

Herausforderung Backup-Strategie

# Welchen Datenverlust kann sich Ihr Unternehmen leisten?

Durch die steigende Komplexität der IT müssen bestehende Backup-Architekturen auf den Prüfstand und angepasst werden. Nur so lassen sich die Anforderungen bei Design, Performance, Robustheit, Ransomware-Schutz, Cyberresilienz und Wiederherstellung im Katastrophenfall bewältigen.

In einer Zeit, in der Cyberangriffe, Ransomware, Datenlecks und Systemausfälle immer häufiger und raffinierter werden, stehen Unternehmen vor enormen Herausforderungen. Die Bedrohungen sind vielfältig – von gezielten Hackerangriffen über unabsichtliche Datenverluste bis hin zu großflächigen Systemausfällen. Zugleich steigen die Anforderungen an Compliance und Datenschutz kontinuierlich, getrieben durch strenge gesetzliche Vorgaben wie die Datenschutzgrundverordnung (DSGVO) und die neue NIS2-Richtlinie, die nun in der gesamten EU umgesetzt wird. Diese Entwicklungen zwingen Unternehmen, ihre Backup-Strategien zu überdenken und anzupassen. Die Frage, wie ein möglicher Datenverlust verhindert oder minimiert werden kann, ist angesichts dieser Entwicklungen relevanter denn je. Es hat sich bewährt, folgende Aspekte bei der Betrachtung zu berücksichtigen.

#### # Cloud-Backups und hybride Ansätze.

Cloud-Backups haben sich als eine effektive Methode zur Datensicherung etabliert. Unternehmen nutzen zunehmend Infrastructure-as-a-Service (IaaS) und Software-as-a-Service (SaaS), auch um Daten sicher zu speichern und wiederherzustellen. Hybride Backup-Szenarien, die sowohl On-Premises- als auch Cloud-Lösungen integrieren, bieten dabei zusätzliche Flexibilität und Sicherheit. Allerdings erhöhen diese hybriden Ansätze die Komplexität der Backup-Infrastruktur erheblich und erfordern ein Umdenken bei traditionellen Backup-Konzepten.

#### # Ausfall-Rechenzentrum in der Public Cloud.

Dieser Ansatz ermöglicht es Unternehmen, im Katastrophenfall schnell auf eine meist vollständig replizierte IT-Infrastruktur zuzugreifen. Diese Strategie minimiert Ausfallzeiten und stellt sicher, dass geschäftskritische Prozesse nahezu ohne Unterbrechung weiterlaufen können. Doch muss dieses Szenario ebenfalls in ein gesamtheitliches Backup- und Recovery-Konzept eingebunden werden. Alle technischen und organisatorischen Maßnahmen zum Schutz von IT-Systemen und Daten vor Verlust oder Missbrauch müssen entsprechend angepasst werden.

#### # Backup von SaaS-Daten.

Mit der wachsenden Nutzung von SaaS-Diensten wie Microsoft 365 kommt das Shared-Responsibility-Konzept ins Spiel. Dieses Konzept besagt, dass Cloud-Anbieter zwar für die Infrastruktur sorgen, die Verantwortung für die Datensicherung jedoch beim Nutzer liegt. Dies erfordert eine klare Definition von Backup- und Aufbewahrungsrichtlinien sowie die Implementierung von rollenbasiertem Zugriff und Zero-Trust-Sicherheitsmodellen, um unbefugten Zugriff zu verhindern.

#### # Datensicherung für Container-Umgebungen.

Container-Technologie ist inzwischen in den meisten Unternehmen ein fester Bestandteil der produktiven IT-Systeme. Allerdings stellt die Sicherung von Daten in Container-Umgebungen eine besondere Herausforderung dar. Hier

**\*1** In der Praxis sind manuelle Sicherungs- und Wiederherstellungsprozesse immer noch anzutreffen – diese sind eine zuverlässige Quelle für Fehler mit schwerwiegenden Folgen.

sind automatisierte, regelmäßige Backups sowie das sichere Speichern von Backups getrennt vom Cluster essenziell. Zudem sollten Namespaces separat gesichert werden, um eine bessere Granularität bei der Datenwiederherstellung zu gewährleisten. Regelmäßige Prüfungen der Wiederherstellbarkeit sind natürlich auch in Container-Umgebungen unerlässlich, damit im Ernstfall schnell und zuverlässig reagiert werden kann.

#### # Ransomware-Schutz und Cyberresilienz.

Ransomware-Angriffe sind eine der größten Bedrohungen für Unternehmen. Immutable Backups, die nach dem Schreiben nicht mehr verändert werden können, und Air-Gapped-Backups, die physisch oder logisch vom Netzwerk getrennt sind, bieten hier effektiven Schutz. Zusätzlich sollten Unternehmen ihre Backups durch automatisierte Cyber-Detection-Scans sichern und regelmäßig die Wiederherstellbarkeit der Backups prüfen, um im Ernstfall vorbereitet zu sein.

#### # Edge-Backups.

Mit der zunehmenden Verbreitung des Internet of Things (IoT) und von Edge-Computing müssen Backup-Lösungen auch Daten an den Netzwerkrändern erfassen und sichern. Dies erfordert robuste Backup-Lösungen, die mit dezentralisierten Datenquellen umgehen können.

#### # Automatisierung und Orchestrierung.

In der Praxis sind manuelle Sicherungs- und Wiederherstellungsprozesse immer noch anzutreffen – diese sind eine zuverlässige Quelle für Fehler mit schwerwiegenden Folgen. Darüber hinaus wirken sich diese Verfahren negativ auf die Häufigkeit und Qualität der Wiederherstellungstests aus. Automatisierte Backup-Prozesse und Orchestrierungs-Tools helfen, die Verwaltung komplexer Backup-Umgebungen zu erleichtern. Diese Tools minimieren menschliche Fehler und verbessern die Konsistenz und Zuverlässigkeit der Datensicherungen.

**\*|** Bestehende Backup-Architekturen müssen regelmäßig geprüft werden, um sicherzustellen, dass sie den aktuellen Anforderungen hinsichtlich Design, Performance, Robustheit, Ransomware-Schutz und Cyberresilienz gewachsen sind.

#### **# Künstliche Intelligenz und maschinelles Lernen.**

Der Einsatz von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) ermöglicht die Optimierung von Backup-Strategien. Diese Technologien können Anomalien erkennen, potenzielle Probleme vorhersagen und somit die Gesamteffizienz und Sicherheit der Backup-Prozesse steigern. Perspektivisch wird so ein KI-gestützter adaptiver Datenschutz möglich, bei dem ungewöhnliche Aktivitäten zusätzliche Schutzmaßnahmen auslösen.

#### **# Kostenoptimierung und Effizienz.**

Natürlich muss auch die Kosten- und Effizienz-Frage mit Blick auf Backup-Architekturen immer wieder gestellt werden. Backup-Lösungen, die deduplizierte und komprimierte Daten speichern, sind für Unternehmen von großer Bedeutung. Diese Lösungen helfen, Speicherkosten zu senken, ohne Kompromisse bei der Datensicherheit oder -verfügbarkeit einzugehen.

**Fazit.** Die Komplexität in der IT und die Datenmenge nehmen kontinuierlich zu, insbesondere in hybriden Umgebungen. Heutige Workloads sind vielfältig, dynamisch und werden nicht mehr nur an einem zentralen Rechenzentrum betrieben. Bestehende Backup-Architekturen müssen daher regelmäßig geprüft werden, um sicherzustellen, dass sie den aktuellen Anforderungen hinsichtlich Design, Performance, Robustheit, Ransomware-Schutz und Cyberresilienz gewachsen sind. Besonders wichtig ist auch die Fähigkeit zur schnellen und zuverlässigen Wiederherstellung im Katastrophenfall.

Wichtige Fragen, auf die Sie in diesem Zusammenhang eine Antwort haben sollten:

- #** Ist Ihr Backup- und Wiederherstellungs-Konzept den Herausforderungen in modernen, hybriden IT-Umgebungen gewachsen?

- #** Welchen Datenverlust kann sich Ihr Unternehmen leisten?

- #** Verfügen Sie über wirksame Maßnahmen für Ransomware-Schutz und Cyberresilienz?

- #** Werden Sie von Ihrer Backup-Lösung im täglichen Betrieb angemessen unterstützt – durch Automatisierung, Orchestrierung, maschinelles Lernen oder künstliche Intelligenz?

Hilfreich ist hier ein praxisorientierter Workshop mit erfahrenen IT-Spezialisten, in dem unter anderem diese Fragen detailliert geklärt werden. Zielsetzung eines solchen Workshops ist die Entwicklung eines modernen Backup-Konzepts, das Ihre bestehende Backup-Umgebung für die aktuellen Herausforderungen rüstet – und mögliche Datenverluste im Katastrophenfall vermeidet oder zumindest reduziert. Die Frage, welchen Datenverlust sich ein Unternehmen leisten kann, sollte dabei stets im Mittelpunkt stehen.

Die Controlware-Experten aus dem Bereich Data Center & Cloud unterstützen Sie in allen Belangen einer modernen Backup-Infrastruktur. Vordefinierte Consulting Pakete, wie Health Checks oder moderne Backup-Konzepte, erlauben einen praxisnahen, pragmatischen »Kickstart«. So können Sie zügig die ersten Vorteile einer Modernisierung nutzen. Darauf aufbauend entsteht zudem eine klare Roadmap für die weitere Entwicklung einer tragfähigen Backup- und Recovery-Strategie in Ihrem Unternehmen.



Adam Hufnagel,  
Team Lead Business Development  
Data Center & Cloud,  
Controlware GmbH  
[www.controlware.de](http://www.controlware.de)  
[blog.controlware.de](http://blog.controlware.de)