

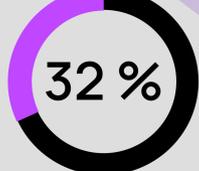
# 7

## Gründe für den Backup von Microsoft-365-Daten

Immer mehr Unternehmen nutzen Microsoft 365™ für E-Mail, Datenspeicherung und Produktivität. Vielen sind die Lücken dieser Lösung bei der Datenaufbewahrung jedoch nicht bewusst.

Um Ihr Team zufriedenzustellen und Ihre Daten abzusichern, sollten Sie sich um eigene Backups kümmern.

### Datenverlust in Zahlen



der Unternehmen haben schon einmal Daten aus SaaS-Anwendungen verloren<sup>1</sup>



der IT-Verantwortlichen halten Verluste von Microsoft-365-Daten durch das Arbeiten in Remote- und Hybrid-Umgebungen künftig für wahrscheinlicher<sup>2</sup>

4,24 Mio. \$

4,24 Millionen US-Dollar kostet durchschnittlich ein Datenschutzverstoß<sup>3</sup>

### Sogar Microsoft selbst empfiehlt einen Backup:

Es wird empfohlen, die **Inhalte und Daten** **regelmäßig zu sichern, die Sie in den Diensten oder während der Verwendung von Drittanbieter-Apps und -Diensten speichern.**<sup>4</sup>

- Microsoft-Servicevertrag<sup>4</sup>

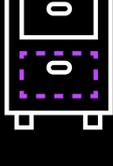
### Und warum?

#### Aus diesen 7 Gründen:



#### Versehentliches Löschen:

Benutzer können versehentlich freigegebene OneDrive® -Ordner, ihren Posteingang oder SharePoint® -Websites löschen. Microsoft 365 Business Standard bewahrt Daten standardmäßig nur 14 Tage lang auf (verlängerbar auf 30 Tage).



#### Aufbewahrungslücken:

Daten ausscheidender Mitarbeiter werden gelöscht, sobald das zugehörige Konto gelöscht wird. Um diese Daten zu erhalten, müssen Sie das Konto gebührenpflichtig erhalten oder die Daten rechtzeitig in ein freigegebenes Postfach überführen.



#### Insider-Bedrohungen:

Benutzer können große Datenbestände löschen, indem sie versehentlich einen schädlichen Link anklicken oder gezielt in böser Absicht handeln. Geschieht dies am Ende des Aufbewahrungszeitraums, sind die Daten für immer verloren.



#### Externe Bedrohungen:

Hacker können Microsoft-365-Konten angreifen – entweder gezielt oder im Rahmen größerer Aktionen – und darin befindliche Daten verschlüsseln oder löschen.



#### Rechtliche Vorgaben und Compliance:

Wie lange Daten mindestens aufbewahrt werden müssen, ist gesetzlich geregelt; die HIPAA-Vorgaben in den USA sehen beispielsweise Fristen von bis zu sechs Jahren vor. Ohne entsprechendes Microsoft-365-Abonnement verstoßen Sie also schnell gegen Gesetze.



#### Weniger Kontrolle:

Im Fall eines Datenverlusts sind Sie auf die Unterstützung von Microsoft angewiesen. Doch ob die Daten wiederbeschafft werden können, hängt davon ab, wie lange der Vorfall zurückliegt. Mit einer eigenen Dateninstanz durch eine externe Backup-Lösung erhalten Sie mehr Kontrolle und stellen Ihre Kunden zufrieden.



#### Kosten:

Die Preise für externe Backup-Lösungen variieren. Nicht bei allen ist ein Backup-Speicher in der Cloud inbegriffen. Ideal ist also eine Lösung, deren Festpreis auch Cloud-Speicher beinhaltet.

### N-able™ Backup

#### bietet Ihnen diese (und noch viele weitere) Vorteile:



Daten sieben Jahre lang aufbewahren und Risiken im Zusammenhang mit Compliance, Datenaufbewahrung, versehentlichem Löschen und Angriffen von innen und außen eindämmen



Jederzeit Kontrolle über die Aufbewahrung und Wiederherstellbarkeit der Daten dank eigener Backups.



Rentabler Service: Niedrigere Kosten pro Lizenz als bei anderen Lösungen (inklusive Cloud-Speicher im Basispreis)\*

### Warum etwas riskieren? Sorgen Sie kostengünstig für den Backup von Microsoft-365-Daten

[N-able Backup testen](#)

\* Es gilt unsere Fair-Use-Richtlinie.

1. „The Hidden Dangers of Your Cloud Data“, Jacksonville Business Journals. bizjournals.com/jacksonville/news/2021/06/01/the-hidden-dangers-of-your-cloud-data.html (Zugriff August 2021).

2. „An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches Research by Egress Reveals“, Business Wire. businesswire.com/news/home/20210511005132/en/An-Alarming-85-of-Organizations-Using-Microsoft-365-Have-Suffered-Email-Data-Breaches-Research-by-Egress-Reveals (Zugriff August 2021).

3. „2021 Cost of a Data Breach Report“, IBM und Ponemon Institute. https://www.ibm.com/de-de/security/data-breach (Zugriff August 2021).

4. „Microsoft-Servicevertrag“, Microsoft. https://www.microsoft.com/de-de/servicesagreement/ (Zugriff August 2021).

Dieses Dokument dient nur zu Informationszwecken und stellt keine Rechtsberatung dar. N-able übernimmt weder ausdrücklich noch stillschweigend Gewähr noch Haftung oder Verantwortung für Korrektheit, Vollständigkeit oder Nutzen der in diesem Dokument enthaltenen Informationen.

Mit N-able können IT-Fachleute Unternehmen effektiv bei der Digitalisierung unterstützen. Mit unserer flexiblen Technologieplattform und leistungsstarken Integrationen lassen sich Systeme, Daten und Netzwerke bequem überwachen, verwalten und sichern. Unser wachsendes Portfolio an Sicherheits-, Automatisierungs- sowie Backup- und Wiederherstellungslösungen richtet sich an Fachleute für das IT-Service-Management. N-able vereinfacht komplexe Umgebungen und sorgt dafür, dass Kunden ihre Probleme selbst in die Hand nehmen können. Wir bieten umfassenden, proaktiven Support in Form von praktischen Schulungen und Ressourcen. So können Sie hochwertige Services liefern und Ihren Erfolg ausbauen. n-able.com/de

N-ABLE, N-CENTRAL und andere Marken und Logos von N-able sind ausschließlich Eigentum von N-able Solutions ULC und N-able Technologies Ltd. Sie sind gesetzlich geschützte Marken und möglicherweise beim Patent- und Markenamt der USA und in anderen Ländern registriert oder zur Registrierung angemeldet. Alle anderen hier genannten Marken dienen ausschließlich zu Informationszwecken und sind Marken (oder registrierte Marken) der entsprechenden Unternehmen.

© 2022 N-able Solutions ULC und N-able Technologies Ltd. Alle Rechte vorbehalten.