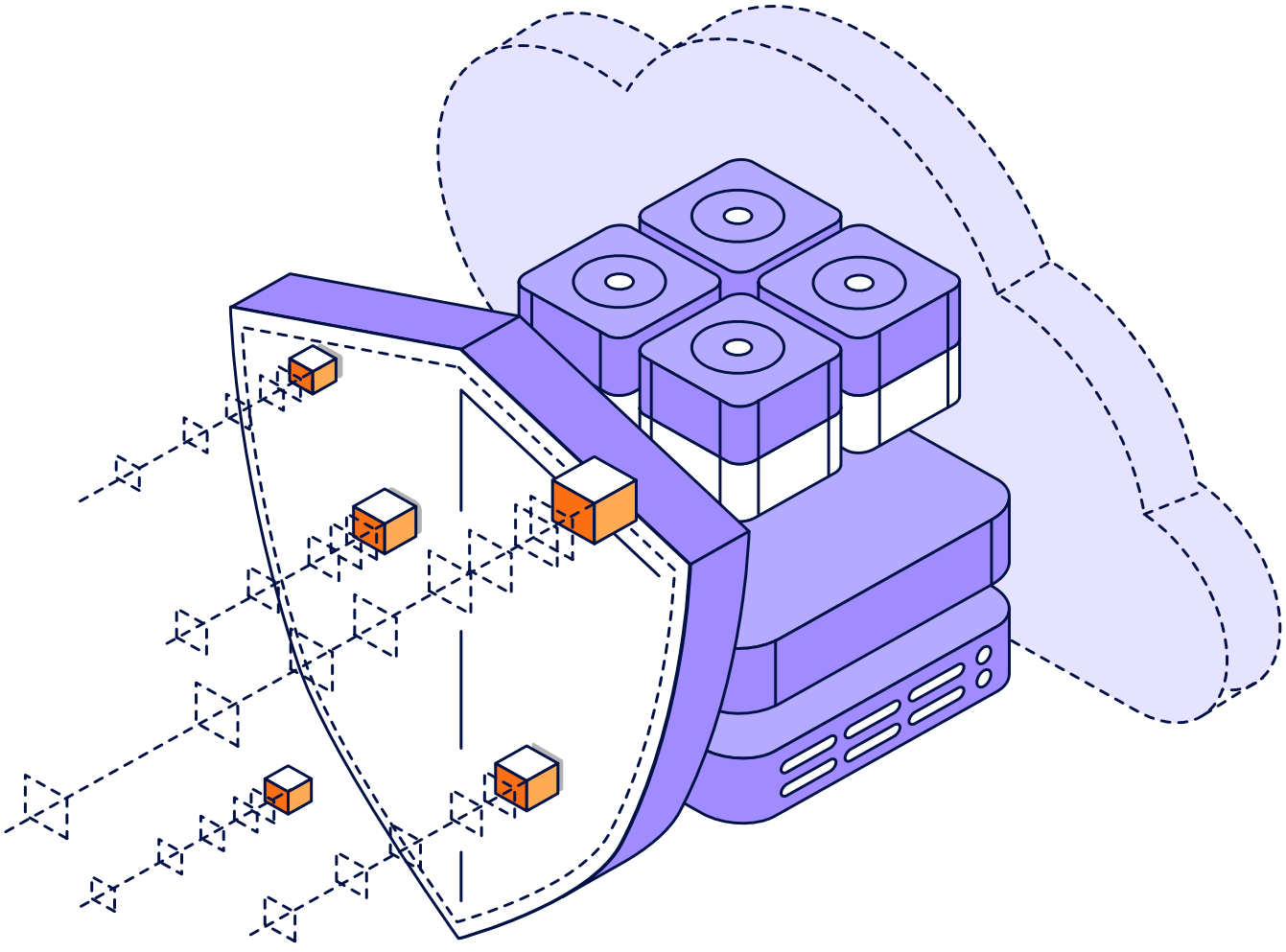
Cyberresilienz für die Hybrid Cloud

Erkenntnisse von mehr als 7.000 IT- und Sicherheitsexperten



In den letzten Jahren hat sich im Hinblick auf die Datenspeicherung ein fortdauernder Wandel vollzogen: Die rein lokale Speicherung im Rechenzentrum wich zunächst einem schrittweisen ***Cloud-Ansatz für einzelne Services***, gefolgt von ***Cloud-First-Strategien*** und ***umfassenden Hybrid-Modellen***, und mittlerweile nutzen die meisten Unternehmen ***strategische Multi-Cloud-Umgebungen*** als Standardbereitstellungsmodell für moderne IT. Die Frage, die Unternehmen 2024 beschäftigen wird, lautet nicht, ob und welche cloudbasierten Services sie verwenden werden. Vielmehr geht es darum, wie viele Clouds erforderlich sind und wie die IT-Teams deren Verwaltung stemmen soll – zusätzlich zu all den anderen Aufgaben wie Cybersicherheit, Datensicherung und kritischen IT-Kontrollen.

Um eine Antwort auf diese Fragen zu finden, haben wir für diesen Research Brief drei unabhängige Befragungen aus dem Zeitraum August 2022 bis März 2023 ausgewertet:

- **Cloud-Datensicherungstrends 2023**
  Befragung von 1.700 IaaS-, PaaS- und SaaS-Administratoren zu ihren Datensicherungsstrategien
- **Report „Datensicherungstrends 2023“**
  Befragung von 4.200 IT-Führungskräften mit Zuständigkeit für die Datensicherungsstrategien ihrer Unternehmen
- **Ransomware Trends Report 2023**
  Befragung von 1.200 CISO-/SecPro-/Backup-Experten, deren Unternehmen 2022 Cyberangriffe erlitten

Alle drei Befragungen wurden von unvoreingenommenen Analysten in unabhängigen Forschungseinrichtungen durchgeführt, die Daten anschließend von Veeam® erworben und in verschiedener Form veröffentlicht. Dieser Report beleuchtet vier wesentliche Aspekte:

- Cloudbasierte Services sind der Schlüssel für den Schutz von Rechenzentren und in der Cloud gehosteten Workloads.
- Clouds sind genauso anfällig für Ransomware-Angriffe wie andere Umgebungen, vielleicht sogar anfälliger.
- Eine Cloud lässt sich effektiv mit einer anderen Cloud schützen, aber nicht mit sich selbst.
- Die für Sicherheit, Disaster Recovery und Clouds zuständigen Teams sind nicht aufeinander abgestimmt – dieses Problem hat höchste Priorität!

Cloudbasierte Services sind der Schlüssel für den Schutz von Rechenzentren und in der Cloud gehosteten Workloads

82%

der Unternehmen verwenden jetzt cloudbasierten Storage mit Immutability-Funktionalitäten.

Untersuchungen zeigen übereinstimmend, dass cloudbasierte Services beim Schutz interner ebenso wie cloudbasierter Workloads unverzichtbar sind. *Vor allem ermöglichen sie* ***„überlebensfähige" Repositories*** *(z. B. Unveränderlichkeit bzw. Immutability) und* ***Disaster-Recovery-Infrastruktur*** *im Bedarfsfall.*

Die meisten Unternehmen vertrauen beim Schutz vor Ransomware-Angriffen auf zwei Erkenntnisse, die beinahe universale Gültigkeit haben:

- Wer Server in Rechenzentren schützen will, muss Daten außerhalb (z. B. an einem externen Standort oder in der Cloud) speichern.
- Für die Wiederherstellung nach einem Ransomware-Angriff werden gegen Cyberbedrohungen immune Backup-Kopien benötigt.

Untersuchungen zu Ransomware-Trends 2023 zeigen, dass diese beiden Grundsätze heutzutage weithin anerkannt sind: **82%** der Unternehmen bewahren unveränderliche Kopien in einer Cloud-Umgebung auf.

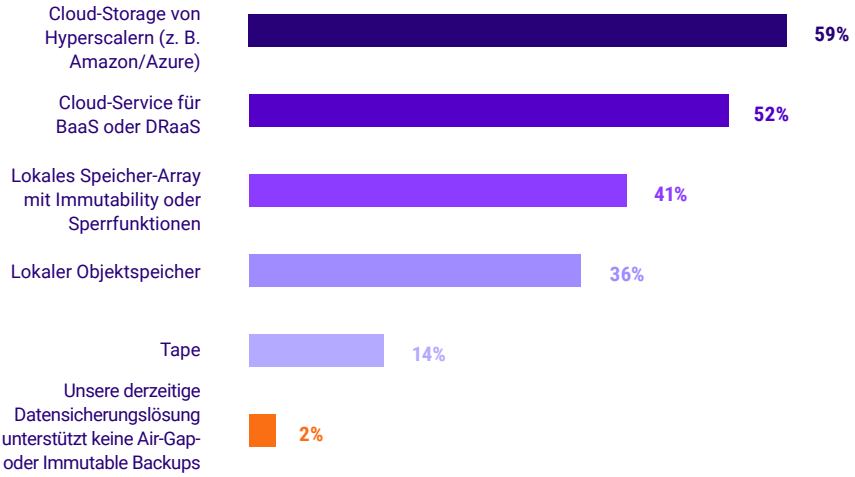


Abbildung 1.1

Nutzt Ihre Organisation bei der Nutzung der folgenden Systeme Offline-, durch ein Air-Gap getrennte oder unveränderliche Backups?

Hat ein Unternehmen für überlebensfähige Backup-Kopien gesorgt, können weitere Aspekte herkömmlicher Business-Continuity- oder Disaster-Recovery-Strategien (BC-/DR-Strategien) hinzugezogen werden. Cyberangriffe gelten heute zunehmend als einer von vielen Notfällen – wenn auch als besonderer –, woraus ganz logisch folgt, dass Cyberresilienz und Disaster Recovery als in engem Zusammenhang stehend gesehen werden. So oder so drängt sich unmittelbar die Frage auf: **„In welche Umgebung soll die Wiederherstellung oder das Failover erfolgen?"**

Unternehmen haben aus Cyberangriffen gelernt, dass zu einer umfassenden Wiederherstellungsstrategie die Fähigkeit gehört, die Server ihrer Rechenzentren nach einem Ransomware-Angriff oder sonstigen Katastrophenszenario in einer cloudbasierten Infrastruktur wiederherzustellen.

Abbildung 1.2

Wohin haben Sie Ihre Daten nach einem Ransomware-Angriff auf Ihre Server wiederhergestellt?

Die oben genannten Daten zeigen, dass die meisten Unternehmen eine hybride Strategie verfolgen, die je nach Ausmaß des Vorfalls flexible Optionen bietet. **71%** der Unternehmen können Daten mittels einer Cloud-Lösung, **81%** mittels lokaler Infrastruktur wiederherstellen – die große Schnittmenge verweist auf ein hohes Maß an Flexibilität. In Vorbereitung auf verschiedenste Katastrophenszenarien im Rahmen ihrer Disaster-Recovery-Pläne sehen **54%** der Unternehmen alternative Standorte für Failovers vor und **46% cloudbasierte Infrastruktur als DR-Standort**. Dabei gibt es mehrere Möglichkeiten, cloudgestützte Disaster-Recovery-Standorte bereitzustellen.

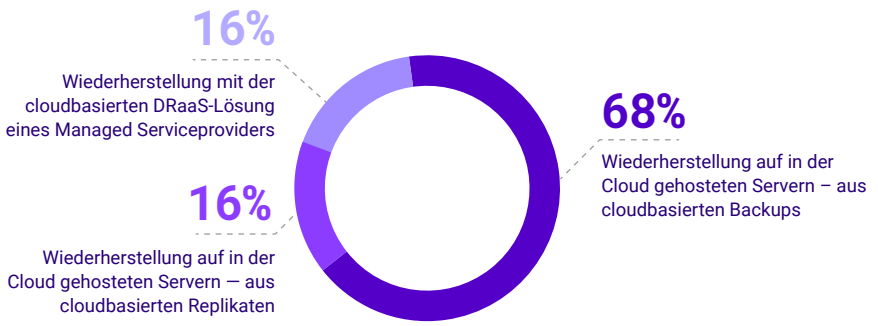


Abbildung 1.3

Wie erfolgt die Wiederaufnahme des Betriebs bei der Nutzung von Cloud-Services für die Disaster Recovery?

Unabhängig davon, ob ihr Disaster-Recovery-Plan einen Disaster-Recovery-as-a-Service-Provider (DRaaS-Provider) oder eine selbst verwaltete cloudbasierte Infrastruktur wie Amazon Web Services oder Microsoft Azure vorsieht, müssen mindestens zwei kritische Anforderungen erfüllt sein:

- Die Fähigkeit, eine Backup-Datei während der Wiederherstellung zu transformieren, z. B. durch Wiederherstellung und Bereitstellung eines ursprünglich physischen oder virtuellen Produktionsservers in einer Cloud-Host-Umgebung.
- Die Fähigkeit, den Wiederherstellungsprozess zu orchestrieren, einschließlich Quarantäne zur Malware-Erkennung während des Wiederherstellungs-Workflows.

Allerdings sind nur

- **18 %** der Unternehmen in der Lage, Skripte für orchestrierte Workflows zur Failover-Wiederherstellung zu erstellen und auszuführen.
- **44 %** verwenden einen isolierten Testbereich – also eine Sandbox – für die Malware-Erkennung während der Wiederherstellung, um zu verhindern, dass ihre Umgebung erneut infiziert wird.

Die Geschäftsführung jedes Unternehmens sollte sich damit auseinandersetzen, ob die vorhandene – interne oder externe – Lösung zur Datensicherung eine automatische Wiederherstellung im großen Stil zulässt und/oder eine sichere Wiederherstellung garantiert.

Clouds sind genauso anfällig für Ransomware-Angriffe wie andere Umgebungen, vielleicht sogar anfälliger

Nachforschungen haben ergeben, dass **cloudbasierte Workloads von Cyberangriffen im selben Maße betroffen sind wie andere Umgebungen**. *Der Grund dafür ist vermutlich, dass cloudbasierte Services in hybriden IT-Architekturen nahtlos verfügbar sind. Da viele Unternehmen für den Schutz ihrer Cloud-Services vor unbefugten Zugriffen andere Sicherheitstechnologien einsetzen müssen als für die Daten im Rechenzentrum, sind sogar zusätzliche Angriffsmöglichkeiten denkbar, z. B. die Trennung der Verbindung zwischen Anwendern und Cloud-Plattformen.*

So wie Unternehmen einst erkennen mussten, dass die Cloud nicht nur im Kommen, sondern längst da ist, müssen sie heute zur Kenntnis nehmen, dass die Außerbetriebnahme lokaler Plattformen hinter der Bereitstellung neuer Workloads in cloudbasierten Services hinterherhinkt. IT-Strategien werden also immer hybrider und zugleich gewinnen in der Cloud gehostete Infrastrukturen an Boden.

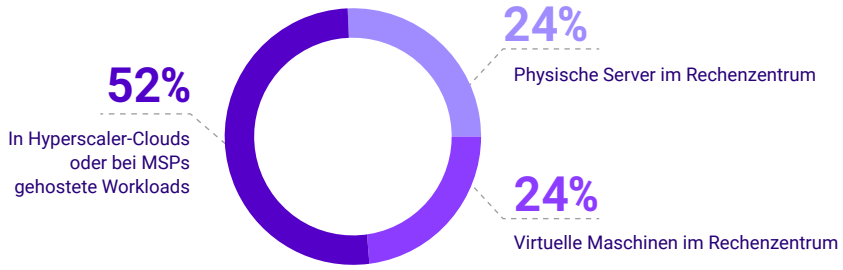


Abbildung 2.1

Prognose: „hybride" Verteilung von Plattformen für Produktionsserver 2024.[6]

Im Gegensatz zur Entwicklung von Plattformen in klassischen Rechenzentrumsumgebungen gibt es – unabhängig vom Cloud-Anbieter – nicht nur eine einzige Cloud-Architektur, die bereitgestellt, verwendet und geschützt werden muss. Vielmehr existieren unzählige solcher Architekturen von verschiedenen Providern, deren Managementansätze sich auch noch wesentlich unterscheiden können.

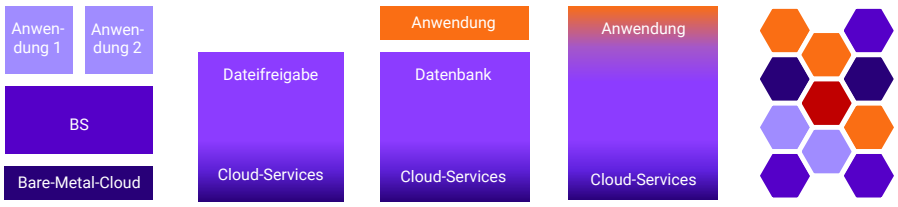


Abbildung 2.2

Unzählige Cloud-Architekturen

Obwohl cloudbasierte Services oft als resilient betrachtet werden, kommt es leider dennoch zu Ausfällen. Gründe dafür sind Probleme beim Cloud-Serviceprovider, von Administratoren fehlkonfigurierte Cloud-Services oder fehlerhafte Verbindungen zwischen Anwendern und Cloud-Services. Laut Untersuchung nahmen Ausfälle durch Cyberangriffe von 2021 bis 2022 zu. In beiden Jahren waren Cyberangriffe sogar die Ursache für den schwerwiegendsten Ausfall überhaupt – ohne Aussicht auf Besserung 2023.[7]

- **48 %** der Unternehmen waren infolge von **„nicht verfügbaren Public-Cloud-Ressourcen“** von Unterbrechungen ihres IT-Betriebs betroffen.
- **52 %** der Unternehmen waren infolge von **„Infrastruktur- oder Netzwerkausfällen“** von Unterbrechungen ihres IT-Betriebs betroffen.
- **53 %** der Unternehmen waren infolge von **„Cybersicherheitsvorfällen“** von Unterbrechungen ihres IT-Betriebs betroffen.

Die Befragung von 1.200 Opfern von Cyberangriffen ergab, dass cloudbasierte Daten fast ebenso oft von Verschlüsselung oder anderen Folgen betroffen waren wie lokale Daten im Rechenzentrum.

Bei den meisten Cyberangriffen ist der erste Eindringversuch mehr oder weniger Glückssache (z. B. hoffen Phisher, dass irgendjemand auf einen infizierten Link in einer E-Mail klickt). Sind die Angreifer aber erst einmal im System, nutzen sie bekannte Schwachstellen oder potenzielle Sicherheitslücken in beliebten IT-Plattformen gezielt aus. Der Ransomware Trends Report 2023 zeigt, dass es **Cyberkriminelle bei 38 % der Angriffe auf cloudbasierte Workloads abgesehen hatten.**[8]

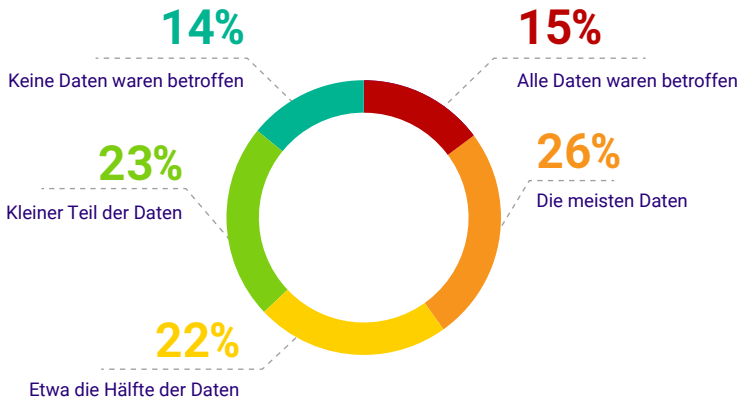


Abbildung 2.3

Anteil der in Cloud-Plattformen gehosteten Daten, die vom letzten Ransomware-Angriff betroffen waren, in %.[9]

Aus der Tatsache, dass die Infektionsraten bei allen Daten unabhängig vom Speicherort – Rechenzentrum, Zweigstelle / externer Standort oder Cloud – vergleichbar hoch sind, lassen sich zwei wichtige Schlüsse ziehen:

- Da hybride IT-Umgebungen nahtlos ineinandergreifen, können Cyberkriminelle nach dem Eindringen in die Umgebung eines Opfers genauso leicht auf cloudbasierte Daten zugreifen wie auf Anwendungen und Dateien im physischen Rechenzentrum.
- Aus diesem Grund müssen in der Cloud gehostete Dateien, Datenbanken und Anwendungen ebenso streng geschützt werden wie lokale Workloads.

2024 ist erstmals damit zu rechnen, dass mehr Workloads außerhalb selbst verwalteter physischer Rechenzentren ausgeführt werden als innerhalb.

Eine Cloud lässt sich effektiv mit einer anderen Cloud schützen, aber nicht mit sich selbst

2 : 1

Zahlenverhältnis zwischen „traditionellen" IT-Backup-Teams und Cloud-Administratoren, die Datensicherungsaufgaben übernehmen

Alle drei Untersuchungen befassten sich mit der Frage, wer 2023 für die Sicherung von Cloud-Daten zuständig war und wie diese Daten geschützt wurden. Das Ergebnis: ***Das „Kernteam" (oder der Serviceprovider), das die restlichen lokalen Daten eines Unternehmens schützt, ist meist auch mit dem Schutz der Cloud-Daten betraut****. Viel Ungewissheit besteht noch, inwieweit es typisch ist, dass Unternehmen die integrierten Tools einer Plattform für die einzige Option halten, anstatt auf eine heterogene Enterprise-Lösung für Backups zu setzen.*

Doch bevor wir uns mit dem „Wie" befassen, lohnt ein Blick darauf, wer für den Schutz cloudbasierter Workloads zuständig ist. Hier ergibt sich ein recht einheitliches Bild: In etwa 2/3 der Fälle obliegt die Datensicherung dem „traditionellen" IT-Backup-Team, nur in 1/3 der Fälle den Cloud-Administratoren.

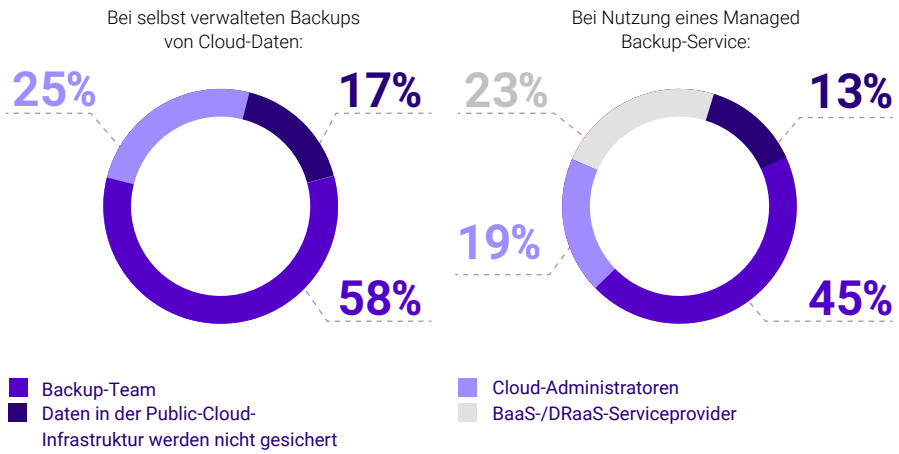


Abbildung 3.1

Wer ist in Ihrem Unternehmen im Allgemeinen für das Management von Backups / die Datensicherung von in der Cloud gehosteten Servern verantwortlich?[10]

Überraschend ist, dass **13%** angeben, ihr Unternehmen sichere cloudbasierte Infrastrukturen überhaupt nicht. Für viele Unternehmen, die einen hybriden Ansatz verfolgen, schließt daran die Erkenntnis an, dass sich Cloud-Backups in derselben Cloud, in einer anderen Region, in einer anderen Cloud oder sogar an einem lokalen Standort befinden können.
Diese Einsicht spielt bei der Wahl einer Backup-Lösung für cloudbasierte Workloads eine entscheidende Rolle:

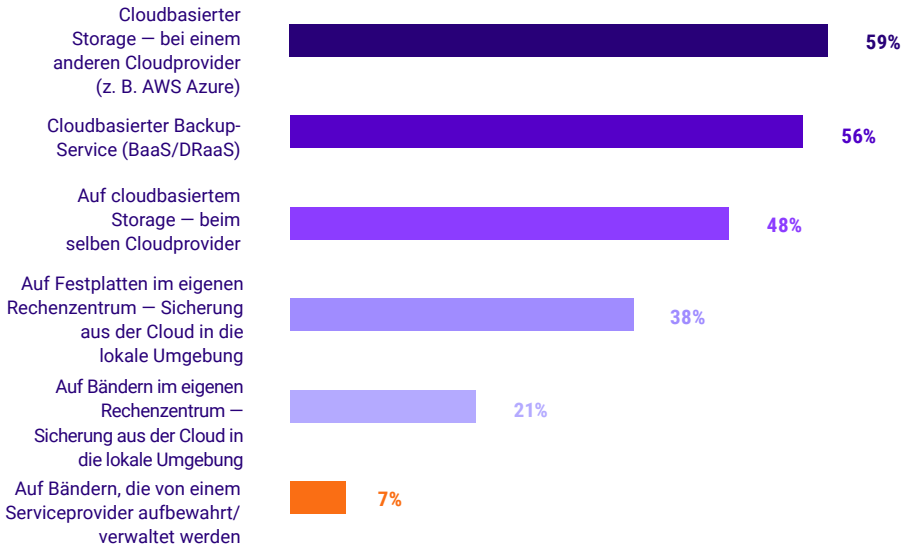


Abbildung 3.2

Wo speichern Sie Backups von Cloud-Daten, die Sie mindestens ein Jahr aufbewahren?[11]

- **37%** der IT-Führungskräfte betrachten die „Fähigkeit, Workloads zwischen Clouds zu verschieben", als wesentliches Merkmal einer „modernen" oder „innovativen" Datensicherungslösung.[12]
- **88%** der Unternehmen haben bereits Workloads aus einer Cloud-Umgebung in eine lokale Umgebung zurückverlagert oder in eine andere Cloud-Umgebung verschoben.[13]

Bei der Wahl einer Backup-Lösung für cloudbasierte Workloads besteht natürlich auch die Option, einfach die integrierten Tools oder die Exportfunktion zu nutzen, die viele Cloud-Provider für einzelne Workloads anbieten. Wer sich dafür entscheidet, dem ist oft nicht bewusst, dass für den

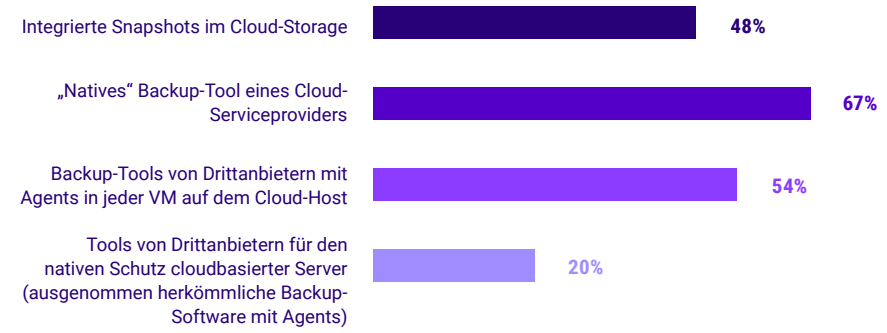


Abbildung 3.3

Welche Mechanismen zur Sicherung von in der Cloud gehosteten Daten sind Ihnen bekannt (unabhängig davon, ob Sie sie derzeit nutzen)?

umfassenden Schutz von Cloud-Workloads auch Tools von Drittanbietern zur Verfügung stehen.[14]

Falls Sie Snapshots in Erwägung ziehen, sollten Sie sich fragen, ob Sie sich ausschließlich auf Snapshots Ihrer lokalen Dateiserver verlassen würden. Snapshots sind nützliche Tools für die Wiederherstellung beinahe aktueller Kopien, wobei die Wiederherstellung unter Umständen sofort erfolgen kann. Dennoch sind Snapshorts kein vollwertiger Ersatz für Backups, aus folgenden Gründen:

- Infektionsrisiko durch identische Speicherumgebung (mit IaaS-Storage-Stack verbundener Standalone-NAS, einschließlich gemeinsamer Anmeldedaten)
- Langfristig hohe Betriebskosten, weshalb die meisten Unternehmen Snapshots nur für wenige Tage aufbewahren, aber Backups über Wochen, Monate und Jahre

Sollten Sie native workloadorientierte oder integrierte Tools in Erwägung ziehen, prüfen Sie, ob Ihre lokalen Plattformen mit einer der folgenden Methoden geschützt werden:

- Nur ZDLRA (oder RMAN) zum Schutz von **Oracle**-Datenbanken
- Nur NT Backup-Tool (oder System-Tool) zur Sicherung von **Windows-Servern**
- Nur VDPA zur Sicherung von **VMware**-Hosts
- Nur ASB zur Sicherung von **Microsoft 365**

Fragen Sie sich dann, wie viele Tools Ihr IT-Backup-Team verwalten möchte und wie hoch Ihr Storage-Budget ist – bedenken Sie dabei, dass jedes dieser Tools verschiedene Repositories und Formate nutzt. Noch dazu sind Snapshot- und andere plattformgebundene (d. h. integrierte) Tools in der Regel dafür gedacht, nach Fehlern in der jüngsten Vergangenheit (z. B. überschriebene Daten oder Importfehler) ein Quick Rollback vorzunehmen. Dementsprechend kurz sind die avisierten Aufbewahrungszeiten, was solche Tools noch problematischer macht. Für die Wiederherstellung nach einem Angriff mit Ransomware, die womöglich schon wochenlang im System schlummert, sind diese taktischen Tools jedenfalls unzureichend (oder ausgesprochen kostspielig). Diese Überlegungen werden durch folgende Untersuchungsergebnisse erhärtet:

- **35%** der IT-Führungskräfte betrachten den **„standardisierten Schutz von lokalen und IaaS-/SaaS-Umgebungen“** als wesentliches Merkmal einer „modernen“ oder „innovativen“ Datensicherungslösung.[15]
- **42%** der Unternehmen sind der Ansicht, dass **„Schutzfunktionen für cloudbasierte Workloads“** bei Enterprise-Datensicherungslösungen ein absolutes Muss sind.[16] Diese Überlegung war 2023 sowohl die häufigste als auch die wichtigste Antwort.

35%

der IT-Führungskräfte betrachten den „standardisierten Schutz von lokalen und IaaS-/SaaS-Umgebungen“ als wesentliches Merkmal einer „modernen“ oder „innovativen“ Datensicherungslösung.

Die für Sicherheit, Disaster Recovery und Clouds zuständigen Teams sind nicht aufeinander abgestimmt – dieses Problem hat höchste Priorität!

In allen drei Untersuchungen wurden Personen in unterschiedlichen Rollen befragt, darunter IT-Führungskräfte mit Zuständigkeit für die Datensicherung, CISOs und ähnliche leitende Entscheidungsträger, Sicherheitsexperten, IaaS-/PaaS-/SaaS-Administratoren und Anwender von Backup-Tools. Jedes Mal kam heraus, dass Kernfunktionen nie in den Händen eines einziges Teams lagen. Anders gesagt, es gab immer überlappende Aktivitäten und Zuständigkeiten. Trotzdem waren nur die wenigsten der Befragten davon überzeugt, ***dass ihre Teams hinsichtlich des strategischen Vorgehens und/oder der Implementierung und Anwendung von Technologien gut aufeinander abgestimmt waren.***

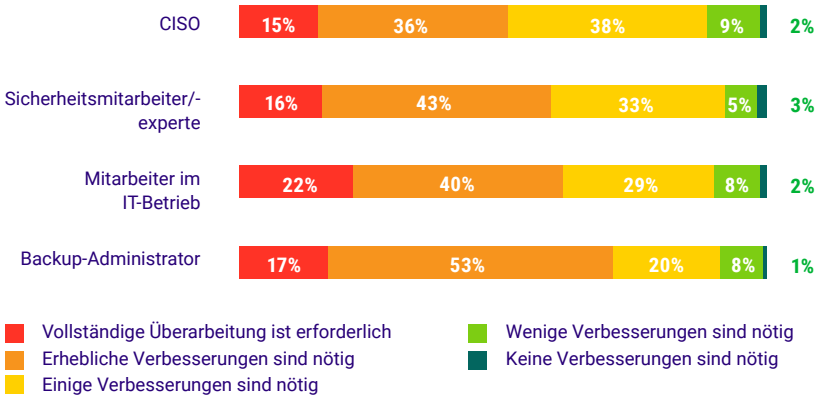


Abbildung 4.1

In welchem Umfang sind Verbesserungen nötig, um die IT-Backup-Teams und die Cybersicherheits-Teams in Ihrem Unternehmen vollständig aufeinander abzustimmen?

Die meisten Untersuchungen beschäftigen sich zwar schwerpunktmäßig mit den Gründen und Strategien, die die Technologiewahl beeinflussen, aber die Befragungsergebnisse zeigen auch, dass die Koordination zwischen den beteiligten Rollen sehr zu wünschen übrig lässt.[17]

Von den vier Rollen, die im **Ransomware Trends Report 2023** beleuchtet wurden, äußerten sich diejenigen, die am „nächsten" an der Behebung von Vorfällen dran waren (z. B. Backup-Administratoren gegenüber CISOs), am unzufriedensten über die teamübergreifende Zusammenarbeit und Abstimmung.

Ähnliche Abstimmungsprobleme zeigten sich zwischen SaaS- und Backup-Administratoren bei der Begründung und Wahl der Tools zum Schutz von Microsoft 365-Daten sowie zwischen IaaS-/PaaS- und Backup-Administratoren hinsichtlich der Strategien und Tools zum Schutz cloudbasierter Server, Dateifreigaben und Datenbanken.

Wichtige Fragen

Aus den Untersuchungen, für die über einen Zeitraum von acht Monaten mehr als 7.000 Personen befragt wurden, lassen sich einige wichtige Fragen ableiten, die für Ihre Cyberresilienz-Strategie relevant sein können:

- Sind alle Backup-Dateien unveränderlich und werden sie extern gespeichert? Werden die Backup-Dateien von einem erfahrenen Serviceprovider oder selbst verwaltet?
- Ist es möglich, eine Cloud-Infrastruktur als Disaster-Recovery-Standort zu nutzen? Falls nicht, was ist der Grund dafür?
- Werden alle cloudbasierten Daten, einschließlich IaaS-, PaaS- und SaaS-Workloads, gesichert? Falls ja, werden für jede Cloud separate Tools verwendet oder werden Tools übergreifend für alle Clouds (und lokalen Workloads) bereitgestellt?
- Wie gut ist die Teamkoordination hinsichtlich der Sicherung von lokalen, IaaS-, PaaS- und SaaS-Workloads?
- Wie gut ist die Teamkoordination hinsichtlich Cyberschutz und Daten-Backups?
- Wann wurde die Wiederherstellung cloudbasierter Daten zum letzten Mal getestet?
- Wann wurde die umfassende Wiederherstellung eines Rechenzentrums zum letzten Mal getestet?
- Wann wurden die Cyber- und BC-/DR-Playbooks zum letzten Mal geprüft und aktualisiert?

Wenn Sie Fragen zu den Untersuchungsergebnissen und deren praktischer Relevanz haben, wenden Sie sich bitte an StrategicResearch@veeam.com.

Die in diesem Research Brief zitierten Reports können Sie unter folgenden Links abrufen:

- **Cloud-Datensicherungstrends 2023**
  Befragung von 1.700 IaaS-, PaaS- und SaaS-Administratoren zu ihren Datensicherungsstrategien
- **Report „Datensicherungstrends 2023“**
  Befragung von 4.200 IT-Führungskräften mit Zuständigkeit für die Datensicherungsstrategien ihrer Unternehmen
- **Ransomware Trends Report 2023**
  Befragung von 1.200 CISO-/SecPro-/Backup-Experten, deren Unternehmen 2022 Cyberangriffe erlitten

Die Einschätzung von Veeam

Die Plattform von Veeam für Datensicherung und -management

Unternehmen müssen heute mehr denn je darauf vertrauen können, dass ihre Daten zuverlässig geschützt und jederzeit verfügbar sind – in lokalen Umgebungen ebenso wie am Edge oder in der Cloud. Veeam bietet eine zentrale Plattform für cloudbasierte, virtuelle, physische, SaaS- und Kubernetes-Umgebungen. Unsere Kunden können sich darauf verlassen, dass ihre Anwendungen und Daten vor Ransomware und anderen Katastrophen geschützt bleiben und stets verfügbar sind – dank einer unkomplizierten, flexiblen, zuverlässigen und leistungsstarken Plattform.

Mit Veeam steht Kunden ein kompetenter Partner zur Seite, der sie bei der schnellen Umsetzung ihrer digitalen Transformation, beim Schutz vor Cyberkriminalität und bei der Gewährleistung eines stabilen Geschäftsbetriebs unterstützt. Mit unseren Lösungen sind Ihre Daten umfassend geschützt und jederzeit verfügbar. Profitieren Sie mit der #1 Backup- und Recovery-Lösung von niedrigeren Kosten, weniger Komplexität und geschäftlichem Erfolg.

Weitere Informationen finden Sie unter **https://www.veeam.com/de**.

Unter **http://vee.am/hybridcloudinquiry** können Sie einen Beratungstermin mit einem Hybrid-Cloud-Experten von Veeam anfordern.

Bei Fragen zu den Umfrageergebnissen senden Sie bitte eine E-Mail an StrategicResearch@veeam.com.

1 Ransomware Trends Report 2023, Frage 29
2 Ransomware Trends Report 2023, Frage 25
3 Datensicherungstrends 2023, Frage 45
4 Datensicherungstrends 2023, Frage 46
5 Ransomware Trends Report 2023, Frage 21
6 Datensicherungstrends 2023, Frage 2
7 Datensicherungstrends 2023, Fragen 13 und 14
8 Ransomware Trends Report 2023, Frage 9
9 Ransomware Trends Report 2023, Frage 6
10 Datensicherungstrends 2023, Frage 17
11 Cloud-Datensicherungstrends 2023, Frage 8
12 Datensicherungstrends 2023, Frage 17
13 Datensicherungstrends 2023, Frage 4
14 Cloud-Datensicherungstrends 2023, Frage 35
15 Ransomware Trends Report 2023, Frage 17
16 Datensicherungstrends 2023, Frage 4
17 Ransomware Trends Report 2023, Frage 1