

Sechs kostspielige Data Protection-Lücken in Microsoft 365 und wie man sie schließt

Wenn Sie Microsoft 365 nutzen, können Sie sich auf einen zuverlässigen Zugriff auf die enthaltenen Applikationen mit sehr hoher Verfügbarkeit verlassen. Microsoft hat einen ausgezeichneten Ruf, was die Verfügbarkeit und den Betrieb seiner eigenen Cloud-Infrastruktur betrifft, übernimmt jedoch keine Verantwortung für den Schutz der Microsoft 365-Daten. Tatsächlich empfiehlt Microsoft sogar ausdrücklich, dass Benutzer:innen selbst ihre Daten mit Backup-Apps oder Backup-Diensten von Drittanbietern schützen. Um den Microsoft-Servicevertrag zu zitieren: „Wir bemühen uns, die Dienste am Laufen zu halten; alle Online-Dienste sind jedoch gelegentlich von Unterbrechungen und Ausfällen betroffen, und Microsoft haftet nicht für Unterbrechungen oder Verluste, die Ihnen infolgedessen entstehen. Im Fall eines Ausfalls oder einer Unterbrechung des Dienstes **sind Sie möglicherweise vorübergehend nicht in der Lage, Ihre Inhalte abzurufen. 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“.

Dennoch glauben viele Unternehmen immer noch, dass Microsoft für Microsoft 365 eine umfassende Data Protection und langfristige Datenaufbewahrung bietet, obwohl es in Wirklichkeit wenig oder gar keinen Schutz vor den häufigsten Ursachen für folgenschwere Datenverluste wie versehentliches Löschen und Malware-Angriffe bereitstellt. Die Folge dieses Trugschlusses ist eine Data Protection-Lücke, die in vielen Unternehmen zu unangenehmen Überraschungen führen kann. IT-Verantwortliche müssen sich ihrer Verantwortung für den Schutz der Microsoft 365-Daten ihres Unternehmens bewusst sein und eine umfassende Backup-Lösung implementieren, um sich vor den gängigsten Ursachen für Datenverlust zu schützen.

Sechs wichtige Bereiche, die jedes Unternehmen beim Schutz von Microsoft 365-Daten berücksichtigen sollte

1. Versehentliche Löschung von Daten

Datenrisiko: Im Rahmen ihrer täglichen Arbeit löschen Mitarbeitende regelmäßig Microsoft 365-Daten wie Benutzerprofile, E-Mails und Anhänge aus Exchange Online, Dateien aus OneDrive for Business oder Online-Inhalte aus Teams und SharePoint. Diese Löschungen können versehentlich passieren oder absichtlich erfolgen und später bereut werden. In beiden Fällen kann es zum Verlust wichtiger Daten kommen.

Schwachstelle bei Microsoft: Diese Art von Löschvorgängen werden systematisch über das gesamte Netzwerk repliziert. Ältere Daten können sogar vollständig gelöscht werden („hard-deleted“) und sind dann nicht mehr wiederherstellbar. Etwas weniger problematisch sind kürzlich erfolgte Löschungen von neueren Ressourcen, da Dateien/E-Mails, die nur normal gelöscht wurden („soft-deleted“), oft noch aus dem Papierkorb oder dem Ordner „Wiederherstellbare Elemente“ gerettet werden können.

2. Probleme im Zusammenhang mit der Aufbewahrungsrichtlinie

Datenrisiko: Geänderte oder falsche Prioritäten in den Datenaufbewahrungsrichtlinien von Microsoft 365 können dazu führen, dass Daten dauerhaft gelöscht werden. Dieses Risiko kann nur teilweise durch die Überprüfung und Aktualisierung der Aufbewahrungsrichtlinien behoben werden.

Schwachstelle bei Microsoft: Microsoft 365-Kund:innen sind selbst für die Verwaltung der Aufbewahrungsrichtlinien verantwortlich. Kommt es jedoch aus irgendeinem Grund zu einer endgültigen Löschung aufgrund des Ablaufs der

bestehenden Aufbewahrungsrichtlinie, kann Microsoft die gelöschten Inhalte nicht wiederherstellen.

3. Interne Sicherheitsbedrohungen

Datenrisiko: Zusätzlich zu routinemäßigen, nicht böswilligen Löschungen müssen Sie Ihre Daten und Ressourcen in Microsoft 365 auch vor böswilligen Änderungen oder Zerstörungen durch verärgerte oder gekündigte Mitarbeitende, Auftragnehmer oder Partner schützen.

Schwachstelle bei Microsoft: Mit Ausnahme von kürzlich gelöschten Ressourcen bietet Microsoft keinen Schutz vor böswilliger Zerstörung oder Änderung von M365-Daten.

4. Externe Sicherheitsbedrohungen

Datenrisiko: Microsoft 365-Daten sind anfällig für Datenveränderung oder -zerstörung durch verschiedene Malware-Bedrohungen – insbesondere Ransomware, die Benutzerdaten verschlüsselt und für die Freigabe ein Lösegeld verlangt.

Schwachstelle bei Microsoft: Microsoft bietet kaum Schutz vor Angriffen durch Malware (z. B. Ransomware) und nur sehr eingeschränkte Möglichkeiten, verschlüsselte oder veränderte Daten in den Zustand kurz vor einem Malware-Angriff zurückzusetzen.

5. Migration einer lokalen Microsoft Office-Installation

Datenrisiko: Wenn Ihr Unternehmen von einer herkömmlichen, lokal installierten Microsoft Office-Suite zu Cloud-basierten Microsoft 365-Diensten wechselt, muss in der Regel eine veraltete Data Protection-Lösung durch eine neue, Cloud-fähige Lösung ersetzt werden. Diese beiden Backup-Lösungen sind oft nicht kompatibel, sodass es unmöglich ist, Ihre bisherigen Daten in der neuen Umgebung wiederherzustellen.

Schwachstelle bei Microsoft: Microsoft selbst bietet keine Lösung für Datenverluste bei der Migration von Office-Applikationen zu Microsoft 365 an. Nur wenige Data Protection-Lösungen von Drittanbietern integrieren Backup-Funktionen für klassische Office-Applikationen und Microsoft 365, und wenn, dann sind diese Funktionen meist nur für eine der beiden Umgebungen verfügbar (und nicht für beide).

6. Rechtliche Aspekte und Compliance

Datenrisiko: Compliance-Vorschriften und rechtliche Aspekte können die Kosten der oben beschriebenen ungeschützten Datenverluste noch weiter in die Höhe treiben. Ein unwiederbringlicher Verlust von Microsoft 365-Daten kann zu behördlichen oder branchenspezifischen Bußgeldern, Strafen, Umsatz- und Aktienkursverlusten führen, das Vertrauen der Kund:innen erschüttern und den Ruf Ihres Unternehmens schädigen.

Schwachstelle bei Microsoft: In Bezug auf alle oben beschriebenen Datenrisiken kann Microsoft wenig tun, um Unternehmen, die Microsoft 365 nutzen, vor einer Vielzahl von Compliance- und Rechtsverstößen zu schützen. Nach einem Ransomware-Angriff kann ein Unternehmen, das die personenbezogenen Daten seiner in der EU ansässigen Kund:innen in SharePoint Online speichert, Anfragen nach Kopien dieser Daten möglicherweise nicht mehr nachkommen, was einen Verstoß gegen die DSGVO darstellt.

Schützen Sie Ihre Microsoft 365-Daten

Wenn Sie Microsoft 365 nutzen, dann sollten Sie die unzureichende Data Protection von Microsoft mit Acronis Cyber Protect, einer der zuverlässigsten und benutzerfreundlichsten Backup-Lösungen, ergänzen. Acronis Cyber Protect schützt Ihre geschäftskritischen Daten in Microsoft 365 vor bekannten und neuen Bedrohungen mit schnellen Backups, zuverlässigen zeitpunktgenauen Wiederherstellungen, flexiblen Recovery- und Cloud-Storage-Optionen sowie einer Schnellsuchfunktion.

Microsoft gewährleistet die Ausfallsicherheit seiner eigenen Cloud-Infrastruktur, aber der Schutz Ihrer Daten liegt in Ihrer Verantwortung. Führungskräfte aus Wirtschaft und Technologie auf der ganzen Welt vertrauen auf Acronis Cyber Protect, um ihre Microsoft 365-Daten zu schützen und einen ununterbrochenen Geschäftsbetrieb zu gewährleisten.

Möchten Sie mehr über Acronis Cyber Protect erfahren? Testen Sie unsere Lösung noch heute 30 Tage lang kostenlos!

JETZT TESTEN

