Backup and Recovery | 5 Min. Lesezeit

Wie Sie Datensicherheit auch in Zeiten von Cyberangriffen gewährleisten.

Maschinen können ausfallen, Mitarbeiter krank und Kunden zahlungsunfähig werden. Das alles ist unglücklich, aber meist keine Katastrophe. Anders sieht es aus, wenn Ihre gesammelten digitalen Unternehmensdaten plötzlich nicht mehr verfügbar sind. Dann drohen im schlimmsten Fall Geschäftsausfälle mit teilweise massiven Umsatzeinbußen. Und dieser Fall tritt immer häufiger ein, weil die Bedrohungen zunehmen und viele Betriebe keine vollständig integrierte Backup-Strategie ihrer Daten haben. Damit Ihnen das nicht passiert, erfahren Sie in diesem offline Blogartikel alles über die vielfältigen Ursachen für Datenverluste und wie Sie sich mit effizienten und intelligenten Backup- und Recovery-Lösungen wirksam davor schützen können.

IT for innovators.

3 Herausforderungen der Datensicherung: Cyberattacken, steigende Cloud-Komplexität und Backup-Parallelitäten - darauf müssen Sie achten

Es gibt unzählige Möglichkeiten, warum Daten plötzlich nicht mehr verfügbar sind oder ganze Serversysteme ausfallen. Naturkatastrophen und Gebäudebrände zählen seit jeher dazu. Vergleichsweise neu und um ein Vielfaches wahrscheinlicher sind heute dagegen die Bedrohungen durch Cyberkriminalität.

1. Datenverluste durch Cyberattacken – fast so gewöhnlich wie ein Schnupfen

Cyberkriminalität hat enorm zugenommen. Ablesen lässt sich dies an den Ausgaben für Cybersecurity in Unternehmen. So hatte der globale Markt 2004 gerade mal einen Wert von rund 3,5 Millionen US-Dollar. Inzwischen gehen Experten für den Zeitraum von 2021 bis 2025 von weltweiten Cybersecurity-Investitionen in Höhe von 1,75 Billionen US-Dollar aus. Die am schnellsten wachsende Kriminalitätsform sind Ransomware-Attacken. 2021 wurde alle 11 Sekunden ein Unternehmen angegriffen, 2019 lag die Frequenz noch bei 14 Sekunden. Viele dieser Angriffe führen zu Datenverlusten. Mehr noch: Bei über 40 Prozent der betroffenen Unternehmen konnten die Daten nicht wiederhergestellt werden. Diese alarmierenden Zahlen verdeutlichen: Datenverluste durch Hackerangriffe sind heute fast so gewöhnlich wie ein Schnupfen. Mit einem Unterschied: Die Folgen können weitaus dramatischer sein. Dies bestätigt etwa der Digitalverband Bitcom, der nach einer Erhebung im Sommer 2021 allein für die deutsche Wirtschaft mit Schäden in Höhe von jährlich 223 Milliarden Euro rechnet.

2. Datensicherung ist eine schnell wachsende und zunehmend komplexe Herausforderung

Die Unternehmen sind sich der Risiken bewusst. Auf die Frage nach drängenden und für den weiteren digitalen Wandel entscheidenden Aufgaben nannten laut IDC-Studie über 90 Prozent der befragten Firmen die Modernisierung der eigenen Datensicherheit inklusive Datensicherung und Wiederherstellung. Folgerichtig planen laut IDC-Studie 52 Prozent der Teilnehmer bereits konkret, Zeit und Geld in ihre Datensicherungs- und Wiederherstellungspläne zu investieren.

Bleibt die Frage, wie es zu diesem hohen Handlungsbedarf kommen konnte? Die Antwort ist vielschichtig. Eine zentrale Rolle spielt das dynamisch steigende Datenvolumen. So prognostiziert etwa das Institut der Deutschen Wirtschaft (IDW) mit dem Hinweis auf eine Studie der International Data Corporation eine Explosion der weltweiten Datenmenge von etwa 33 Zettabyte im Jahr 2018 auf 175 Zettabyte bis 2025. Dies, so das IDW, bedeute Steigerungsraten von jährlich 27 Prozent! Im gleichen Tempo müsste auch die Soft- und Hardware für die Datensicherung wachsen. Eine Herausforderung, die nicht nur an den Budgets, sondern auch an fehlen-

Das erfahren Sie in 5 Min.

- **3 Herausforderungen der Datensicherung:** Cyberattacken, Cloud-Komplexität und Backup-Parallelitäten - darauf müssen Sie achten
- **Das Ziel:** Die eigene IT-Resilienz systematisch stärken und sich wirksam gegen Datenverluste absichern
- **Die Lösung:** Aufbau einer individuell abgestimmten Backup- und Recovery-Architektur nach Best Practice
- **Fazit**

Stefan Richter
Backup-Experte bei
ACP IT Solutions AG

den Backup-Spezialisten und Personalressourcen scheitert.

3. Backup-Risiken lauern in der Parallelität von Cloud-, On-Premise- und Hybrid-Strukturen

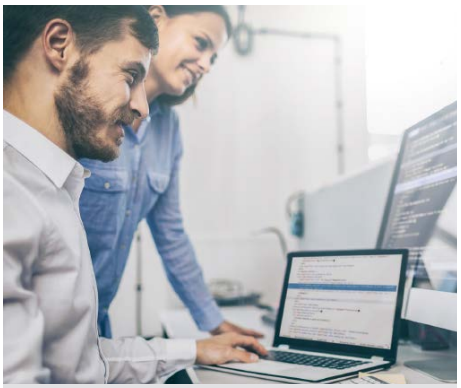
Durch die Mobilisierung der Arbeit in den vergangenen zwei Jahren und die Zunahme der Homeoffice-Tätigkeit sind viele Anwendungen nicht mehr On-Premise angesiedelt, sondern in der Cloud.

Als Beispiel sei hier nur die Microsoft Office 365-Suite genannt: Standard-Anwendungen wie Excel, PowerPoint oder Outlook liegen nicht mehr auf unternehmenseigenen Servern, sondern – genau wie die mit diesen Office-Apps tagtäglich produzierten Daten – in der Cloud. Viele IT-Verantwortliche gehen davon aus, dass Ihre Daten in der Microsoft-Cloud sicher sind und sich im Störfall jederzeit wiederherstellen lassen. Dies ist ein Irrglaube. Microsoft übernimmt die Verantwortung für das Erstellen und Pflegen von Backups nicht.

Hinzu kommt: Durch den sprunghaft steigenden Backup-Aufwand muss oft schnell in neue Hard- und Software investiert werden. Dabei werden vorhandene und neue Systeme nicht immer konsequent verbunden. Zudem laufen einige Anwendungen und Datenspeicher nach wie vor On-Premise, andere befinden sich in eigenen oder Drittanbieter-Clouds, weitere dezentrale Infrastrukturen kommen durch Edge-Computing hinzu. Um auf der sicheren Seite zu sein, müssten all diese Inseln in eine einzige umfassende Backup-Lösung eingebunden werden. Die Realität sieht anders aus: Viele Unternehmen produzieren immer neue Daten- und Backupsilos. Ganzheitliche und intelligente Backup- und Recovery-Lösungen fehlen.

Das Ziel: Die eigene IT-Resilienz systematisch stärken und sich wirksam gegen Datenverluste absichern

Die Folgen einer fehlenden ganzheitlichen Backup- und Recovery-Lösung können verheerend sein. Unternehmen haben oft eine Patchwork-Lösung, die essenzielle Anforderungen nicht erfüllt und kritische Lücken in der Datensicherung lässt. Dies kann dazu führen, dass die Wiederherstellung geschäftskritischer Systeme, Anwendungen und Daten im Ernstfall scheitert oder sehr viel mehr Zeit und Aufwand kostet als geplant. Wie wichtig der Faktor Zeit ist, zeigt etwa eine US-amerikanische Studie. Demnach haben 93 Prozent der befragten Unternehmen, bei denen der Datenzugriff durch Datenlecks für zehn oder mehr Tage ausfiel, das folgende Geschäftsjahr nicht überstanden. Dies bedeutet im Umkehrschluss: Unternehmen, die ihre Daten und IT-Systeme schnell wiederherstellen können, sind widerstandsfähiger und überstehen IT-Ausfälle und Datenverluste besser.



Wie widerstandsfähig ist Ihre IT?

Lassen Sie es auf einen Test ankommen! Unsere Experten beraten Sie mit dem IT-Check für den Mittelstand.

Vereinbaren Sie jetzt direkt einen Termin!

ZUM IT-CHECK

KONTAKT AUFNEHMEN

ACP IT Solutions AG
+49 40 8090776 77
acp.nord@acp.de
www.acp.de

Ist diese Basis erstmal geschaffen, stellt sich bei einem Ausfall wichtiger Clouddienste oder zentraler Teile der IT-Infrastruktur die alles entscheidende Frage: Wie lange dauert es, den Normalbetrieb wiederherzustellen? Je schneller dies gelingt, desto besser. Wo die Daten und Systeme laufen ist zweitrangig. Entscheidend ist eine gute Vorbereitung. Um sie zu gewährleisten, sollten Unternehmen einen Notfallwiederherstellungsplan entwickeln. Dieser umfasst sowohl organisatorische als auch technische Maßnahmen. Obligatorisch sind eine unternehmensspezifische Risikobewertung im Vorfeld, der Aufbau eines Reaktionsplans sowie geeignete Versicherungsdeckungen. Ebenfalls die Einrichtung und Dokumentation von Notfallkontakten in physischer Form sowie eine strategisch durchdachte Kommunikationsstrategie.

Wichtig: Im Ernstfall kommt es darauf an, schnell wieder auf wichtige Daten und Informationen zugreifen und den Geschäftsbetrieb fortführen zu können.

Doch was bedeutet schnell?
Folgende Kennzahlen definieren die Stellgrößen:

- **Recovery Point Objective (RPO):** RPO beschreibt den Zeitraum, der zwischen dem letzten durchgeführten Backup und dem Eintritt des Störfalls liegt.
- **Recovery Time Objective (RTO):** RTO ist die strategisch definierte Zeitspanne, innerhalb derer betroffene Daten und Dienste wiederhergestellt sein müssen.
- **Recovery Time Actual (RTA):** RTA ist die Zeitspanne, die tatsächlich vergeht, bis alle Daten vollständig wiederhergestellt und für Anwendungen zugänglich sind.

Im Idealfall hätten alle drei Kennzahlen den Wert null. Praktisch ist das nicht erreichbar. Ziel ist es jedoch, die Wiederherstellungszeiten mit wirtschaftlich vertretbarem Aufwand so weit wie möglich zu reduzieren. Der Schlüssel dazu sind individuell abgestimmte Datensicherungs- und Wiederherstellungsprozesse auf ständig neuestem Stand der Technik.

Die Lösung: Aufbau einer individuell abgestimmten Backup- und Recovery-Architektur nach Best Practice

Der Aufbau und die stetige Weiterentwicklung individueller Backup- und Recovery-Lösungen ist für viele Betriebe in Eigenregie kaum zu stemmen. Dafür fehlen Inhouse meist die nötigen Experten und Personalkapazitäten. Zudem wären angesichts des schnellen Datenwachstums regelmäßig hohe Investitionen in neueste Hard- und Software sowie in die Auslegung und Administration der Backup-Infrastruktur erforderlich.

„Unsere Zusammenarbeit mit ACP ist von Vertrauen und Offenheit geprägt. Wir pflegen ein produktives Miteinander, das ich in jeder Hinsicht schätze. Auf einer Skala von 1 bis 5 gibt es von mir 5 Sterne für die Zusammenarbeit."

Sven Kückmann
Teamleiter IT, Bette GmbH & Co. KG

ZUR SUCCESS-STORY

Wie sich die eigene Datensicherheit nachhaltig und systematisch verbessern lässt?

Wir empfehlen:

- Eine **individuell kalibrierte Backup- und Recovery-Lösung**, die eine ebenso kosteneffiziente wie bedarfsgerechte Datenarchivierung gewährleistet.
- **Schnelle, zuverlässige Wiederherstellungsprozesse**, welche die Resilienz des Unternehmens stärken.
- Integration eines **Notfall-Wiederherstellungsplans**.
- Zuverlässige **Hard- und Softwarelösungen von Technologieführern** wie Hewlett Packard Enterprise und Veeam.
- **Externe Backup- und Speicherkapazitäten** in ISO 27001-zertifizierten Rechenzentren in Deutschland

Fazit

Sollten Sie sich jetzt fragen, woher Sie die Experten und Personalkapazitäten für den Aufbau einer solchen Backup- und Recovery-Lösung bekommen und wie Sie das Ganze finanzieren, haben wir abschließend noch einen Tipp: ACP IT Solutions bietet dafür ein umfassendes Portfolio an Managed Services an. Das Spektrum reicht von Storage-Konzepten für die Datensicherung vor Ort, etwa auf Basis von HPE StoreOnce-Technologien, bis hin zu verschiedenen Veeam-basierten Cloud-Backup-Lösungen. Darunter zum Beispiel Managed Backup für Office 365, Managed Cloud Backup oder Managed Cloud Replication.

Partner

Hewlett Packard Enterprise

VEEAM

Wie Sie Ihre Backup- und Recovery-Strategie schnell und effektiv optimieren? Wir beraten Sie gerne in einem kostenlosen Experten-Gespräch.

Sprechen Sie uns an!

ACP IT Solutions AG
+49 40 8090776 77
acp.nord@acp.de
www.acp.de