CARBONITE

Die Bedeutung von Datensicherung bei Office 365

Entwicklung einer effektiven Strategie zum Schutz von Office 365-Daten

Entwicklung einer effektiven Strategie zum Schutz von Office 365-Daten

Software as a Service-Aanwendungen wie Microsoft Office 365 haben ihren festen Platz in der heutigen mobilen Welt – die Vorteile des einfachen Zugriffs auf Dokumente von jedem beliebigen Gerät aus und der vereinfachten Zusammenarbeit liegen auf der Hand. Viele Unternehmen sind jedoch nach wie vor der Auffassung, dass nach einem Wechsel zu Office 365 keine Datensicherung mehr nötig sei. Einem kürzlich veröffentlichten Bericht der Enterprise Strategy Group zufolge hält eines von vier Unternehmen eine Datensicherung bei Office 365 für nicht notwendig.

Dieser Irrglaube mag zum Teil darauf beruhen, dass Microsoft Office 365 bereits einige Schutzmaßnahmen gegen Datenverlust anbietet. Viele IT-Verantwortliche gehen deshalf einfach davon aus, dass Daten, die sich in der Cloud befinden, automatisch gesichert würden. Wieder andere meinen, die Datensicherung werde durch die Dateisynchronisierung von Microsoft OneDrive ersetzt. Das alles stimmt nicht. Eine Datensicherung ist bei Office 365 genauso wichtig wie bei standortgebundenen Microsoft-Anwendungen.

In diesem eBook lernen Sie die häufigsten Ursachen für einen Datenverlust bei Office 365 kennen, erfahren, warum es nicht ausreicht, sich auf den Papierkorb und dessen Wiederherstellungsoptionen oder auf OneDrive zu verlassen, und was Sie selbst zum Schutz Ihrer geschäftskritischen Office 365-Daten tun können.

Schwachstellen bei Office 365

Die Datensicherungsrichtlinien von Microsoft garantieren keine vollständige und schnelle Wiederherstellung gelöschter oder beschädigter Office 365-Daten. Kurz: Microsoft stellt sicher, dass Ihre Daten nicht verloren gehen. Microsoft sichert Ihnen aber nicht zu, diese Daten wiederherstellen zu können.

Das ist natürlich problematisch. Können geschäftskritische Informationen nicht wiederhergestellt werden, so kann dies zu Umsatzverlusten, Kundenverlust und Rufschädigung führen. Hinzu kommt: Unterliegt Ihr Unternehmen speziellen Datenaufbewahrungspflichten, kann ein Datenverlust sogar rechtliche Konsequenzen haben.

Wie bereits erwähnt, sind Office 365-Daten vielfach genauso gefährdet wie lokal gespeicherte Daten. Werfen wir daher einen Blick auf die häufigsten Schwachstellen:

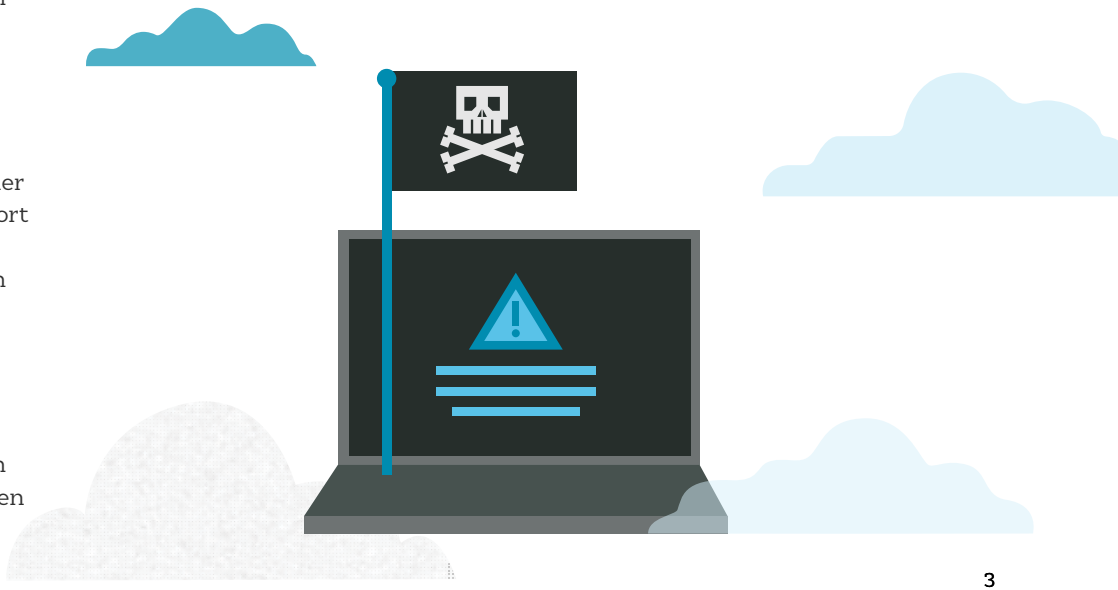
Versehentliches Löschen:
Die erste und naheliegendste Ursache ist das versehentliche Löschen – ein Mitarbeiter löscht aus Versehen eine Datei oder einen Ordner. Nutzer können Daten und Konversationen in SharePoint, Groups oder Teams leicht löschen oder bestehende Versionen überschreiben. Gelöschte Daten sind kein Weltuntergang, wenn man es sofort bemerkt. Man kann sie aus dem Papierkorb heraus wiederherstellen. Der Papierkorb bewahrt gelöschte Dateien jedoch nur für einen begrenzten Zeitraum auf.

Böswilliges Löschen:
In einigen Fällen liegt bei einer Datenlöschung kein Versehen vor. Verärgerte Mitarbeiter können ihre eigenen Dateien oder Dateien in gemeinsam genutzten Ordnern absichtlich löschen, bevor sie das Unternehmen verlassen, oder ein Außenstehender kann über einen gestohlenen Laptop mit schwachem Passwort Zugriff auf Office 365-Daten und -Ordner erlangen. Schlimmstenfalls löscht ein globaler Office 365-Administrator bei seinem Ausscheiden aus dem Unternehmen Nutzerkonten und sperrt alle anderen Administratoren.

Wenn wichtige Dateien aufgrund versehentlichen oder böswilligen Löschens verloren gehen, beeinträchtigt das natürlich die Produktivität. Das ist nicht nur unbequem: Wenn Mitarbeiter ihre täglichen Aufgaben nicht mehr ausführen können, sind Umsatzverluste unweigerlich die Folge. Und wenn Ihr Unternehmen Datenaufbewahrungspflichten unterliegt, kann dies auch rechtliche Konsequenzen nach sich ziehen.

Ransomware (und andere Malware):
Häufig wird irrtümlich angenommen, dass Office 365-Daten vor Ransomware und anderen Arten von Malware sicher seien. Das ist definitiv nicht der Fall. Ransomware kann Office 365-Dateien in der Cloud sperren und damit viele Nutzer beeinträchtigen. Ein mögliches Szenario könnte so aussehen: Ein Nutzer lädt unwissentlich Ransomware auf den Laptop herunter und lokale Dateien werden infiziert.
Falls er die OneDrive-Synchronisierung eingeschaltet hat, werden die infizierten Dateien sofort in die Cloud kopiert. Und damit noch nicht genug: Ransomware ist so konzipiert, dass sie sich in Netzwerken über gemeinsam genutzte Dateien und Ordner ausbreitet. Da OneDrive zur Zusammenarbeit gedacht ist, kann gerade dieses Programm besonders anfällig für derartige Angriffe sein.

Probleme bei der Individualisierung:
Die Individualisierung von Office 365 bietet viele Vorteile. Jedoch erhöhen personalisierte Designs, Lösungen, Workflows, Branding und andere Modifizierungen der Bedienungsoberflächen das Risiko technischer Fehler und Störungen. Schlimmstenfalls muss die Individualisierung eventuell zurückgenommen werden, falls Fehler auftreten. Je nach dem betroffenen System kann ein Datenverlust zu einer Ausfallzeit von Stunden oder sogar Tagen führen.



OneDrive ist keine Datensicherung

Da OneDrive Kopien der Nutzer-Dateien in der Microsoft Cloud speichert, glauben viele IT-Verantwortliche, es könne eine Datensicherung ersetzen. Dabei kann die Nutzung von OneDrive als Datensicherung sogar zu Datenverlusten führen: Falls eine Datei auf einem lokalen Gerät gelöscht oder infiziert wird, wird diese Änderung automatisch in OneDrive synchronisiert. Mit anderen Worten: Die Datei wird auch auf allen synchronisierten Geräten gelöscht oder infiziert.

Die Office 365-Aufbewahrung gibt Unternehmen die Kontrolle darüber, welche Dateien für welchen Zeitraum aufbewahrt werden. Aufbewahrungsregeln können unter anderem auf dem Datum der Erstellung oder der letzten Änderung, dem Dateityp oder auf bestimmten Stichwörtern basieren. Mit ihrer Hilfe können Unternehmen gesetzliche Aufbewahrungspflichten erfüllen und das Risiko von Rechtsstreitigkeiten oder Sicherheitsverstößen mindern. Innerhalb der einzelnen Anwendungen von Office 365 unterscheiden sich die Aufbewahrungseinstellungen jedoch, und einige Apps, z.B. Microsoft Teams, besitzen von Haus aus gar keine Aufbewahrungsfunktionen.

OneDrive bietet einige Wiederherstellungsoptionen über den Papierkorb. Viele Merkmale einer echten Datensicherung fehlen dem Papierkorb jedoch:

- Die Dateiversionen sind keine unveränderlichen, isolierten Wiederherstellungspunkte. Wenn daher eine aktive Datei gelöscht wird, werden auch alle älteren Versionen dieser Datei gelöscht. Werden Dateien dauerhaft aus dem Papierkorb gelöscht, können sie nicht wiederhergestellt werden.
- Der Papierkorb lässt keine zentrale Verwaltung von Nutzerdaten zu. Anders ausgedrückt: Er erlaubt der IT-Abteilung keine Steuerung der Datensicherung und -wiederherstellung.
- Er erstellt keine einheitlichen Wiederherstellungspunkte über Dateien, Ordner und Nutzer hinweg. Somit wird eine umfassende Wiederherstellung im Ernstfall zu einem zeitraubenden, manuellen Prozess. Zum Beispiel muss ein Nutzer bei einer Wiederherstellung nach einem Ransomware-Angriff manuell nach den richtigen Wiederherstellungspunkten suchen und jede Datei einzeln wiederherstellen.

All das erfordert einen manuellen Eingriff und hält die IT-Abteilung und/oder andere Mitarbeiter von ihrer gewohnten Arbeit ab. Wie bereits erwähnt, führen Betriebsausfälle zu Umsatzverlusten.

Entwicklung einer Strategie zum Schutz von Office 365-Daten

Eine Strategie zum Schutz von Office 365-Daten beginnt bei der Schulung der Mitarbeiter. Die meisten Cyberangriffe erfolgen via Phishing oder böswillige Websites. Daher ist es wichtig, dass Mitarbeiter wissen, wie sie Phishing-Mails identifizieren können und wen es bei einer verdächtigen Mail zu informieren gilt. Zudem müssen Leitlinien zur sicheren Internetnutzung erstellt und durchgesetzt werden. Und schließlich sind Mitarbeiter zur Wichtigkeit starker Passwörter und deren Erstellung und Verwaltung zu schulen.

Zudem ist auch ein ergänzender Antiviren-Schutz entscheidend. Da sich Viren und Malware leicht von einer lokalen Maschine auf Cloud-Daten ausbreiten können, bilden IT-Sicherheitsmaßnahmen einen wesentlichen Bestandteil des Office 365-Schutzes. Ransomware wird kontinuierlich verändert, um ihr Aufspüren zu verhindern. Daher sollten Sie sicher stellen, dass Ihre Antivirus-Software genauso aktuell ist. Einige Antivirus-Lösungen sind cloudgestützt, d.h. sie werden automatisch aktualisiert. Für die Verwaltung kann das ein Vorteil sein.

Die Datensicherung ist die beste Methode zum Schutz gegen versehentliches oder böswilliges Löschen von Dateien, sonstige Anwenderfehler, Ransomware und Datenbeschädigung. Die nativen Tools von Microsoft bieten hier etwas Schutz, jedoch gewährleisten erst Datensicherungslösungen von Drittanbietern, dass Sie alle Office 365-Daten schnell wiederherstellen und so die entsprechenden Aufbewahrungspflichten und Datenschutzrichtlinien umsetzen können.

Nicht alle Sicherungstools für Office 365 sind identisch ausgestattet. Tatsächlich bieten die meisten keinen Schutz für alle Office-Anwendungen. Zum Beispiel fehlt bei vielen Produkten der Support für Microsoft Teams. Andere bieten keinen granularen Restore oder die Wiederherstellung von Genehmigungen. Wenn Sie also ein Datensicherungsprodukt für Office 365 auswählen, vergewissern Sie sich, dass es Funktionen enthält, die Sie benötigen. Carbonite Backup for Office 365 schützt beispielsweise die gesamte Microsoft Office 365 Suite, inklusive Teams, OneDrive, Exchange, SharePoint, Planner und Skype for Business.

Einige Sicherungstools für Office 365 besitzen Funktionen, die den Bedarf bei Governance und Compliance unterstützen, zum Beispiel in Hinblick auf DSGVO-Richtlinien. Carbonite Backup for Office 365 bietet beispielsweise ein dediziertes Privacy Dashboard, das Nutzern das „Recht auf Vergessenwerden“ gibt sowie die geforderte Verarbeitung von Anfragen Betroffener zur Erteilung von Auskünften zu personenbezogenen Daten und Audits bereitstellt.

Letztendlich kann die Einrichtung einer Datensicherungsstrategie für Office 365 auch beim Sparen von Aufbewahrungskosten helfen. Falls Ihr Unternehmen Nutzerdaten für einen bestimmten Zeitraum aufbewahren muss, kann das Verlängern von Office 365-Lizenzen ehemaliger Mitarbeiter teuer werden. Carbonite Backup for Office 365 ermöglicht das Aufbewahren ihrer Dateien und E-Mails zu einem Bruchteil der Kosten einer entsprechenden Microsoft-Lizenz.

Sprechen Sie uns an und erfahren Sie mehr über Carbonite Backup for Office 365:

+49 2162 91980 20 SalesDACH@carbonite.com www.carbonite.de

W131-0919_EMEA_DE