BayCIX

veeam Insights

Der Status von Hybrid- und Multi-Cloud-Umgebungen 2024

Ein Research Brief aus dem
2024 Data Protection Trends Report

Inhaltsverzeichnis

Einführung

Jedes Jahr führen unabhängige Marktforschungsunternehmen Umfragen unter IT-Verantwortlichen und -Implementierungsexperten durch, die für die Datensicherungsstrategien ihrer Unternehmen zuständig sind. Diese jährlichen Umfragen sollen vor allem Aufschluss darüber geben, welche Strategien die Unternehmen in Bezug auf Hybrid- und Multi-Cloud-Architekturen verfolgen, während ihre IT-Teams versuchen, die Geschäftsprozesse zu unterstützen. Während in den ersten Monaten nach der Corona-Pandemie die Einführung der Cloud deutlich beschleunigt wurde, zeigt sich in den darauffolgenden vier Jahren eine relativ konsistente Verteilung der Workloads auf Rechenzentren, Private Clouds und mehrere Public Clouds.

Für 2024 wird laut Angaben der Unternehmen fast die Hälfte ihrer produktiven Workloads in einer Public Cloud ausgeführt. Der Rest verteilt sich zu gleichen Teilen auf physische Server und virtuelle Maschinen in ihren Rechenzentren.

Was in der IT-Landschaft der letzten Jahrzehnte nicht zu beobachten war, ist die Vielfalt der bevorzugten „Goldstandard"-Produktionsplattformen. Früher beruhten erstklassige Rechenzentren fast ausschließlich auf Novell NetWare- oder Windows Server-Infrastrukturen. Später wurden diese von virtualisierten Infrastrukturen von VMware, Hyper-V und anderen Hypervisoren überholt. Bei diesen vergangenen Generationen waren echte Migrationen von der bisherigen bevorzugten Plattform zu der neuen Plattform nicht ungewöhnlich. Dabei wurde eine einzelne erstklassige Datensicherungslösung gewählt, die für die neue Plattform (z. B. Veeam für VMware) und die zahllosen Clouds geeignet war.

Wie hoch schätzen Sie den prozentualen Anteil von Servern in den folgenden Formaten an der Infrastruktur Ihres Unternehmens im Jahr 2024?

27% Virtuelle Maschinen im Rechenzentrum

28% Physische Server im Rechenzentrum

45% In der Cloud gehostete Serverinstanzen bei einem „Hyperscaler" oder Serviceprovider (MSP)

Zwar stellen Rechenzentren auch 2024 weiterhin wichtige IT-Services für Unternehmen jeder Größe bereit, auch Folgendes ist jedoch keine Seltenheit:

- Nutzung von Azure, AWS, Google und anderen Infrastruktur-Clouds
- Nutzung spezieller Infrastrukturservices für Dateifreigaben oder Datenbanken
- Neben der Nutzung gängiger SaaS-Plattformen wie Microsoft 365 oder Salesforce

Bei so viel Begeisterung für Cloud-Services liegt die Vermutung nahe, dass das moderne Rechenzentrum an Bedeutung verliert. Dies ist jedoch nicht richtig. Die Daten deuten vielmehr darauf hin, dass die meisten Unternehmen eine „Cloud-Smart-Strategie" verfolgen. Dabei werden für neue Workloads standardmäßig in der Cloud gehostete Workloads in Betracht gezogen, was den Prozentsatz der weiter vom Rechenzentrum bereitgestellten IT-Services reduziert, ohne dass diese Workloads tatsächlich aus den physischen Einrichtungen migriert werden.

Zudem spielen immer häufiger Geschäftsprozesse und wirtschaftliche Erwägungen eine Rolle bei der Entscheidung, welche Workloads lokal oder extern gehostet werden. Selbst innerhalb einer Cloud kann nicht davon ausgegangen werden, dass der „Weg in die Cloud" nur in eine Richtung oder zu einem einzigen Serviceprovider führt. Stattdessen bietet die Anforderung, Workloads fließend zwischen Rechenzentren und Clouds, zwischen Clouds und wieder zurück verschieben zu können, sowohl Chancen als auch Herausforderungen.

Dieser Research Brief enthält Daten und Erkenntnisse für drei wichtige Stakeholder, die vor der Aufgabe stehen, eine „Cloud Smart"-Strategie für ihre Unternehmen umzusetzen:

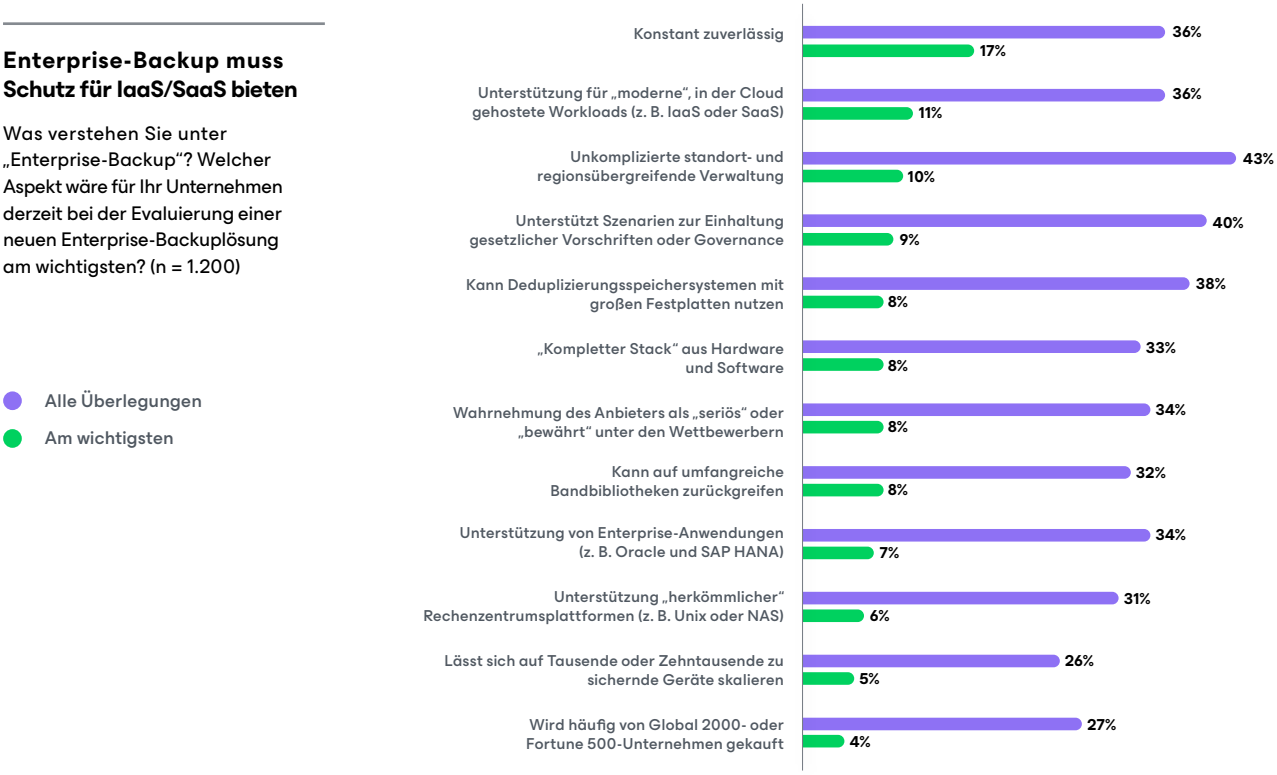
- **Führungskräfte,** die für die IT-Bereitstellung in ihren Unternehmen verantwortlich sind
- **Experten für die Implementierung von IT-Architekturen**, die Cloud-Services nutzen
- **Backup-Experten**, die für die lokale und externe Datensicherung von Unternehmensressourcen zuständig sind

„Enterprise“-Backups müssen IaaS/SaaS schützen

Laut 1.200 großen Unternehmen sind die beiden wichtigsten Funktionalitäten ihrer nächsten Datensicherungslösung „höhere Zuverlässigkeit“ und „besserer Schutz von in der Cloud gehosteten Workloads“.

Enterprise-Backup muss Schutz für IaaS/SaaS bieten

Was verstehen Sie unter „Enterprise-Backup“? Welcher Aspekt wäre für Ihr Unternehmen derzeit bei der Evaluierung einer neuen Enterprise-Backuplösung am wichtigsten? (n = 1.200)



Der Schutz von „Enterprise“-Anwendungen (z. B. Oracle) und „traditionellen“ Rechenzentrumsplattformen (z. B. NAS) taucht zwar immer noch in der Liste auf, beide Punkte haben jedoch eine weitaus geringere Priorität, was vermutlich darauf zurückzuführen ist, dass die Unternehmen bereits über herkömmliche Backuplösungen für diese herkömmlichen Plattformen verfügen. Werden hingegen mit herkömmlichen Backupmethoden moderne Workloads (z. B. Clouds) gesichert, sinkt logischerweise die Zuverlässigkeit der Sicherung und Wiederherstellung. Es überrascht daher nicht, dass „Zuverlässigkeit“ und „Schutz der Cloud“ beide als wichtigste Triebkräfte für Veränderungen genannt werden.

IT-Verantwortliche profitieren dank der Möglichkeit, neben Rechenzentrumskomponenten eine in der Cloud gehostete Infrastruktur zu nutzen, von betrieblicher Agilität und wirtschaftlicher Effizienz, da sie ihre IT-Services auf der bzw. den für den jeweiligen Workload am besten geeigneten Plattform(en) bereitstellen können.

Hybridarchitekten müssen darauf achten, dass ihre Teams bei der Modernisierung der Produktionsstrategien auch die Datensicherung modernisieren, damit geschäftskritische Workloads, die bisher im Rechenzentrum *gut geschützt* waren, nicht plötzlich in der Cloud *unzureichend oder überhaupt nicht geschützt* sind.

Für Datensicherungsexperten besteht die Herausforderung darin, entweder die auf das Rechenzentrum ausgerichtete standardmäßige Backuplösung durch verschiedene in der Cloud gehostete Dienstprogramme zu ergänzen (z. B. bietet jede Produktionscloud einen Copy-Job, einen Papierkorb oder einen integrierten Snapshot) oder eine moderne Backup-Plattform zu wählen, die nicht nur herkömmliche Workloads, sondern auch gängige Clouds schützen kann. Bei Letzterem gilt es zusätzlich, Konsistenz zu gewährleisten, da Workloads bei veränderten geschäftlichen Anforderungen fließend zwischen Clouds migriert werden können.

Moderne Datensicherung muss mehr bieten als nur Cyberresilienz

Die Modernisierung der Datensicherung sollte vor allem auf den Schutz vor der allgegenwärtigen und fast unvermeidlichen Bedrohung durch Ransomware ausgerichtet sein. Es wäre jedoch ein großer Fehler, für die Datensicherungsstrategie nur diese Bedrohung zu berücksichtigen, auch wenn sie stets gegenwärtig ist. Laut neuesten Studien waren Cyberangriffe zwar die häufigste und folgenreichste Ursache für IT-Ausfälle — 40% aller Unternehmen waren davon betroffen —, aber die meisten anderen Krisen, die sich schon immer auf IT- und Geschäftsprozesse ausgewirkt haben, bestehen nach wie vor:

37%

waren von Ausfällen aufgrund von **Infrastrukturproblemen** betroffen

34%

waren aufgrund von Problemen mit **der Anwendungssoftware** von Ausfällen betroffen

33%

waren von Ausfällen aufgrund von **menschlichen Fehlern** betroffen (z. B. Löschen, Überschreiben usw.)

32%

erlitten Ausfälle aufgrund von Problemen mit **dem** Betriebssystem

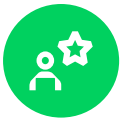
31%

waren von Ausfällen aufgrund der **Nichtverfügbarkeit der Public Cloud betroffen**

29%

waren von Ausfällen aufgrund von **Naturkatastrophen** (z. B. Brand, Überschwemmung, Unwetter usw.) betroffen

Es sei daran erinnert, dass fast keine dieser Ursachen durch die Nutzung cloudbasierter Ressourcen im Vergleich zu den eigenen Rechenzentren gemindert werden können. Für in der Cloud gehostete Workloads gelten nicht nur dieselben Anforderungen an Backups, sondern auch an die Disaster Recovery. Zwar könnten Cloud-Services die durch physischen Speicher oder Serverkomponenten verursachten Fehler verringern, alle anderen Argumente für ein modernes Datensicherungskonzept für Rechenzentren sollten jedoch auch für Hybrid- und Public-Cloud-Umgebungen gelten.



Für IT-Verantwortliche, zu denen sowohl der Chief Information Officer als auch der Chief Information Security Officer gehören, müssen die Disaster-Recovery-Strategien von Unternehmen, die bereits erhebliche IT-Ausfälle umfassen, nun um Cyberangriffe und Probleme beim Zugriff auf Public Clouds als einen Teil der *Vorbereitung ausgeweitet werden.*

Für Hybridarchitekten, zu denen sowohl IT-Architekten als auch sicherheitsorientierte Ingenieure zählen, unterscheidet sich die für die Bereitstellung von in der Cloud gehosteten Services erforderliche Verschmelzung der Fachgebiete von den spezialisierten Rollen eines Sicherheitsspezialisten für Zugriffskontrolle und Prävention/Erkennung, eines IT-Betriebsspezialisten und/oder eines Spezialisten für Infrastruktur, Virtualisierung, Server usw. Zwar ermöglicht diese Verschmelzung den Benutzern unter Umständen eine nahtlosere Nutzung der IT-Services, sie macht es jedoch noch schwieriger, diese Ressourcen vor den zahllosen oben genannten Ursachen für Ausfälle zu schützen.

Für Datensicherungsexperten bedeutet die Erkenntnis, dass Daten Daten sind, unabhängig davon, ob sie von Servern oder Services bereitgestellt werden, dass eine universelle Herangehensweise an die Datensicherung erforderlich ist. In diesem Fall müssen *die zu schützenden Komponenten* neben den gängigen SaaS-Anwendungen auch die in der Cloud gehostete Infrastruktur (IaaS) sowie Plattformen wie in der Cloud gehostete Dateien und Datenbanken umfassen.

Unternehmen suchen nach einer modernen, cloudbasierten Datensicherung

Auf die Frage, was für eine „moderne“ Datensicherung am wichtigsten ist, nennen viele Unternehmen mindestens eine cloudbasierte Funktionalität:

39%
möchten von einer großen Cloud in eine andere wechseln (z. B. von Amazon zu Azure)

38%
wünschen sich einen konsistenten Schutz für lokale und IaaS/SaaS-Workloads

37%
möchten ihre Datensicherungslösung nutzen, um lokale Workloads in eine Cloud zu migrieren

27%
möchten eine Cloud-Infrastruktur als Disaster-Recovery-Standort nutzen

Einige dieser Funktionalitäten sind speziell auf allgemeine IT-Anforderungen abgestimmt:

Für IT-Verantwortliche stehen alle vier Funktionalitäten im Einklang mit dem Wunsch nach Flexibilität für das Unternehmen bei der Entscheidung, ob und welche Clouds zur IT-Bereitstellung für die Geschäftsbereiche genutzt werden sollen. Der oberste Punkt ist wohl der wichtigste, da Unternehmen mit der Frage kämpfen, welche Hypervisoren sie in ihren Rechenzentren verwenden und mit welchen Clouds sie diese ergänzen sollen. Zwar bietet fast jede große Plattform ein Dienstprogramm zur Migration von Workloads zu ihrer eigenen Technologie, doch nur selten — wenn überhaupt — bieten sie ein Dienstprogramm zur anderweitigen Verlagerung der Workloads. Daher überrascht es nicht, dass IT-Führungskräfte diese Fähigkeit als Attribut moderner Datensicherung am höchsten bewerten.

Für Hybridarchitekten, deren Teams unzählige Wochenenden damit verbracht haben, Workloads von Servern zu Hypervisoren, zu alternativen Hypervisoren und jetzt in die Cloud(s) zu migrieren, ist der erste Schritt immer ein gutes Backup und dann eine erfolgreiche Testwiederherstellung. Andererseits ist es verständlich, dass IT-Implementierungsexperten in der diesjährigen Studie das Potenzial der einfachen „Wiederherstellung“ des Backups in der neuen Cloud — auch als Migration bezeichnet — erkannt haben. Nicht nur das Backup wird „getestet“, sondern die ursprüngliche Umgebung bleibt auch unberührt, falls die Migration abgebrochen wird.

Für Datensicherungsexperten gilt Folgendes: Aufbauend auf den für Hybridarchitekten beschriebenen anerkannten Vorteilen müssen die Mitarbeiter, die für die Datensicherung und die Nutzung der oben beschriebenen Funktionalitäten verantwortlich sind, sicherstellen, dass die Datensicherungslösung des Unternehmens das diversifizierte Rechenzentrum und Cloud-Standardservices schützen kann sowie Serverinstanzen, die auf einem bestimmten Hypervisor oder in einer bestimmten Cloud gesichert wurden, in die Konstrukte „transformieren“ kann, die für die Wiederherstellung dieser Serverinstanzen auf einem anderen Hypervisor oder Cloud-Host benötigt werden (z. B. Amazon zu Azure, VMware zu Hyper-V, VMware zu Azure usw.).

So bewirken diese Überlegungen Veränderungen

Angesichts des Potenzials an Agilität und Effektivität, das sich aus einer „Cloud Smart"-Strategie ergibt, ist die Begeisterung für Hybrid- und Multi-Cloud-Umgebungen zu Recht groß. Doch ohne moderne Datensicherungsfunktionalitäten, die speziell für die zahllosen Clouds moderner Unternehmen entwickelt wurden, werden viele Initiativen für die Digital Transformation und IT-Modernisierung scheitern. Daher überrascht es nicht, dass 92% der Unternehmen ihre Datensicherungsbudgets für 2024 um durchschnittlich 6,6% aufgestockt haben — ein bemerkenswerter Anstieg angesichts der von IDC prognostizierten Erhöhung des gesamten IT-Budgets um nur 3,5%. Anders ausgedrückt: Während die IT insgesamt ein etwas höheres Budget erhält, werden die unverhältnismäßig gestiegenen Investitionen in die Datensicherung wahrscheinlich zu Lasten anderer, weniger priorisierter IT-Initiativen gehen.

Für den IT-Verantwortlichen, der wahrscheinlich auch für die Budgetplanung verantwortlich war, ist dies ein Zeichen der Entschlossenheit, alle Daten des Unternehmens sowohl in den Rechenzentren als auch in den Clouds zu schützen.

Hybridarchitekten sind sich der Notwendigkeit einer ganzheitlichen Datensicherung nach dem Motto „Bei einer Modernisierung der Produktion muss auch die Datensicherung modernisiert werden" bewusst.

Für Datensicherungsexperten, die diese Ergebnisse verantwortlich sind, dürfte es keine Überraschung sein, dass 54% der Unternehmen beabsichtigen, im Laufe des Jahres 2024 zu einer anderen primären Backuplösung zu wechseln. Manche Unternehmen ergänzen ihre herkömmliche Backuplösung für Rechenzentren dabei möglicherweise mit einer anderen gängigen Backuplösung, mit der zahllose Cloud-Umgebungen geschützt werden können. Dies könnte jedoch der Katalysator dafür sein, dass sie erkennen, dass der „Aufwand für die Umstellung" ihrer traditionellen Backuplösung durch den „Aufwand für die Ausführung mehrerer einzelner Produkte für die einzelnen Cloud-Services" problemlos aufgewogen wird.

Dieser Research Brief basiert auf der Befragung von 1.200 unabhängigen IT-Verantwortlichen und -Implementierungsexperten, die für die Datensicherungsstrategien ihrer Unternehmen verantwortlich sind. Die Umfrage wurde Ende 2023 durchgeführt und im Januar 2024 veröffentlicht. Die Daten wurden von Analysten kuratiert und eingeschätzt, die zuvor für ESG und Gartner tätig gewesen waren und zusammen auf 70 Jahre Erfahrung im Bereich der Datensicherung zurückblicken.

Klicken Sie hier, um den vollständigen Data Protection Trends Report für 2024 herunterzuladen.

Jason Buffington
@JBuff
VP, Market Strategy
Veeam Software

Dave Russell
@BackupDave
VP, Enterprise Strategy
Veeam Software

Über Veeam Software

Veeam, weltweit marktführender Anbieter von Lösungen für die Datensicherung und die Wiederherstellung nach Ransomware-Angriffen, hat es sich zum Ziel gesetzt, Unternehmen in die Lage zu versetzen, durch Datensicherheit, Datenwiederherstellung und Datenfreiheit für ihre Hybrid Cloud maximale Ausfallsicherheit zu erreichen. Mit der Veeam Data Platform haben IT- und Sicherheitsverantwortliche die Gewissheit, dass ihre Anwendungen und Daten stets geschützt und verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und betreibt Niederlassungen in über 30 Ländern. Weltweit hat das Unternehmen mehr als 450.000 Kunden, die auf Veeam vertrauen, um ihren Geschäftsbetrieb aufrechtzuerhalten. Profitieren Sie mit Veeam von maximaler Ausfallsicherheit. Erfahren Sie mehr unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.