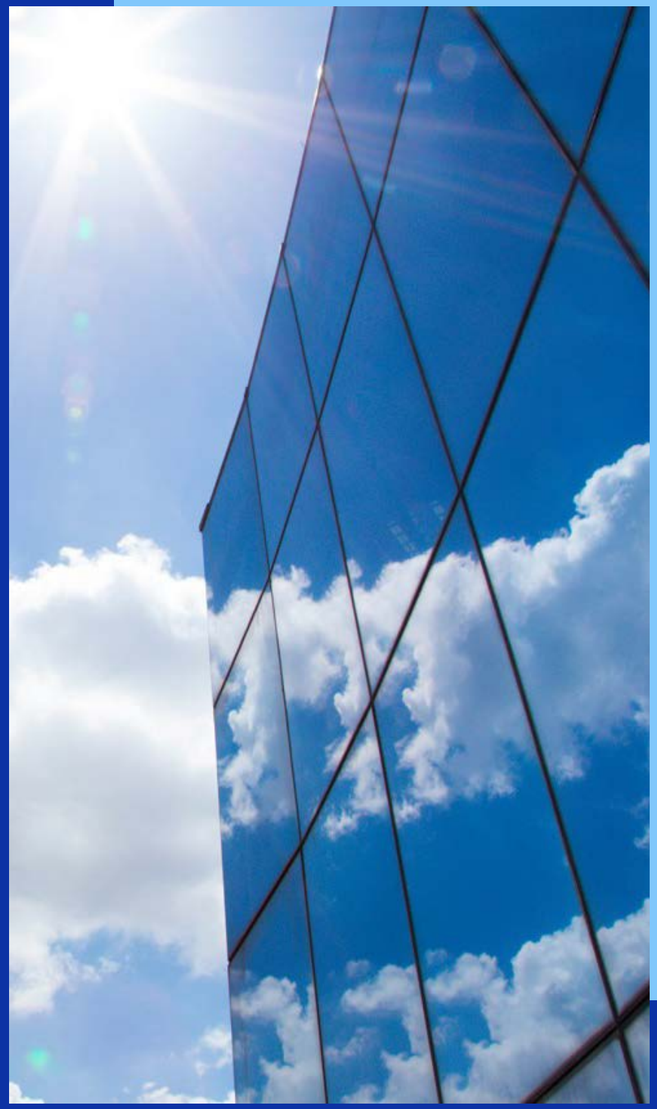
Global Data Protection Index

Ausfallsicherheit bei Cyberangriffen für Multi-Cloud

DELL Technologies

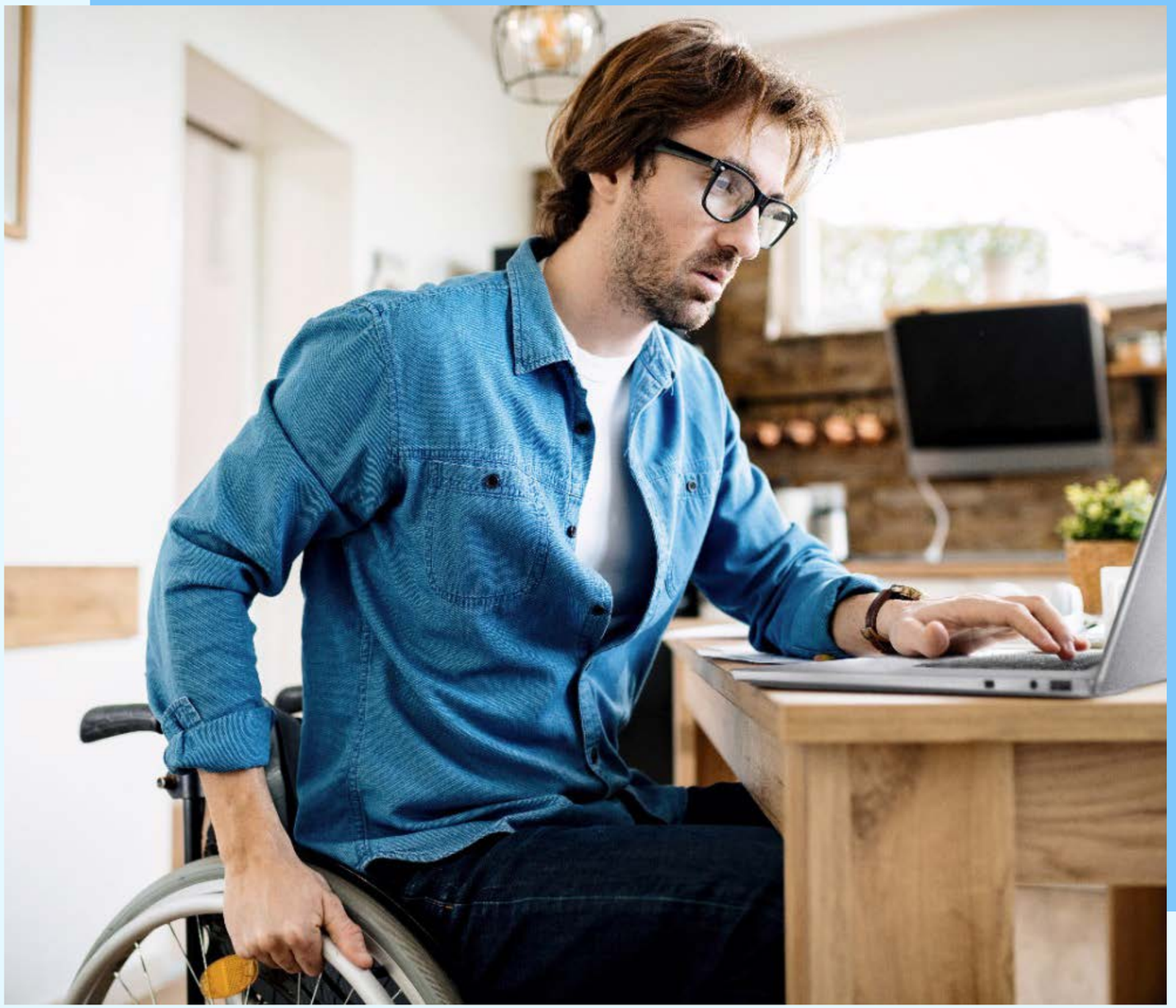
Inhaltsverzeichnis



Einführung

In der heutigen digital transformierten Welt sind Daten aufgrund ihrer entscheidenden Rolle in der Unternehmensstrategie ein Hauptziel für stark zunehmende Cyberbedrohungen. Der Vormarsch der generativen KI und die Ausweitung auf hybride Multi-Cloud-Umgebungen haben diese Risiken erhöht. Dabei verursachen Cyberangriffe erhebliche finanzielle Schäden – im Vergleich zum Vorjahr verdoppelten sie sich auf durchschnittlich 1,4 Millionen USD. Vor diesem Hintergrund stehen Unternehmen vor der Herausforderung, ihre immer komplexer werdenden Cloud-Ressourcen zu schützen und zu sichern, was den dringenden Bedarf an robusten, cybersicheren Data-Protection-Strategien in dieser sich ständig weiterentwickelnden Landschaft unterstreicht.

Dieses E-Book präsentiert die Ergebnisse des von Vanson Bourne in Auftrag gegebenen Global Data Protection Index 2024 von Dell Technologies, einer Umfrage unter 1.000 IT-EntscheidungsträgerInnen und 500 IT-SicherheitsentscheidungsträgerInnen weltweit. Sofern nicht anders angegeben, werden bei historischen Vergleichen nur die Ergebnisse der 1.000 IT-EntscheidungsträgerInnen herangezogen.



Die Data-Protection-Risikolandschaft

Das Navigieren auf dem komplexen Terrain der Data Protection bleibt eine enorme Herausforderung für Unternehmen, eine Hürde, die sich direkt auf ihren Weg zur digitalen Transformation auswirkt. Die überwiegende Mehrheit (90 %) der Unternehmen hat in den letzten 12 Monaten irgendeine Art von Unterbrechung erlebt.

Diese weit verbreitete Unterbrechung geht auch an den IT-Verantwortlichen und IT-Sicherheitsverantwortlichen nicht spurlos vorüber. 79 % der Befragten äußern sich besorgt über potenzielle disruptive Ereignisse im kommenden Jahr.

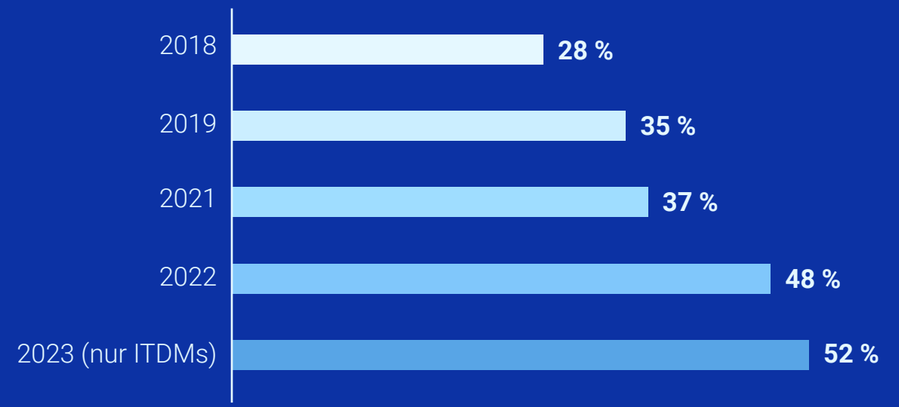
Diese Befürchtungen werfen einen Schatten auf ihr Vertrauen in die Erreichung der Servicelevelziele (SLOs) für Backup und Recovery. 60 % der Befragten sind nicht sehr zuversichtlich, was die Fähigkeiten ihres Unternehmens in diesem Bereich angeht.

Hinzu kommt, dass Datenverluste erhebliche finanzielle Auswirkungen auf die Unternehmen haben, die in den letzten 12 Monaten durchschnittlich 2,61 Millionen USD gekostet haben.

Die zunehmende Bedrohung durch Cyberangriffe

Die Bedrohung durch Cyberangriffe nimmt weiter zu und steht bereits das zweite Jahr in Folge an erster Stelle der Ursachen für Unterbrechungen in Unternehmen. Mehr als die Hälfte (52 %) der IT-EntscheidungsträgerInnen geben an, dass ihr Unternehmen in den letzten 12 Monaten Opfer eines Cyberangriffs oder eines Incidents war, der den Datenzugriff verhindert hat.

Datenzugriffsverlust aufgrund von Cyberangriff oder anderem Cyber-Incident



Cyberkriminelle haben es auf eine ganze Reihe von Einstiegspunkten abgesehen, aber die Angriffe kommen eher von externen Quellen. Bei 55 % der AngreiferInnen war der erste Einstiegspunkt ein externer – NutzerInnen, die auf Spam- oder Phishing-E-Mails und bösartige Links klicken, kompromittierte Nutzerzugangsdaten und gehackte Mobilgeräte.

Kosten von Cyberangriffen

Dies hat beträchtliche finanzielle Auswirkungen auf Unternehmen, da sich die Kosten im Zusammenhang mit Cyberangriffen und anderen cyberbezogenen Incidents in den letzten 12 Monaten mehr als verdoppelt haben:

2022

660.000 USD

2023 (nur ITDMs)

1,41 Mio. USD

Außerdem sind externe Sicherheitsverletzungen die am häufigsten genannte Ursache für Datenverluste und/oder Systemausfallzeiten in Unternehmen.

40 %

Das Risiko des mobilen Arbeitens

Trotz der Beliebtheit von mobilem und hybridem Arbeiten befinden sich Unternehmen in einer prekären Lage. Mehr als acht von zehn Unternehmen (81 %) sind der Meinung, dass sie aufgrund der zunehmenden Zahl von MitarbeiterInnen, die von zu Hause aus arbeiten, einem erhöhten Risiko von Datenverlusten durch Cyberbedrohungen ausgesetzt sind.

Angesichts der wachsenden Zahl an Homeoffice-MitarbeiterInnen steigt auch das Risiko von Datenverlust durch Cyberbedrohungen

2022 **70 %** → **2023** (nur ITDMs) **81%**

Zusammenfassung: Kombination aus „Stimme voll zu“ und „Stimme zu“

Hinzu kommt, dass ein wachsender Teil der Befragten der Meinung ist, dass die bestehenden Data-Protection-Maßnahmen ihres Unternehmens nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen.

Ich befürchte, dass die vorhandenen Data-Protection-Maßnahmen meines Unternehmens nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen

2022 **67 %** → **2023** (nur ITDMs) **75 %**

Zusammenfassung: Kombination aus „Stimme voll zu“ und „Stimme zu“

Ransomware-Policen

In einer Zeit, in der Cyberbedrohungen eine allgegenwärtige Bedrohung darstellen, können Versicherungspolicen Unternehmen Sicherheit bieten. Doch obwohl Ransomware-Policen weit verbreitet sind (93 %), werden sie nur unter strengen Auflagen abgeschlossen:

57 % Mein Unternehmen muss bewährte Verfahren zur Abwehr von Cyberbedrohungen nachweisen.

43 % Die Versicherung hat eine Höchstgrenze für die Auszahlung bei einem Schaden.

40 % Es gibt bestimmte Szenarien, in denen die Police nichtig wäre.

40 % Die Versicherung zahlt nicht aus, da die Zahlung an bestimmte Unternehmen möglicherweise gesetzlich eingeschränkt ist.

85 % Die meisten Unternehmen, die von einem Ransomwareangriff betroffen waren, haben für den Zugriff auf ihre Daten bezahlt.

Aber nur etwas mehr als ein Viertel **(28 %)** wurde von ihrer **Versicherung vollständig entschädigt**, sodass viele **Unternehmen finanziell gefährdet** sind.

Generative KI und Cybersicherheit

Mit zunehmender Anzahl von Cyberbedrohungen zeichnet sich eine deutliche Verschiebung hin zur generativen KI als strategisches Tool zur Stärkung der Cyberabwehr ab.

52 % sind der Ansicht, dass die Integration generativer KI einen Vorteil für die Cybersicherheit ihres Unternehmens im Kampf gegen Cyberkriminelle darstellt.

Dieser Optimismus wird jedoch durch das Wissen um die damit verbundenen Herausforderungen gedämpft.

88 %

der ExpertInnen sind sich einig, dass die Einführung generativer KI große Mengen neuer Daten erzeugen wird, die Schutz- und Sicherheitsmaßnahmen erforderlich machen.

Ebenfalls

88 %

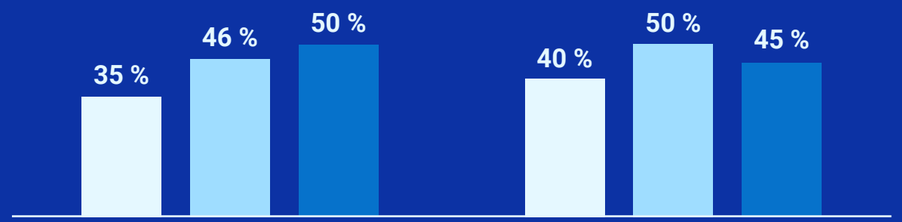
sind der Meinung, dass generative KI den Wert bestimmter Datentypen erhöhen wird, was ein höheres Maß an Data-Protection-Services erfordert.

Diese Erkenntnisse unterstreichen den doppelten Charakter der generativen KI als leistungsstarke Abwehrmaßnahme und als Quelle neuer komplexer Cybersicherheitsaspekte.

Die Nutzung von Multi-Cloud

Die Einführung von Public-Cloud-Lösungen ist nach wie vor eine bevorzugte Strategie für Unternehmen, die Anwendungen bereitstellen oder aktualisieren möchten. Diese Vorliebe führt jedoch auch zu einer zusätzlichen Ebene der Komplexität der Data Protection.

Bereitstellung neuer Anwendungen



Public Cloud (PaaS) (Hardware und Betriebssysteme, die von einem Drittanbieter über das Internet bereitgestellt werden)

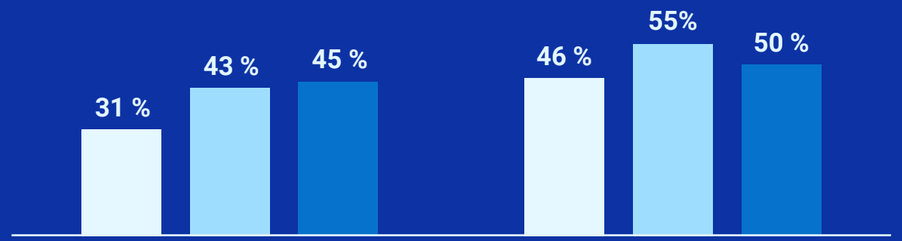
Public Cloud (IaaS) (Geräte wie Server, virtuelle Maschinen und Netzwerkkomponenten, die von einem Drittanbieter über das Internet bereitgestellt werden)

2021

2022

2023 (nur ITDMs)

Aktualisierung vorhandener Anwendungen



Public Cloud (PaaS) (Hardware und Betriebssysteme, die von einem Drittanbieter über das Internet bereitgestellt werden)

Public Cloud (IaaS) (Geräte wie Server, virtuelle Maschinen und Netzwerkkomponenten, die von einem Drittanbieter über das Internet bereitgestellt werden)

96 % der Unternehmen haben Probleme bei der Verwaltung von Daten in Public- und Multi-Cloud-Umgebungen.

44 % haben mit der Komplexität zu kämpfen, die mit der Navigation durch mehrere Public-Cloud-Plattformen verbunden ist, von denen jede ihre eigenen Funktionen und Anforderungen hat.

40 % äußern Bedenken hinsichtlich der Sicherheit ihrer Daten in diesen vielfältigen Umgebungen.

Sicherung einer Multi-Cloud-Umgebung

Angesichts der zunehmenden Cyberbedrohungen fehlt vielen Unternehmen das Vertrauen in die Sicherheit ihrer Daten in der Cloud, insbesondere bei der Bereitstellung neuer Anwendungen und der Aktualisierung bestehender Anwendungen. Tatsächlich ist ihr Vertrauen auf einem historischen Tiefstand.

Prozentsatz der Befragten, die nicht „sehr zuversichtlich“ sind, dass ihr Unternehmen in der Lage ist, alle Daten in Public-Cloud-Umgebungen zu schützen

Es ist verständlich, dass mehr als die Hälfte der Befragten zwei Fähigkeiten als entscheidend für einen effektiven Hybrid- und Multi-Cloud-Betrieb einstuft:

58 %

Die Fähigkeit, Umgebungen mit mehreren Workloads zu schützen

56 %

Sicherstellen einer robusten Cybersicherheit

50 %

Um diese Herausforderungen zu bewältigen, hat die Hälfte der Unternehmen bereits externen Support in Anspruch genommen, um ihre Ausfallsicherheit bei Cyberangriffen zu verbessern.

Fazit

Da Unternehmen zunehmend auf Public-Cloud-Lösungen zurückgreifen, hybride Arbeitsmodelle implementieren und mit generativer KI experimentieren, wird die Bedeutung der Data Protection deutlicher denn je. Dennoch wird die Sicherung und der Schutz digitaler Ressourcen für viele zu einer immer komplexeren Herausforderung. In einer Landschaft, die ständig von Cyberangriffen bedroht ist, ist es für Unternehmen unerlässlich, Maßnahmen zu ergreifen, die die Ausfallsicherheit ihres Betriebs stärken.

Erfahren Sie mehr über die moderne, einfache und robuste Multi-Cloud-Data-Protection von Dell: **www.dell.com/dataprotection**

DELL Technologies

Dell Technologies bietet Cyber Recovery, Backup, Disaster Recovery, langfristige Aufbewahrung und mehr, um Sie beim Schutz Ihrer Daten und Anwendungen zu unterstützen.

VansonBourne

Vanson Bourne ist ein unabhängiger Marktforschungsspezialist für den Technologiesektor. Seinen Ruf für solide und glaubwürdige forschungsbasierte Analysen verdankt das Unternehmen seinen fundierten Forschungsprinzipien und der Fähigkeit, die Meinungen führender Entscheidungsträger in den verschiedenen technischen und betrieblichen Kompetenzbereichen in allen Geschäftszweigen und größeren Märkten einzuholen.
www.vansonbourne.com