Die Herausforderungen im Bereich der Data Protection und die damit verbundenen Unterbrechungen nehmen ständig zu, wobei Public Clouds und Cyberangriffe besonderen Anlass zur Sorge geben. Unternehmen, die in Bezug auf die Data Protection jedoch kontinuierlich auf dem neuesten Stand bleiben, können Risiken minimieren und sich sorgenfreier ihrer digitalen Transformation widmen.

Data-Protection-Maßnahmen sowie Zweifel an ihrer Effizienz machen Unternehmen angreifbar.

Weit verbreitete Bedenken hinsichtlich existierender

65 % 77 %

sind nicht davon überzeugt, dass ihr Unternehmen die

Servicelevelziele für Backup und Recovery erfüllt.

0101010101010101

fürchten, dass in den nächsten zwölf Monaten ein Ereignis eintreten wird,

das zu größeren Unterbrechungen im Betrieb führen wird.

סוסוסימימוסוסו 01011 × 10101 010101010101010101 1010101010101010 **2,21** TB an Daten sind im Durchschnitt in den vergangenen zwölf Monaten verloren

gegangen, was im Durchschnitt zu Kosten in Höhe von ca. 2,80 Millionen USD geführt hat.

Cyberangriffe sind eine



Recovery-Maßnahmen infiziert oder beschädigt werden könnten.

wachsende Bedrohung. 54 %

allgegenwärtige und ständig

berichten, dass ihr Unternehmen in den letzten zwölf Monaten

Opfer eines Cyberangriffs oder eines damit verbundenen Vorfalls war. Dies hat **Unternehmen im Durchschnitt** 2,42 Millionen USD gekostet.





existierenden Data-Protection-Maßnahmen in ihrem Unternehmen nicht ausreichen, um

befürchten, dass die

Malware- und Ransomware-Bedrohungen effektiv zu bewältigen. Künstliche Intelligenz kann Unternehmen dabei unterstützen, die Ausfallsicherheit bei Cyberangriffen

auf die Data Protection.

sind nicht davon

überzeugt, dass alle

geschäftskritischen

Daten im Falle eines

zerstörerischen

اماماماه

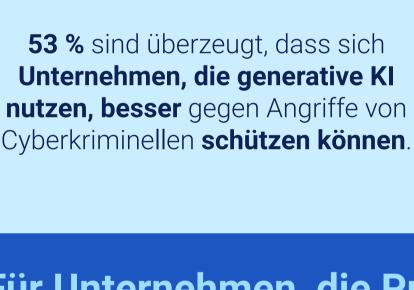
Cyberangriffs wiederhergestellt werden können.



Cyber Recovery.

berichten, dass ihr Unternehmen in KI-Technologie investiert, um sich besser vor Angriffen zu schützen.

zu erhöhen, allerdings bestehen Bedenken in Bezug



Anliegen.

83 %

aller AnwenderInnen, die



Hybrid- oder Public-Cloud-Umgebungen für Updates oder die Bereitstellung von Anwendungen nutzen, sind nicht davon **überzeugt**, dass ihr Unternehmen sämtliche Daten in ihren Public Clouds effektiv schützen kann.



Für die Mehrheit der Befragten waren die

folgenden Faktoren bei der Nutzung von

Hybrid- und Multi-Cloud-Umgebungen

am wichtigsten:

Schutz von Multi-

Sicherstellung von

Cybersicherheit

Workload-Umgebungen

Zum Schutz ihrer Workloads und zur Sicherstellung regelmäßiger Backups benötigen viele Unternehmen Unterstützung von außen.



Dell Technologies bietet Ihnen eine umfassende Lösung für Cyber Recovery, Backup, Disaster Recovery, langfristige Aufbewahrung und vieles mehr, damit Sie all Ihre

Daten und Anwendungen effektiv schützen können. Erfahren Sie mehr über die modernen, unkomplizierten und ausfallsicheren Data-Protection-Lösungen für die

D¢LLTechnologies

Multi Cloud von Dell: Die Studie wurde von September bis Oktober 2023 von Vanson Bourne durchgeführt. Dabei wurden IT-Teams und EntscheidungsträgerInnen im Bereich IT-Sicherheit aus privaten und öffentlichen Unternehmen mit mehr 250 MitarbeiterInnen befragt. Insgesamt wurden 1.500 TeilnehmerInnen aus vier Regionen befragt: 300

Singapur und Südkorea) und 150 aus China.

aus Nord-, Mittel- und Südamerika (USA, Mexiko und Brasilien), 675 aus der Region EMEA (Großbritannien, Frankreich, Deutschland, Italien, Südafrika und VAE), 375 aus der Region APJ (Australien, Indien, Japan,

Im Auftrag von Dell Technologies Quelle: Dell Technologies Innovation Index, Oktober 2023. Copyright © Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein Intel, das Intel Logo und andere Intel Marken sind Marken der Intel Corporation oder deren Tochtergesellschaften. Andere Namen und Marken können das Eigentum anderer Inhaber sein.