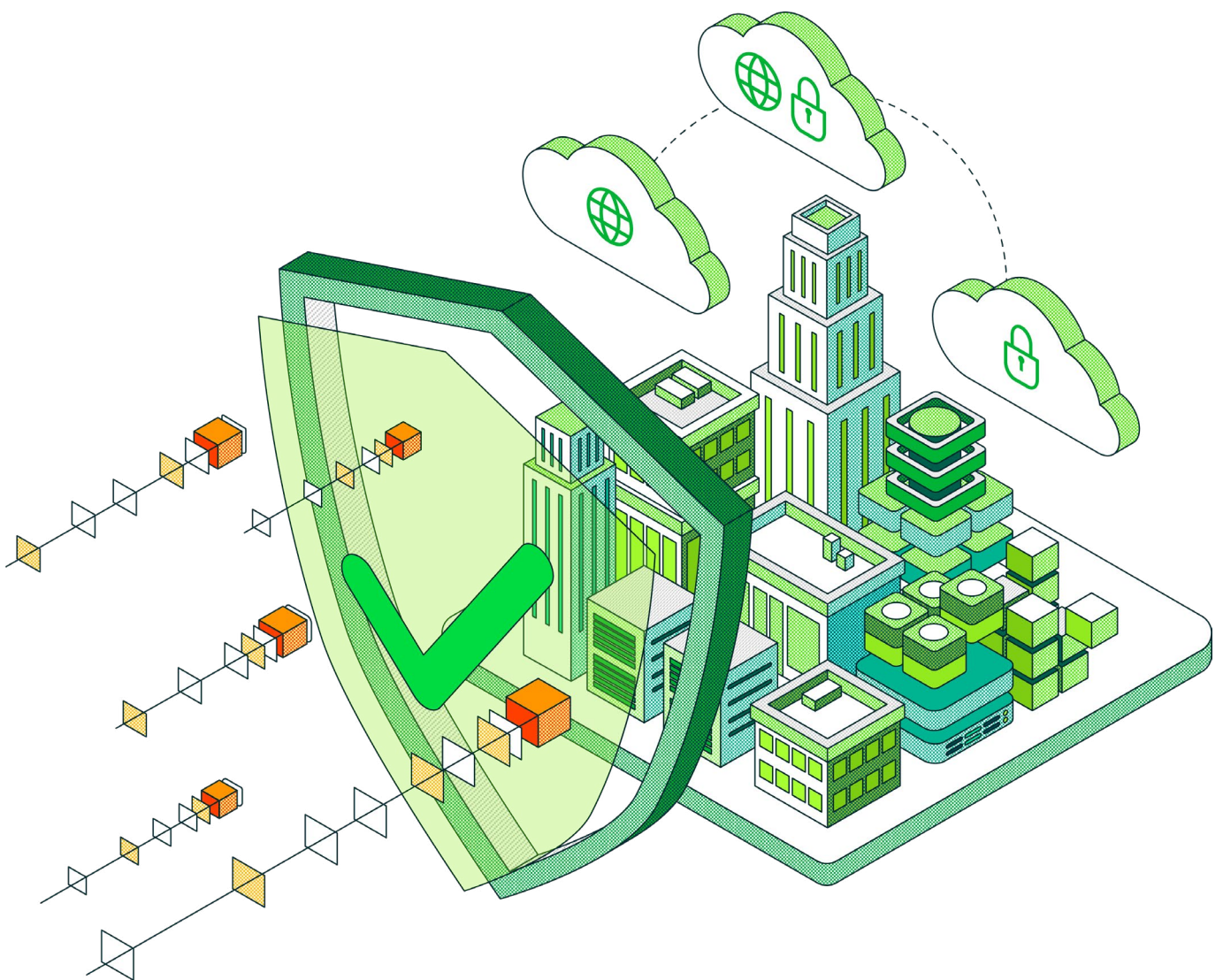


# Datensicherungs- trends 2023

Ausgabe für die Region DACH



Ende 2022 befragte ein unabhängiges Marktforschungsunternehmen **4.200** IT-Verantwortliche und Implementierungsexperten zu verschiedenen Aspekten der Datensicherung, zu ihren Herausforderungen und Strategien. **463** Umfrageteilnehmer stammten aus der Region DACH. Diese umfassende Marktstudie, die jährlich im Auftrag von Veeam durchgeführt wird, soll Aufschluss über die Entwicklung des Markts für Datensicherungslösungen geben. Ziel von Veeam ist es, mit entsprechenden Produktstrategien und Marktinitiativen auf diese Entwicklung zu reagieren.

Laut einer Prognose von Gartner werden sich die IT-Budgets von Unternehmen um **5,1 %** erhöhen, während IDC mit einem Anstieg der IT-Ausgaben um **5,2 %** rechnet. Die Umfrage hat nun ergeben, dass Unternehmen weltweit 2023 von einer Erhöhung ihrer Datensicherungsbudgets um **6,5 %** ausgehen. Der ausführliche Report zu den Datensicherungstrends 2023 steht unter <https://vee.am/DPR23> bereit.



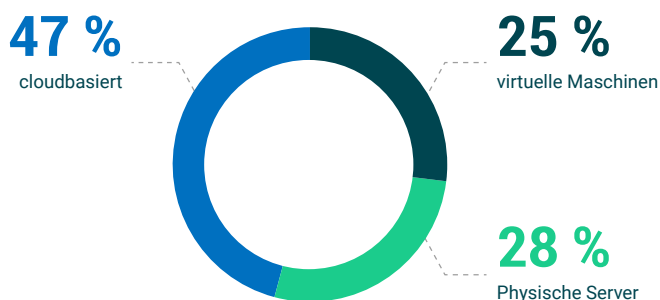
## Hybride Infrastrukturen 2020 bis 2025

Jedes Jahr werden die befragten Unternehmen gebeten, sowohl die Zahl der (physischen und virtuellen) Server in ihrer lokalen Umgebung als auch die Zahl ihrer in der Cloud bereitgestellten Server für das aktuelle Jahr anzugeben und zu schätzen, wie hoch diese Zahlen zwei Jahre später sein werden. Im **ausführlichen Report** finden Sie eine Zusammenfassung der **12.000** Antworten aus vier Umfragen, die den Zeitraum von 2020 bis 2025 abdecken. Für 2023 zeigt sich bei der Verteilung der Serverinstanzen in den hybriden IT-Umgebungen der **4.200** befragten Unternehmen dieses Bild:

der Unternehmen in der Region DACH rechnen 2023 mit einer Erhöhung ihres Datensicherungsbudgets um

**6,9 %**

### Zusammensetzung hybrider IT-Landschaften 2023 (global)



Der Anteil **physischer** Server und **virtueller** Maschinen in den IT-Umgebungen der Unternehmen hat sich bei jeweils rund **50 %** stabilisiert, die übrigen Server werden **in der Cloud gehostet**. Der Trend zur Umstellung auf in der Cloud gehostete Server setzt sich kontinuierlich, wenn auch langsam, fort, was vor allem an der Cloud-First-Strategie von Unternehmen liegt: Neue Workloads, die in der Cloud schneller implementiert werden können als in herkömmlichen Umgebungen, führen zur Deaktivierung von Workloads im Rechenzentrum. In einer hybriden IT-Strategie nimmt damit die Bedeutung des Rechenzentrums weiter ab.

	GLOBAL	REGION									
		EMEA	DACH	UKI	Frankreich	Benelux	Italien	Spanien/ Portugal	Skandinavien	Osteuropa	MEA
Physische Server	28 %	28 %	<b>29 %</b>	28 %	28 %	28 %	29 %	29 %	28 %	27 %	29 %
Virtuelle Maschinen	25 %	26 %	<b>25 %</b>	27 %	25 %	25 %	25 %	25 %	26 %	25 %	25 %
In der Cloud gehostet	47 %	46 %	<b>46 %</b>	45 %	47 %	47 %	46 %	46 %	47 %	48 %	46 %

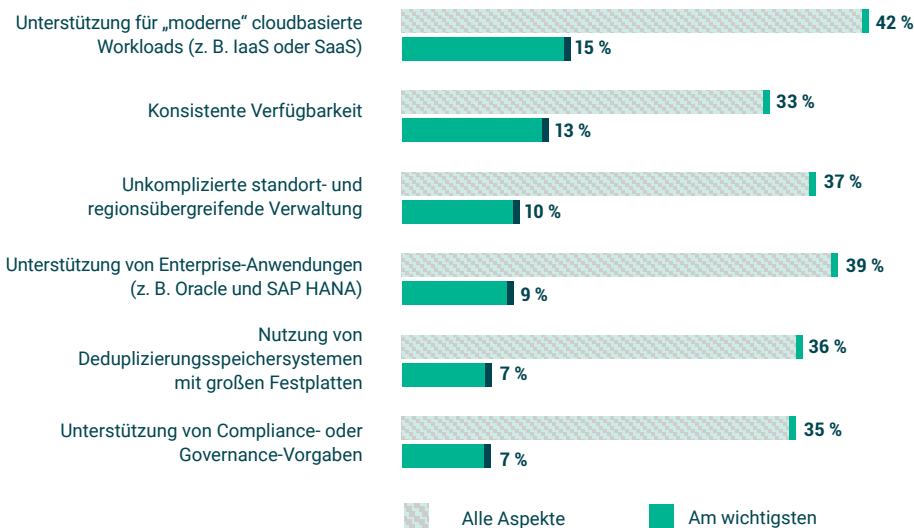
Daraus folgt, dass die Funktionalitäten moderner Datensicherungslösungen alle drei Architekturen (physisch, virtuell und cloudbasiert) gleichermaßen unterstützen müssen. Unternehmen sollten bei ihrer Planung außerdem die Migration von Workloads zwischen verschiedenen Cloud-Umgebungen oder sogar aus der Cloud zurück in die lokale Umgebung berücksichtigen. Auch hier gilt, dass diese flexible Migration von der Datensicherungsstrategie unterstützt werden sollte.

# Was bedeutet „Datensicherung der Enterprise-Klasse“?

Bereits das zweite Jahr in Folge nannten die Umfrageteilnehmer als wichtigsten Aspekt einer „Datensicherungslösung der Enterprise-Klasse“ die **Datensicherung für IaaS und SaaS**. Angesichts der zunehmenden Verlagerung von Infrastrukturen in die Cloud war dieses Ergebnis zu erwarten.

Überraschend hingegen ist, dass als zweitwichtigstes Kriterium die Gewährleistung der **Zuverlässigkeit** genannt wurde. Dabei gilt es jedoch zu bedenken, dass zahlreiche Unternehmen vermutlich nach wie vor herkömmliche Backup-Lösungen nutzen, die ursprünglich für physische Rechenzentren entwickelt wurden. Diese Lösungen verwenden für den Schutz von cloudbasierten Workloads sehr wahrscheinlich agentenbasierte Methoden. Mit herkömmlichen Backup-Verfahren lassen sich nur selten gute Ergebnisse beim Schutz moderner Workloads erzielen.

Daher ist es naheliegend, dass der Schutz cloudbasierter Workloads und Zuverlässigkeit für Unternehmen höchste Priorität haben.



Auf die Frage, weshalb sie auf eine andere primäre Datensicherungslösung umsteigen würden, nannten die meisten Unternehmen als wichtigsten Grund die **Verbesserung der Zuverlässigkeit**. Dieses Ergebnis deckt sich mit den Aspekten, die Unternehmen bei der Wahl einer Datensicherungslösung der Enterprise-Klasse besonders wichtig sind.

## „Moderne“ Datensicherung bedeutet 2023 Schutz vor Cyberangriffen

Was die wichtigsten Funktionalitäten einer modernen Datensicherungslösung betrifft, zeigt der ausführliche Report, dass Cyberangriffe das dritte Jahr in Folge die häufigste Ursache für Ausfälle mit schwerwiegenden Folgen sind. Die Zahl der Ransomware-Attacks nimmt weiter zu:

- 2021 wurden **76 %** der Unternehmen mindestens einmal Opfer eines Ransomware-Angriffs.
- 2022 gaben bereits **85 %** der befragten Unternehmen an, von mindestens einer solchen Attacke betroffen gewesen zu sein.

# 14 %

der Unternehmen in der Region DACH, die auf der Suche nach einer Backup-Lösung der Enterprise-Klasse sind, nennen den **„Schutz von IaaS- und SaaS-Workloads sowie des Rechenzentrums“** als wichtigstes Feature



Abbildung 1.2

Was verstehen Sie unter „Backup der Enterprise-Klasse“?

Welcher Aspekt wäre für Ihr Unternehmen derzeit bei der Evaluierung einer neuen „Datensicherungslösung der Enterprise-Klasse“ am wichtigsten?

# 30 %

der Unternehmen in der Region DACH nennen die **„Verbesserung der Zuverlässigkeit/des Erfolgs von Backups“** als Grund für den Umstieg auf eine andere Backup-Lösung

	GLOBAL	REGION EMEA	DACH	UKI	Frankreich	Benelux	Italien	Spanien/ Portugal	Skandinavien	Osteuropa	MEA
Keine Angriffe 2022	15 %	16 %	<b>21 %</b>	24 %	18 %	25 %	14 %	22 %	13 %	17 %	14 %
Nur ein Angriff	18 %	19 %	<b>24 %</b>	19 %	17 %	24 %	17 %	21 %	23 %	23 %	18 %
Zwei oder drei Angriffe	48 %	46 %	<b>40 %</b>	36 %	49 %	39 %	52 %	41 %	44 %	36 %	48 %
Vier oder mehr Angriffe	18 %	18 %	<b>14 %</b>	18 %	15 %	10 %	16 %	15 %	18 %	22 %	21 %

So alarmierend diese Statistiken sind – die Folgen dieser Attacken wiegen noch schwerer. Auf die Frage nach den schlimmsten Angriffen im Jahr 2022 gaben die Unternehmen an, dass:

- **39 %** ihrer gesamten Produktivdaten erfolgreich verschlüsselt oder zerstört wurden
- nur **55 %** der verschlüsselten/zerstörten Daten wiederhergestellt werden konnten

Es überrascht daher nicht, dass der wichtigste und am häufigsten genannte Aspekt einer „modernen Datensicherungslösung“ die Integration der Datensicherung in eine Strategie zum Schutz vor Cyberbedrohungen ist.

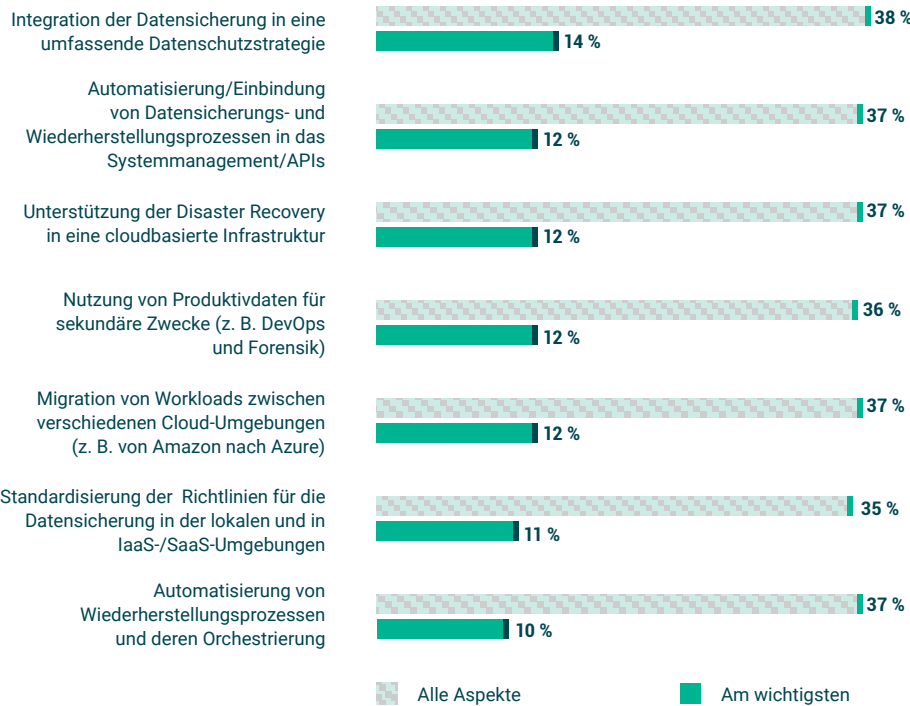


Abbildung 1.5

Was sind für Ihr Unternehmen die zentralen Aspekte einer „modernen“ oder „innovativen“ Datensicherungslösung?

Welcher Aspekt ist für Sie am wichtigsten?

Zwar hat der Schutz vor Cyberangriffen für zahlreiche IT-Verantwortliche weiterhin höchste Priorität, doch wäre es aus strategischer Perspektive verkehrt, die Planung der Datensicherung ausschließlich auf mögliche Attacken auszurichten. Systemausfälle, die durch Netzwerk-, Anwendungs-, Hardware- und Betriebssystemfehler verursacht werden, sind auch in modernen Rechenzentren nach wie vor an der Tagesordnung. Unternehmen sollten sowohl für diese Unterbrechungen als auch für Ausfälle gewappnet sein, die beispielsweise durch Benutzerfehler und Cyberkriminelle verursacht werden.

# BC/DR-Methoden und -Mechanismen

Die zunehmende Nutzung von Cloud-Services für die Datensicherung stellt zahlreiche Unternehmen vor die Frage, ob sie Daten auf lokalen Servern oder in cloudbasierte Infrastrukturen wiederherstellen sollen. Die Umfrageergebnisse zeigen, dass das Interesse an einer Wiederherstellung in die lokale Umgebung und in Cloud-Infrastrukturen 2023 relativ ausgewogen ist. Für die Wiederherstellung genutzt werden jedoch größtenteils cloudbasierte Backups. Ausschlaggebend dafür ist, dass die Zahl der Wiederherstellungspunkte in lokalen Umgebungen abnimmt und Unternehmen ihre Daten zu Aufbewahrungszwecken und zur Gewährleistung von BC/DR verstärkt auf cloudbasierte Speichersysteme auslagern.

Eine Best Practice ist es, davon auszugehen, dass im Krisenfall die primären Experten nicht mehr verfügbar sind. Die meisten BC/DR-Planer empfehlen deshalb, orchestrierte Workflows zu nutzen, bei denen das Know-how in Prozessen gekapselt werden kann. Es empfiehlt sich außerdem, die Workflows so zu testen, wie sie im tatsächlichen Krisenfall ausgeführt werden. Die Ergebnisse der diesjährigen Umfrage zeigen, dass nur **18 %** der befragten Unternehmen im Rahmen ihrer Datensicherungs- oder Failover-Strategie derzeit einen orchestrierten Workflow unterstützen.

# 61 %

der Unternehmen in der Region DACH planen den Einsatz von lokalen Servern für BC/DR, während **39 %** dafür in der Cloud gehostete Infrastruktur nutzen möchten

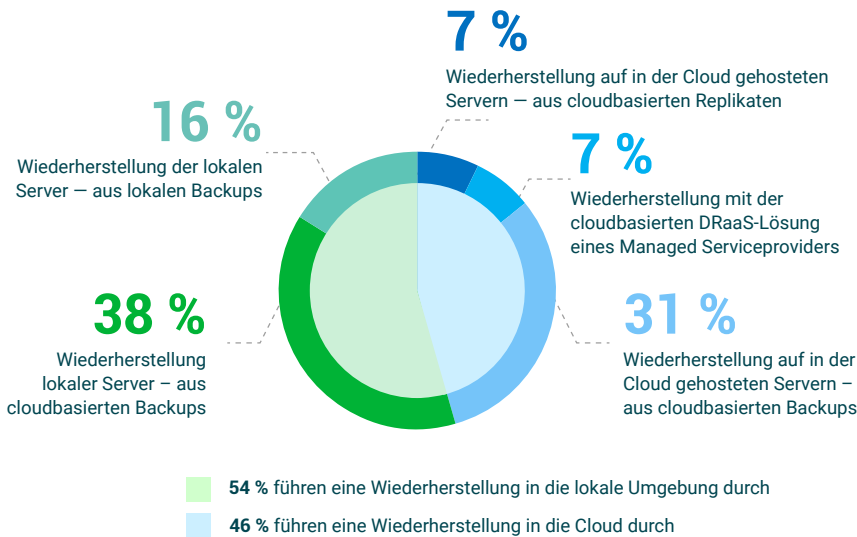


Abbildung 2.3

Wie erfolgt die Wiederaufnahme des Betriebs im Rahmen Ihrer DR-Strategie?

# Die cloudbasierte Datensicherung erfreut sich zunehmender Beliebtheit

Bedeutet cloudbasierter Storage das Ende der Datensicherung auf Tape? Laut den Umfrageergebnissen werden nach wie vor **50 %** der Daten im Lauf ihres Lebenszyklus auf Tape gesichert. **63 %** der Daten werden inzwischen auch irgendwann in der Cloud gespeichert. Dieser Prozentsatz variiert jedoch je nach Land oder Region.

	GLOBAL	REGION		UKI	Frankreich	Benelux	Italien	Spanien/ Portugal	Skandinavien	Osteuropa	MEA
		EMEA	DACH								
% der Daten auf Tape	50 %	53 %	<b>48 %</b>	42 %	51 %	53 %	51 %	49 %	52 %	53 %	52 %
% der Daten in Cloud(s)	63 %	63 %	<b>63 %</b>	56 %	64 %	65 %	66 %	63 %	63 %	69 %	64 %

Zahlreiche Unternehmen nutzen für die Datenaufbewahrung ein dreistufiges Betriebsmodell:

- Speicherung auf lokalen Festplatten für 90 bis 120 Tage
- Aufbewahrung von Cloud-Kopien (einschließlich aktueller und vorheriger Versionen) für einen Zeitraum von zwei bis fünf Jahren
- Tapesicherung eines kleinen Anteils von Daten, die gemäß Vorschriften zehn Jahre oder länger aufbewahrt werden müssen

Der prozentuale Anteil an Daten in der Cloud sollte auch unter dem Blickpunkt „% der Unternehmen, die cloudbasierte Backups nutzen“ betrachtet werden: **67 %** der weltweiten Umfrageteilnehmer nutzen bereits heute Cloud-Services im Rahmen ihrer Datensicherungsstrategie, **74 %** haben dies bis 2025 vor.

Zu den größten Synergien zwischen cloudbasierten Services und Datensicherung gehört eindeutig die cloudbasierte Disaster Recovery, bei der Cloud-Infrastrukturen anstelle von oder als Ergänzung zu einem sekundären Rechenzentrum genutzt werden. 2020 gab es in **53 %** der befragten Unternehmen BC/DR-Funktionalitäten, 2023 sind es bereits **71 %**. Ein noch wichtigeres Ergebnis ist, dass zwar rund **30 %** der Unternehmen weiter mehrere Rechenzentren für BC/DR-Zwecke nutzen, der Prozentsatz der Unternehmen, die Cloud-Services (IaaS/DR oder DRaaS) für BC/DR-Aufgaben einsetzen, sich jedoch zwischen 2020 (**23 %**) und 2023 (**47 %**) mehr als verdoppelt hat. Bis 2025 werden voraussichtlich **55 %** der Unternehmen cloudbasierte DR nutzen.



**71 %**

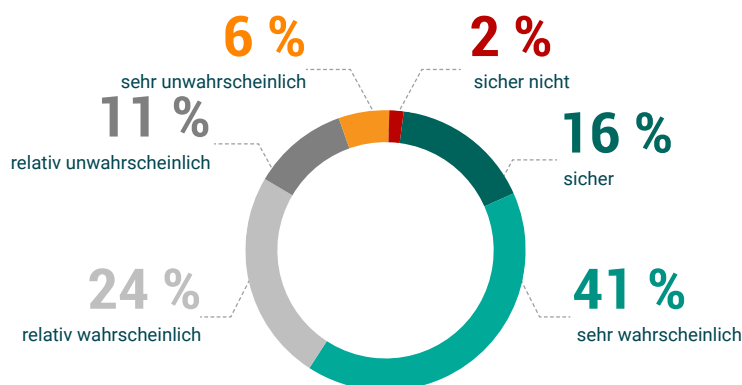
der Unternehmen in der Region DACH planen, bis 2025 Cloud-Services im Rahmen ihrer Datensicherungslösung zu nutzen

	GLOBAL	REGION EMEA	DACH	UKI	Frankreich	Benelux	Italien	Spanien/ Portugal	Skandinavien	Osteuropa	MEA
% der Unternehmen, die eine cloudbasierte Infrastruktur für BC/DR nutzen	47 %	41 %	<b>49 %</b>	41 %	46 %	47 %	40 %	52 %	54 %	49 %	41 %
% der Unternehmen, die mehrere Rechenzentren für BC/DR nutzen	24 %	25 %	<b>23 %</b>	34 %	23 %	22 %	26 %	23 %	24 %	24 %	25 %

## Wird 2023 ein Jahr des Wandels?

Angesichts der Furcht von Unternehmen vor Ransomware, der schwierigen Gewährleistung unterbrechungsfreier IT-Services und der Herausforderungen beim Schutz moderner IaaS- und SaaS-Workloads liegt die Vermutung nahe, dass zahlreiche Unternehmen den höheren Anforderungen durch den Umstieg auf eine andere Backup-Lösung gerecht werden möchten. Und die Umfrageergebnisse untermauern dies. Werden die **35 %** eher neutralen Antworten nicht berücksichtigt, zeigt sich dieses Bild:

- Nur **8 %** der Unternehmen werden 2023 sehr wahrscheinlich nicht auf eine andere primäre Backup-Lösung umstellen.
- **57 %** der Umfrageteilnehmer gaben hingegen an, dass sie wahrscheinlich oder sicher auf eine andere Backup-Lösung umsteigen werden.



**55 %**

der Unternehmen in der Region DACH gehen davon aus, dass sie 2023 auf eine andere Backup-Lösung umsteigen werden



Abbildung 3.6

Wie wahrscheinlich ist es, dass Ihr Unternehmen in den kommenden zwölf Monaten auf eine andere primäre Backup-Lösung/einen anderen Backup-Service umstellt?



## Die Einschätzung von Veeam

### Die Veeam Data Platform

Bei der Transformation ihrer Infrastruktur zur Unterstützung von Cloud-Aspekten wie Backup, Nutzung und Mobilität benötigen Unternehmen eine umfassende Lösung, die zugleich die Komplexität verringert. Die Veeam® Data Platform bietet diese Vorteile:

- Kontrolle der Storage-Kosten mit einer Architektur für intelligentes Cloud-Storage-Tiering
- Speziell für Kubernetes entwickelte Tools für Datensicherung, Wiederherstellung, Disaster Recovery und Mobilität von containerbasierten Anwendungen
- Umfassende Unterstützung für IaaS-/PaaS-/SaaS-Workloads
- Zentrales Monitoring und Management in Kombination mit umfassender API-Abdeckung

Neu- und Bestandskunden von Veeam stehen in Veeam Backup for AWS, Azure, Google Cloud, Microsoft 365 und Salesforce sowie in Kasten K10 für Kubernetes-Workloads branchenführende Funktionalitäten für die besonderen Anforderungen von Hybrid-Cloud-Umgebungen zur Verfügung.

Für Veeam-Anwender, die sich für servicebasierte Angebote interessieren oder ihre Ressourcen erweitern möchten, bietet ein umfassendes Netzwerk von BaaS- und DRaaS-Providern sowie Professional-Services-Partnern Unterstützung bei der optimalen Nutzung ihrer Investitionen in Veeam- und Cloud-Lösungen.



Laden Sie hier den vollständigen Report herunter.



Bei Fragen zu den Umfrageergebnissen senden Sie bitte eine Nachricht an [StrategicResearch@veeam.com](mailto:StrategicResearch@veeam.com).

