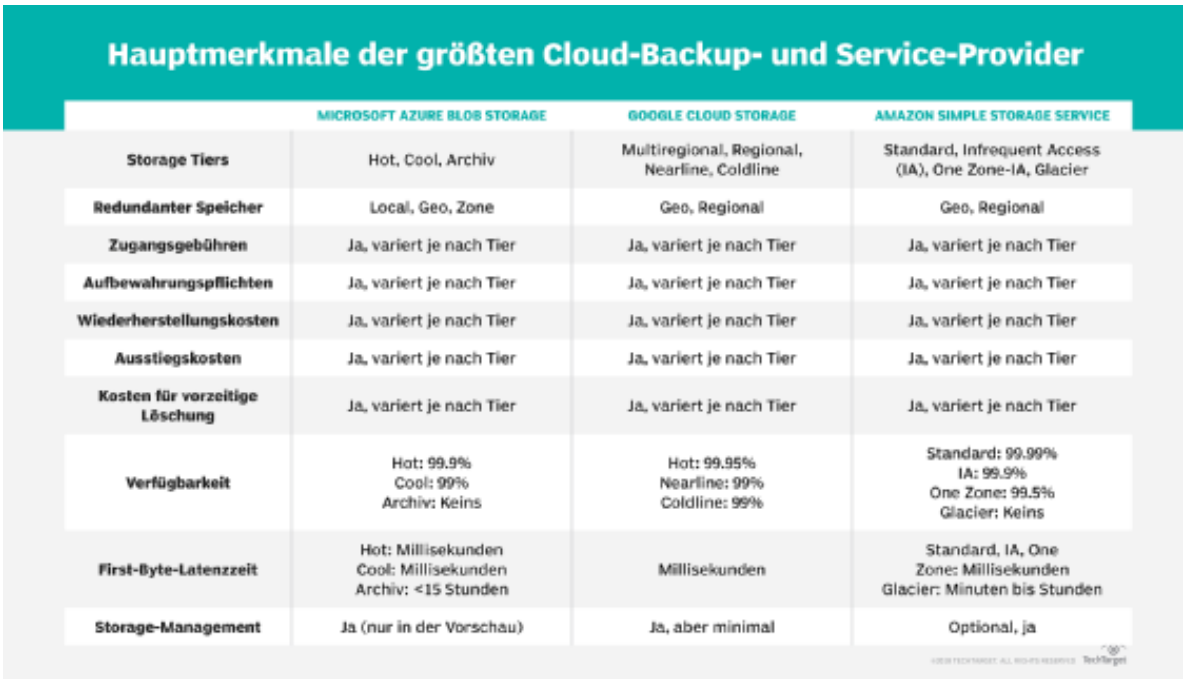
Zusammenfassend lässt sich sagen, dass Cloud-Backup-Lösungen zwar viele Vorteile bieten, aber auch sorgfältige Planung und Berücksichtigung potenzieller Herausforderungen erfordern. Unternehmen müssen die Vor- und Nachteile verschiedener Ansätze abwägen und sicherstellen, dass ihre gewählte Strategie sowohl ihre Sicherungsanforderungen erfüllt als auch im Falle einer notwendigen Wiederherstellung praktikabel und effizient ist.

Cloud-Backup-Anbieter

Es gibt eine Vielzahl von Cloud-Backup-Anbietern. Ein Admin muss diese Anbieter und ihre Serviceportfolio für Datensicherung genau unter die Lupe nehmen, bevor er mit der Planung und Umsetzung des Cloud-Backup beginnt. Im Folgenden finden Sie Beispiele für Fragen, die Sie bei der Bewertung von Anbietern stellen sollten:

- Bietet der Anbieter SLAs an?
- Wird der Anbieter seine SLAs an die Anforderungen der Benutzer anpassen?
- Welche verschiedenen Sicherungsmethoden unterstützt der Anbieter?
- Wie skalierbar sind die Speicherressourcen?
- Welche DR-Testdienste werden angeboten?
- Welche Netzwerkbandbreiten-Ressourcen werden vom Anbieter zur Verfügung gestellt?
- Erlauben die Anbieter den Benutzern, ihre Daten regelmäßig zu testen und zu überprüfen?
- Wie sieht die Gebührenstruktur des Anbieters aus, und welche unterschiedlichen Gebühren können vertraglich vereinbart werden?
- Wie verwaltet der Anbieter die Daten, Datenbanken und Anwendungen des Benutzers?
- Wie stellt der Anbieter sicher, dass die gesicherten Daten geschützt sind, zum Beispiel verschlüsselt?
- Welche Arten von Reports stellt der Anbieter den Nutzern zur Verfügung?
- Wie gewährleisten die Anbieter die Einhaltung von Vorschriften wie HIPAA und DSGVO?

Tabelle 1 vergleicht die führenden Cloud-Backup-Anbieter anhand mehrerer wichtiger Faktoren.



Hauptmerkmale der größten Cloud-Backup- und Service-Provider

	MICROSOFT AZURE BLOB STORAGE	GOOGLE CLOUD STORAGE	AMAZON SIMPLE STORAGE SERVICE
Storage Tiers	Hot, Cool, Archiv	Multiregional, Regional, Nearline, Coldline	Standard, Infrequent Access (IA), One Zone-IA, Glacier
Redundanter Speicher	Local, Geo, Zone	Geo, Regional	Geo, Regional
Zugangsgebühren	Ja, variert je nach Tier	Ja, variert je nach Tier	Ja, variert je nach Tier
Aufbewahrungspflichten	Ja, variert je nach Tier	Ja, variert je nach Tier	Ja, variert je nach Tier
Wiederherstellungskosten	Ja, variert je nach Tier	Ja, variert je nach Tier	Ja, variert je nach Tier
Ausstiegskosten	Ja, variert je nach Tier	Ja, variert je nach Tier	Ja, variert je nach Tier
Kosten für vorzeitige Löschung	Ja, variert je nach Tier	Ja, variert je nach Tier	Ja, variert je nach Tier
Verfügbarkeit	Hot: 99.9% Cool: 99% Archiv: Keins	Hot: 99.95% Nearline: 99% Coldline: 99%	Standard: 99.99% IA: 99.9% One Zone: 99.5% Glacier: Keins
First-Byte-Latenzzeit	Hot: Millisekunden Cool: Millisekunden Archiv: <15 Stunden	Millisekunden	Standard, IA, One Zone: Millisekunden Glacier: Minuten bis Stunden
Storage-Management	Ja (nur in der Vorschau)	Ja, aber minimal	Optional, ja

Abbildung 3: Die drei bekanntesten Cloud-Backup-Anbieter im Schnellvergleich.

Neben den drei bekanntesten CSP – Amazon, Microsoft und Google – stehen zahlreiche andere Cloud-Backup-Angebote zur Verfügung. Zu den bekanntesten gehören unter anderem:

- Acronis Cyber Backup Cloudarcserve ist ein hybrides Cloud BaaS-Produkt.
- Arcserve bietet Unified Data Protection, die Cloud Direct DR und Backup umfasst.
- Asigra verfügt über Cloud-Backup-Funktionen wie eine Software, die verhindert, dass Ransomware Backups beeinträchtigt.
- Backblaze offeriert sowohl Cloud-Backup als auch Cloud-Speicher an.
- Carbonite stellt benutzerfreundliche Datensicherung für Verbraucher, KMUs und Unternehmen zur Verfügung.
- Druva stellt die Data Resiliency Cloud als SaaS-Plattform für Datensicherung, DR und Cyber Resilience bereit.
- IDrive hat eine breite Palette an Cloud-Backup-Diensten.
- Unitrends Cloud Backup ist eine DRaaS-Ressource.
- Veeam Software bietet eine Reihe von Cloud-Backup-Diensten, darunter Veeam Backup & Replication.

Die Nutzung der Cloud-Technologie für Backup-Zwecke erfreut sich großer Beliebtheit, und die vielen verfügbaren Optionen machen sie zu einer wichtigen Wahl für die meisten Unternehmen – unabhängig von ihrer Größe – sowie für einzelne Benutzer. Die vielen Optionen bedeuten auch, dass potenzielle Benutzer ihre Hausaufgaben machen, Angebote und Preisstrukturen sowie die Verfügbarkeit von SLAs vergleichen müssen, um eine fundierte Entscheidung zu treffen.