Global Data Protection Index 2021

Wichtige Erkenntnisse – Juli 2021

VansonBourne

DELL Technologies

Die wichtigsten Erkenntnisse im Fokus

1

Die Data-Protection-Risikolandschaft

2

Die Bedrohung durch Cyberangriffe

3

Schritthalten mit neuen und aufkommenden Technologien

4

Sicherheitslücken in der Data Protection in Cloud-Umgebungen

5

Die Zunahme von As a Service-Lösungen

6

Vereinfachung der Data Protection

5 wichtige Erkenntnisse

Die verbreitete Einführung des Arbeitens im Home Office hat die **Data-Protection- und Cyberrisiken erhöht**

Vielen fehlt das Vertrauen, dass die Data-Protection-Vorkehrungen ihres Unternehmens ausreichen, um sie vor Cyberbedrohungen zu schützen und deren Folgen zu überwinden

Ständige Investitionen in aufkommende Technologien und die Cloud **können zu zusätzlichen Data-Protection-Herausforderungen führen**

Viele sind **daran interessiert, As a Service-Lösungen zu nutzen,** um die Data Protection zu vereinfachen und flexibler zu gestalten

Es gibt Belege dafür, dass die Zusammenarbeit mit **weniger Data-Protection-Anbietern** zu **besseren Ergebnissen bei der Data Protection führt**

Wen haben wir befragt?

1.000 IT-Entscheidungsträger wurden im Februar, März und April 2021 befragt

Unternehmen aus einer Vielzahl von Branchen des öffentlichen und privaten Sektors

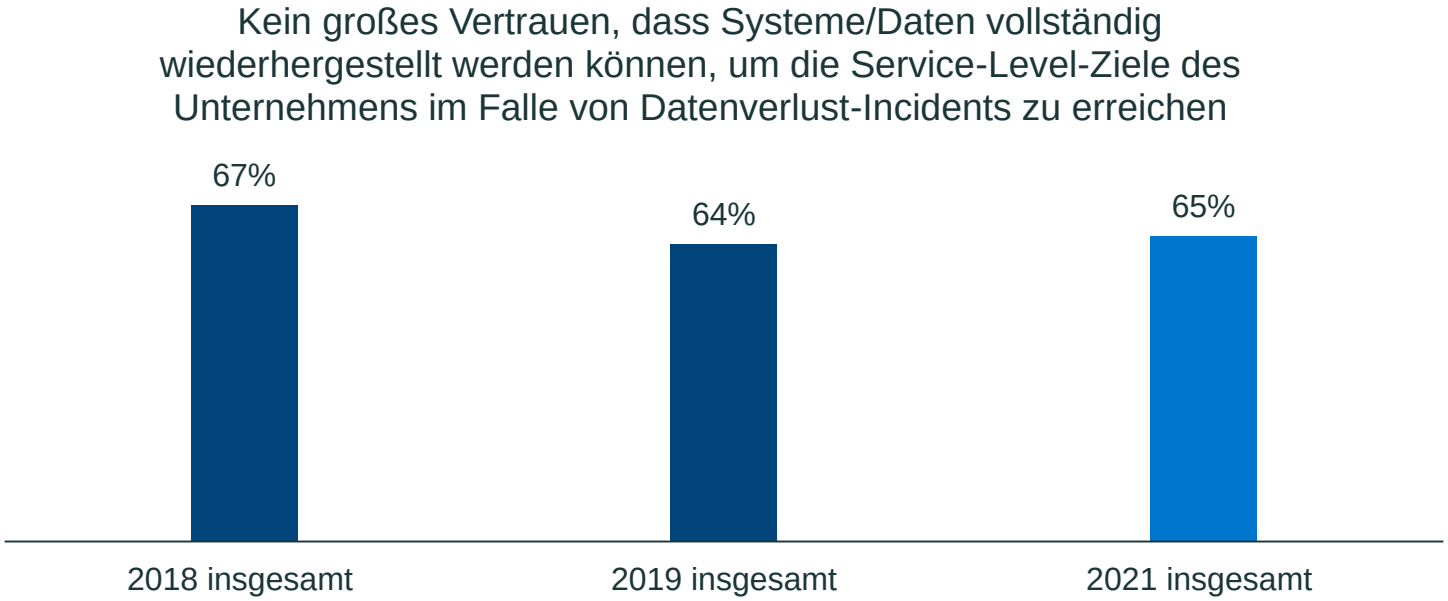
Unternehmen mit mehr als 250 Mitarbeitern

4 Regionen:

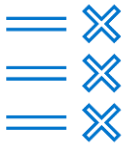
Amerika (200)
EMEA (450)
APJ (250)
China (100)

1. Die Data-Protection-Risikolandschaft

IT-Entscheidungsträger haben kein Vertrauen in die Fähigkeit ihres Unternehmens, die Recovery-SLOs zu erfüllen



Darüber hinaus ist das Vertrauen gering, dass Data-Protection-Funktionen die internen und externen Standards erfüllen – was dadurch noch besorgniserregender wird, dass zwei Drittel der Befragten davon ausgehen, dass sie im nächsten Jahr einen betriebsunterbrechenden Vorfall erleben werden



58 %

haben kein großes Vertrauen, dass ihr Unternehmen **seine Service-Level-Ziele für Backup und Recovery erfüllt**

63 %

haben kein großes Vertrauen, dass die aktuelle(n) Data-Protection-Infrastruktur und -Prozesse ihres Unternehmens **den regionalen Data Governance-Bestimmungen entsprechen**

64 %

machen sich **Sorgen, dass es in den nächsten 12 Monaten zu einem betriebsunterbrechenden Vorfall kommen wird**

Diese Sorge wird dadurch verstärkt, dass Datenverluste und Systemausfallzeiten weiterhin erhebliche finanzielle Auswirkungen auf Unternehmen haben

959.493 $

durchschnittliche Kosten von Datenverlust in den letzten 12 Monaten (in US-Dollar)

513.067 $

durchschnittliche Kosten von ungeplanten Ausfallzeiten in den letzten 12 Monaten (in US-Dollar)

2. Die Bedrohung durch Cyberangriffe

Unternehmen haben nicht das nötige Vertrauen, dass ihre Data-Protection-Maßnahmen die Auswirkungen von Cyberangriffen mindern können. Darüber hinaus sind die meisten davon überzeugt, dass aufgrund von Mitarbeitern, die von zu Hause aus arbeiten, ein erhöhtes Risiko besteht

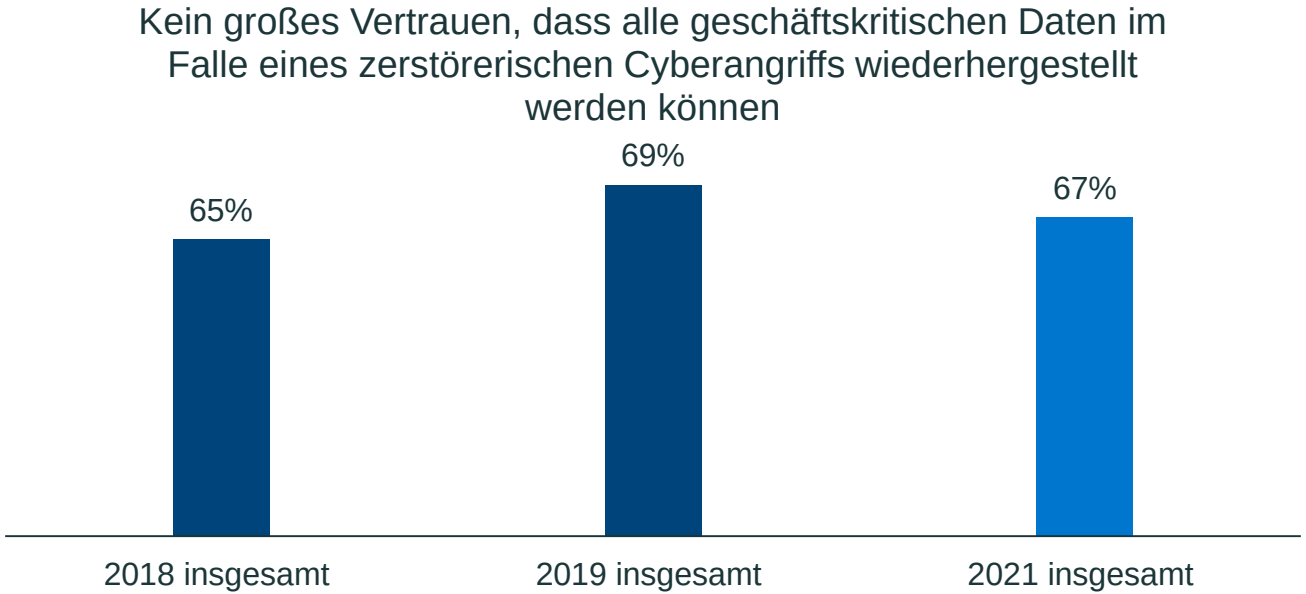
62 %

befürchten, dass die vorhandenen Data-Protection-Maßnahmen des Unternehmens **nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen**

74 %

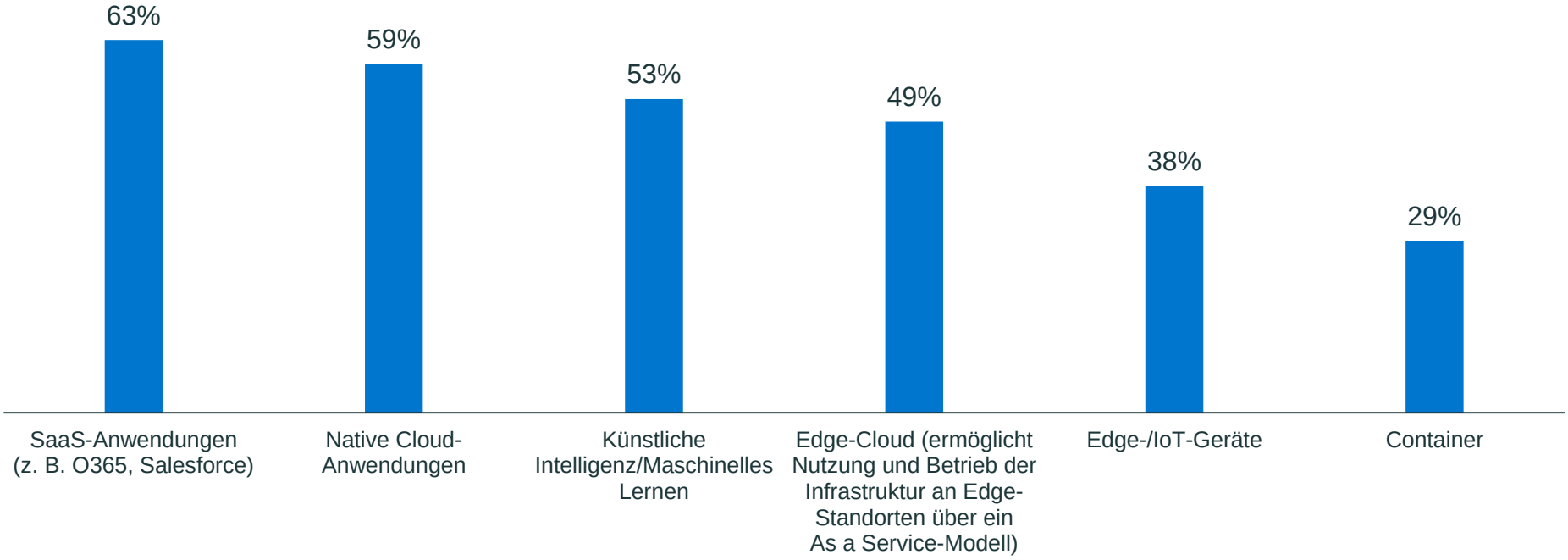
stimmen zu, dass bei ihrem Unternehmen aufgrund der wachsenden Zahl von **Mitarbeitenden im Homeoffice** ein **erhöhtes Risiko von Datenverlusten durch Cyberbedrohungen besteht**

Zu den Bedenken hinsichtlich der Fähigkeit von Unternehmen, mit Malware- und Ransomwarebedrohungen umzugehen, kommt hinzu, dass viele nicht darauf vertrauen, im Falle eines zerstörerischen Cyberangriffs alle geschäftskritischen Daten wiederherstellen zu können

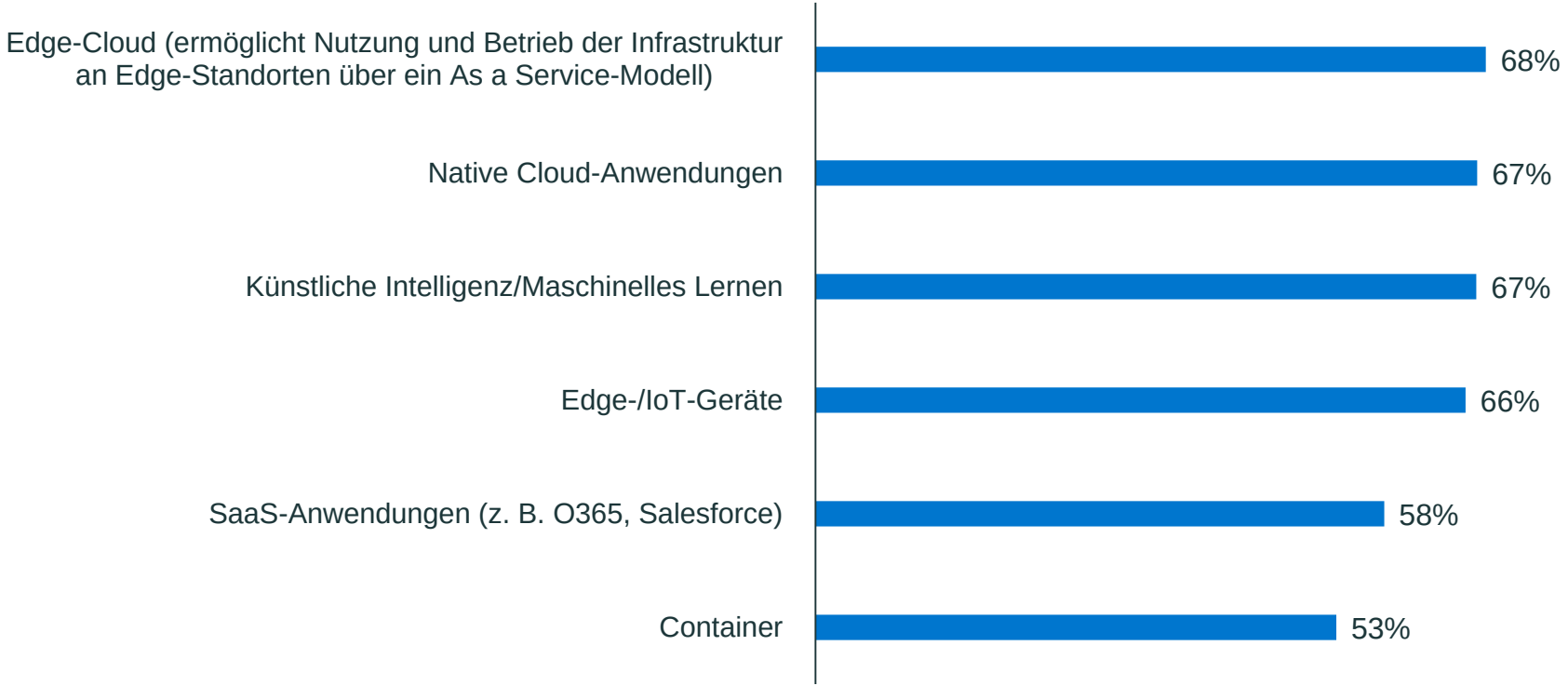


3. Schritthalten mit neuen und aufkommenden Technologien

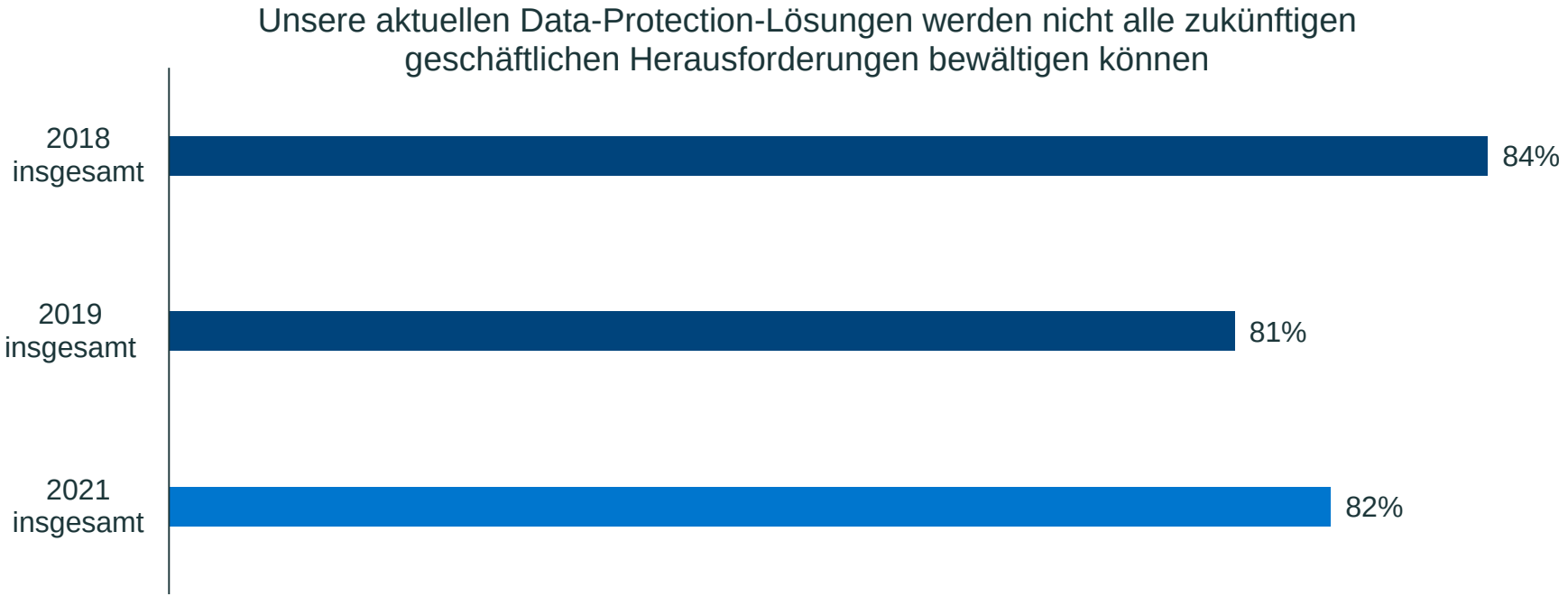
Unternehmen investieren in zahlreiche neue Technologien, die ihre Data-Protection-Herausforderungen möglicherweise noch erschweren können



Und viele Unternehmen tun sich schwer damit, diese Technologien zu schützen



Die Schwierigkeit, neue und neu aufkommende Technologien zu schützen, trägt wahrscheinlich dazu bei, dass das Vertrauen in die Zukunftsfähigkeit von Data-Protection-Lösungen gering ist



Viele sehen in aufkommenden Technologien ein Data-Protection-Risiko und die Besorgnis über künftige betriebsunterbrechende Vorfälle ist groß, insbesondere bei denjenigen, die mehrere Data-Protection-Anbieter verwenden

Aufkommende Technologien (wie KI, IoT, Edge) stellen ein Data-Protection-Risiko dar

Verwenden einen einzigen Data-Protection-Anbieter

57 %

Verwenden mehrere Data-Protection-Anbieter

64 %

Ich mache mir Sorgen, dass es in den nächsten 12 Monaten zu einem betriebsunterbrechenden Vorfall (z. B. Datenverlust, Ausfallzeit usw.) kommen wird

Verwenden einen einzigen Data-Protection-Anbieter

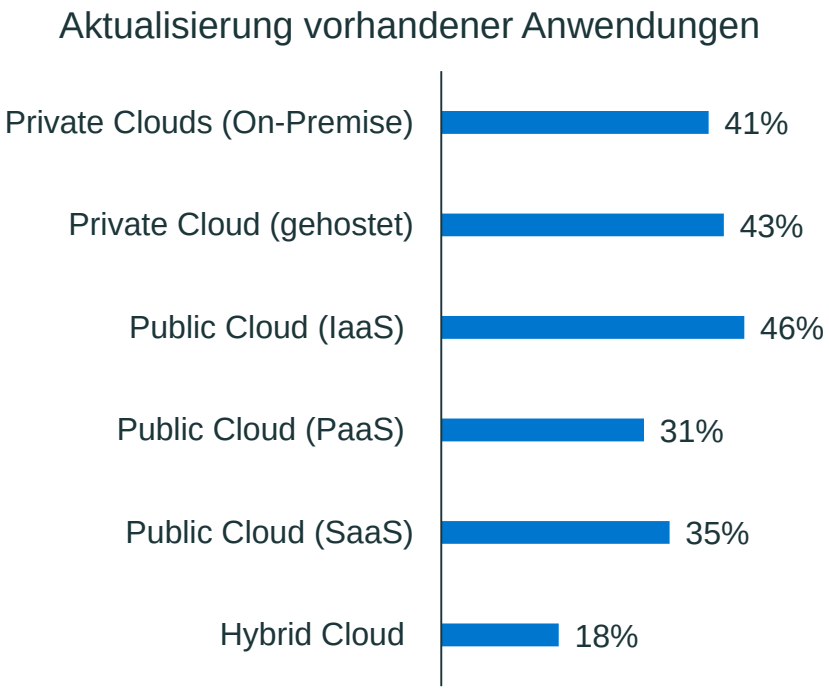
54 %

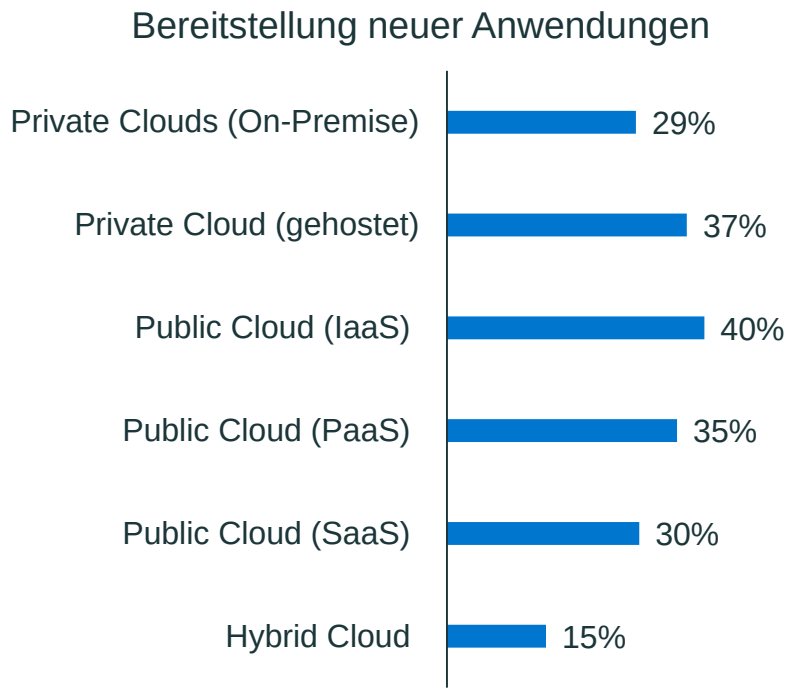
Verwenden mehrere Data-Protection-Anbieter

68 %

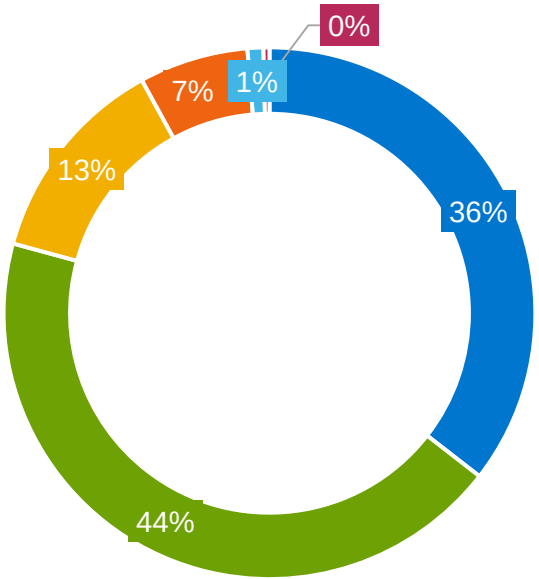
4. Sicherheitslücken in der Data Protection in Cloud-Umgebungen

Anwendungen werden in einer Vielzahl von Umgebungen in den IT-Infrastrukturen von Unternehmen aktualisiert und bereitgestellt



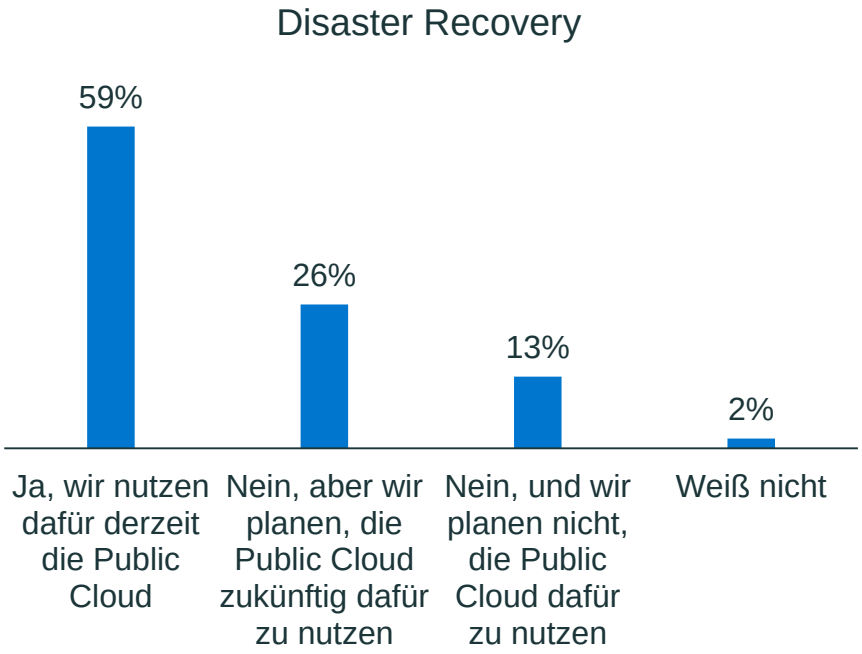


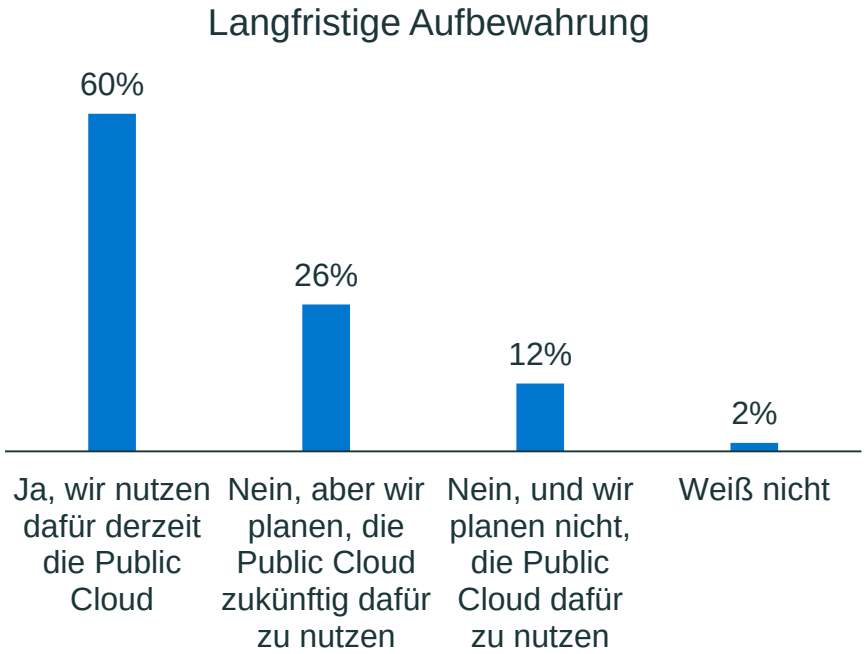
Vielen fehlt es jedoch an Vertrauen, wenn es darum geht, wie gut sie ihre Daten in Public-Cloud-Umgebungen schützen können



- Großes Vertrauen – wir schützen all unsere Daten in der Public Cloud
- Mäßiges Vertrauen – wir schützen alle kritischen Daten in der Public Cloud, aber nicht alle unsere Daten
- Einige Zweifel – wir schützen die meisten unserer kritischen Daten in der Public Cloud
- Kein großes Vertrauen – wir schützen einige unserer kritischen Daten in der Public Cloud
- Überhaupt kein Vertrauen – wir schützen unsere Daten in der Public Cloud nicht
- Weiß nicht

Die Public Cloud spielt in den Unternehmen eine wachsende Rolle bei Strategien für Disaster Recovery und langfristige Aufbewahrung

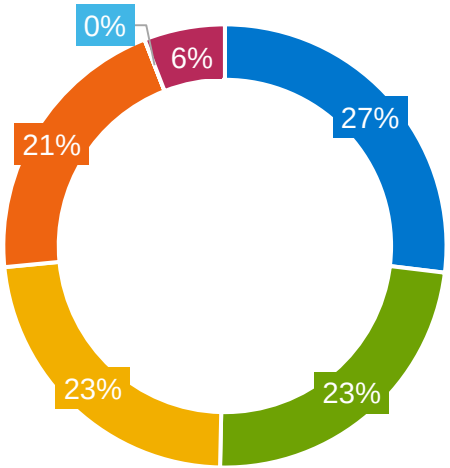




Eine Reihe von Unternehmen, die mehrere Cloud-Umgebungen nutzen, verwenden keine speziellen Lösungen, um sie zu schützen

21 %

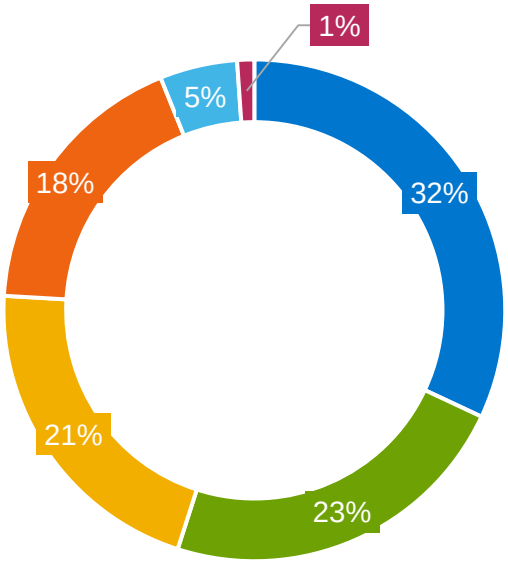
sind der Meinung, dass bei Verwendung mehrerer Cloud-Umgebungen **jeder Cloud-Serviceanbieter** für **den Schutz der Workloads des Unternehmens verantwortlich ist**



- Wir planen ein Upgrade unserer Data-Protection-Lösung, um das Backup von Workloads über mehrere Clouds hinweg zu ermöglichen
- Unsere aktuelle Backuplösung ermöglicht es uns, Workloads zu schützen, die in mehreren Clouds ausgeführt werden
- Wir verwenden mehrere Backuptools zum Schutz von Workloads, die in mehreren Clouds ausgeführt werden
- Jeder Cloud-Serviceanbieter ist für den Schutz unserer Workloads verantwortlich
- Sonstiges
- Wir führen Workloads nicht in mehreren Cloud-Umgebungen aus

Ähnliches gilt für den Schutz virtualisierter Workloads mit VMware in der Cloud

- Wir planen ein Upgrade unserer Data-Protection-Lösung, weil wir Hybrid-Cloud-Backups von VMware-Workloads ermöglichen möchten
- Unser Cloud-Serviceanbieter ist für den Schutz unserer Workloads verantwortlich
- Mit Backuptools, die wir derzeit in der On-Premise-Umgebung nutzen und betreiben
- Mit vom Cloud-Serviceanbieter bereitgestellten Backuptools
- Wir führen keine virtualisierten Workloads mit VMware in der Cloud aus und planen dies auch nicht
- Weiß nicht

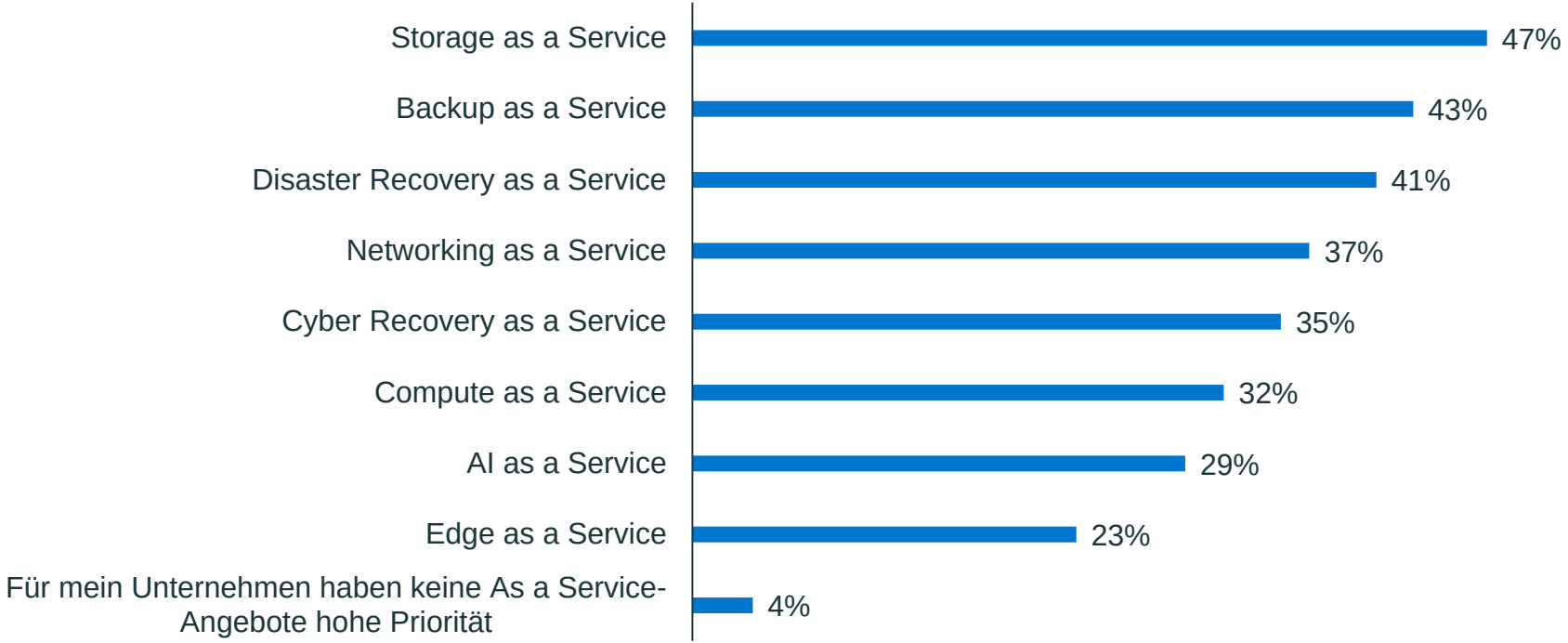


23%

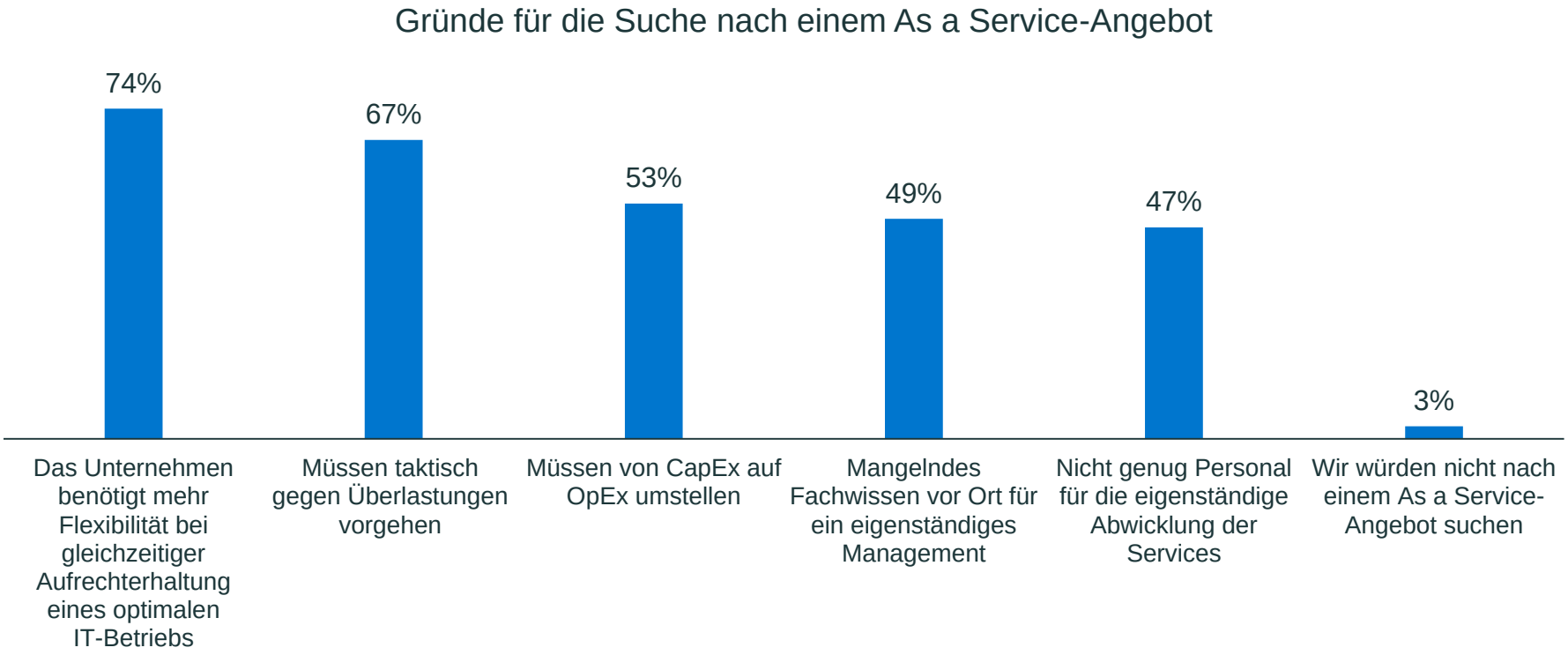
sind der Ansicht, dass ihr **Cloud-Serviceanbieter** für den **Schutz ihrer virtualisierten Workloads verantwortlich ist**

5.Die Zunahme von As a Service-Lösungen

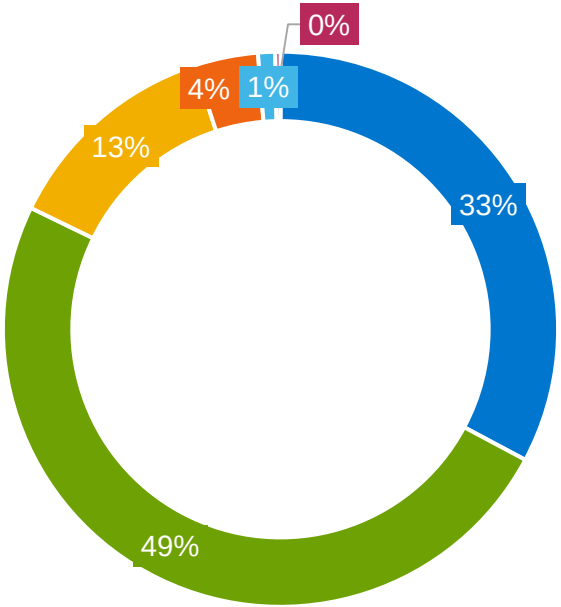
As a Service-Angebote werden von den meisten Unternehmen priorisiert, wobei Backup as a Service und Disaster Recovery as a Service am häufigsten priorisiert werden



Die Beliebtheit von As a Service-Angeboten ist oft auf ihre Flexibilität zurückzuführen



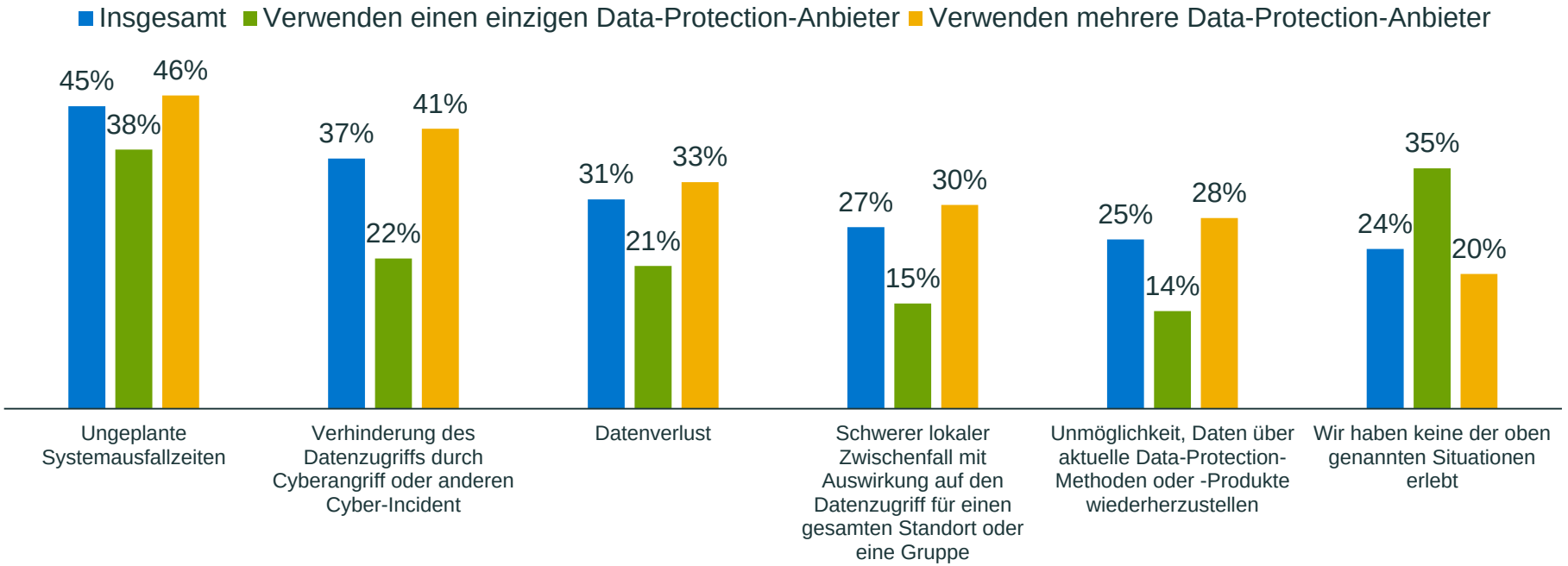
Die große Mehrheit würde lieber mit einem Anbieter zusammenarbeiten, der über mehrere As a Service-Angebote verfügt, was darauf hinweist, dass die Unternehmen ihre Workloads bei weniger Anbietern konsolidieren möchten



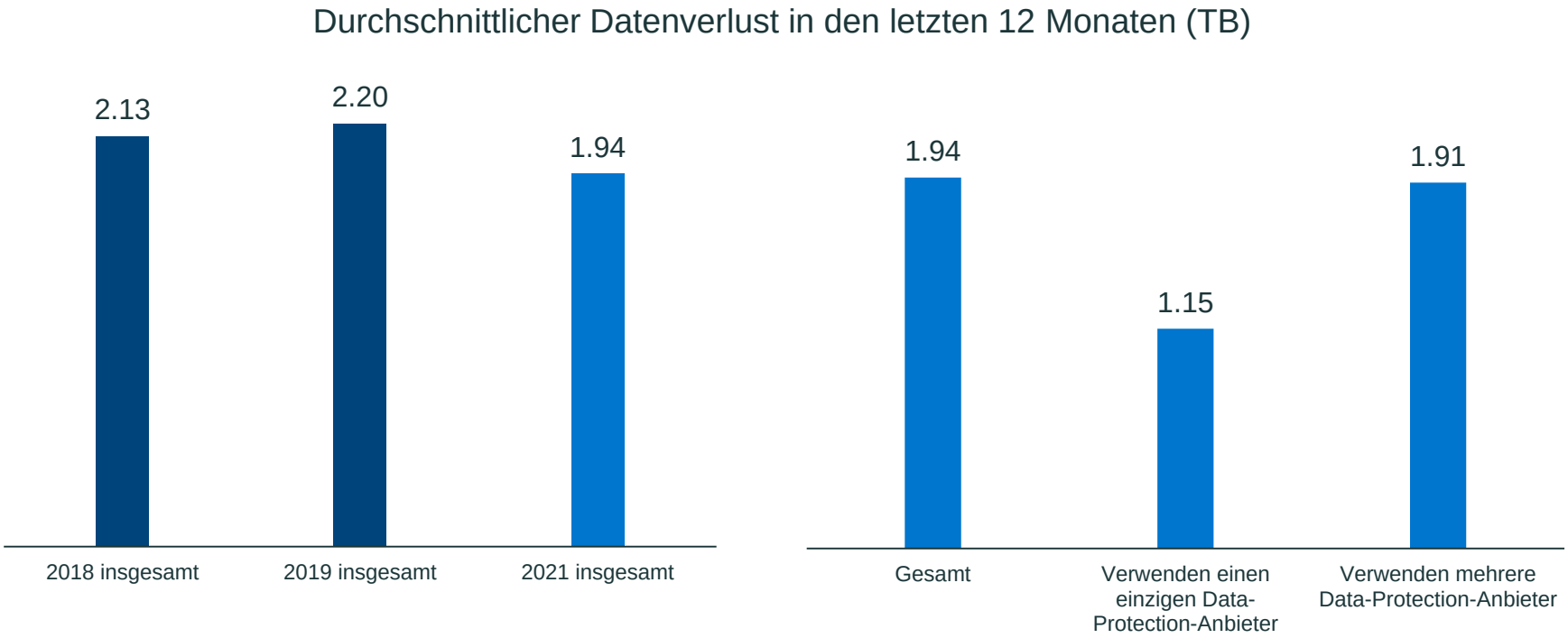
- Es ist weitaus wahrscheinlicher, dass wir einen Anbieter wählen, der mehrere As a Service-Angebote hat
- Es ist etwas wahrscheinlicher, dass wir einen Anbieter wählen, der mehrere As a Service-Angebote hat
- Es ist mir gleichgültig, ob ein Anbieter mehrere As a Service-Angebote hat
- Es ist etwas unwahrscheinlicher, dass wir einen Anbieter wählen, der mehrere As a Service-Angebote hat
- Es ist viel unwahrscheinlicher, dass wir einen Anbieter wählen, der mehrere As a Service-Angebote hat
- Weiß nicht

6. Vereinfachung der Data Protection

Unternehmen, die mehrere Anbieter von Data-Protection-Lösungen nutzen, hatten im vergangenen Jahr häufiger Probleme mit Datenverlusten, Datenzugriff oder Systemausfällen als Unternehmen, die nur einen einzigen Anbieter nutzen



Und Unternehmen, die mehrere Data-Protection-Anbieter nutzen, verlieren im Durchschnitt mehr Daten als Unternehmen, die einen einzigen Anbieter nutzen



Wichtigste Erkenntnisse – Zusammenfassung (1/2)

Die Data-Protection-Risikolandschaft

- Viele haben Bedenken, dass sie im Falle von Datenverlust-Incidents nicht in der Lage sein werden, alle Systeme/Daten wiederherzustellen, um die Service-Level-Ziele zu erreichen.
- Die Angst ist weit verbreitet, dass die Unternehmen in den nächsten 12 Monaten einen betriebsunterbrechenden Vorfall erleben werden, dessen Auswirkungen finanziell ruinös sein könnten.
- Unternehmen müssen Maßnahmen ergreifen, um sicherzustellen, dass sie bereit sind, auf solche Ereignisse zu reagieren, wenn sie auftreten.

Die Bedrohung durch Cyberangriffe

- Die Besorgnis ist groß, dass die Unternehmen nicht in der Lage sind, sich gegen Malware- und Ransomwarebedrohungen zu schützen, und die meisten stimmen zu, dass das Risiko von Cyberangriffen mit der Zunahme der Remotearbeit gestiegen ist.
- Wenn Unternehmen Opfer von Angriffen werden, sind nur wenige zuversichtlich, dass ihr Unternehmen in der Lage wäre, alle geschäftskritischen Daten wiederherzustellen.

Schritthalten mit neuen und aufkommenden Technologien

- Die Unternehmen investieren in eine Reihe neuer und aufkommender Technologien, darunter SaaS-Anwendungen, KI/ML und Edge-/IoT-Geräte, haben aber oft Schwierigkeiten, sicherzustellen, dass ihre Data-Protection-Maßnahmen damit Schritt halten.
- Viele sind der Meinung, dass diese Technologien ein Data-Protection-Risiko darstellen, und diese Risiken tragen vermutlich zu der Befürchtung bei, dass die Unternehmen nicht für die Zukunft gerüstet sind und dass sie in den nächsten 12 Monaten von Unterbrechungen bedroht sein werden.
- Investitionen in aufkommende Technologien sind sinnvoll und sollten gefördert werden, aber die Unternehmen müssen sicherstellen, dass ihre Data-Protection-Infrastruktur diese Technologien unterstützt.

Wichtigste Erkenntnisse – Zusammenfassung (2/2)

Sicherheitslücken in der Data Protection in Cloud-Umgebungen

- Anwendungen werden in einer Reihe von Cloud-Umgebungen aktualisiert und bereitgestellt, doch fehlt es oft an Vertrauen, wenn es darum geht, wie gut die Daten geschützt werden können.
- Die Cloud spielt eine wichtige Rolle bei Strategien für Disaster Recovery und langfristige Aufbewahrung.
- Die Unternehmen müssen sicherstellen, dass sie über spezielle Lösungen zum Schutz von Daten in Multi-Cloud-Umgebungen und virtualisierten Workloads verfügen, da einige Unternehmen immer noch glauben, dass hierfür ihre Cloud-Anbieter verantwortlich sind.

Die Zunahme von As a Service-Lösungen

- As a Service-Lösungen sind für die meisten Unternehmen von Interesse und werden in Zukunft vermutlich ein Teil der Data-Protection-Lösungen vieler Unternehmen sein – Flexibilität ist oft ein wichtiger Grund für dieses Interesse.
- Die meisten Unternehmen bevorzugen As a Service-Lösungen von Anbietern mit mehreren Angeboten – eine Entscheidung, die Data Protection für diese Unternehmen vereinfachen könnte.

Vereinfachung der Data Protection

- Unternehmen, die einen einzigen Data-Protection-Anbieter nutzen, hatten im vergangenen Jahr seltener Incidents mit Datenverlusten, Problemen beim Datenzugriff und ungeplanten Systemausfallzeiten zu verzeichnen als Unternehmen, die mehrere Anbieter nutzen.
- Diejenigen, die einen einzigen Anbieter nutzen, haben darüber hinaus im Durchschnitt weniger Daten verloren als diejenigen, die mehrere Lösungen nutzen.
- Auch wenn Unternehmen versucht sein mögen, ihre Data-Protection-Funktionen durch Investitionen in neue Lösungen zu erweitern, sind sie durch die Konsolidierung ihrer Lösungen bei einem einzigen Anbieter vermutlich besser vor Datenverlusten und Ausfallzeiten geschützt.

Risiken minimieren und Vorsprung gewinnen

Das Konzept von Dell Technologies

Regelmäßige Überprüfungen der Data-Protection-Bereitschaft durchführen

Ausfallsicherheit bei Cyberangriffen zur obersten Priorität machen

Data-Protection-Initiativen mit Dell konsolidieren

Weitere Informationen finden Sie unter DellTechnologies.com/GDPI


DELL Technologies