arcserve®

eBook

VORSICHT VOR ZU VIEL GEFÜHLTER SICHERHEIT

Wie Sie Ihre Microsoft Office 365-Daten schützen

arcserve®

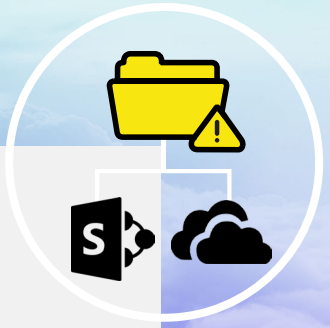
eBook

IHR UNTERNEHMEN IST EINES VON 56% DER UNTERNEHMEN, DIE MICROSOFT OFFICE 365 VERWENDEN.

Office 365 ermöglicht es Ihren Mitarbeitern, überall und jederzeit zu arbeiten - und Ihr Unternehmen ist bei der E-Mail-Kommunikation, der Teamzusammenarbeit sowie der Speicherung von Dokumenten darauf angewiesen.

Auch wenn Microsoft ausgezeichnete Arbeit leistet, um sich um die IT-Infrastruktur für diese Dienste zu kümmern, ist es ein Trugschluss, dass sie sich dort auch um Ihre Daten kümmern, wie Sie es vielleicht erwarten würden. Lesen Sie weiter, um zu erfahren, ob Ihr Unternehmen durch Sicherheitslücken gefährdet ist, die Sie vielleicht noch gar nicht kennen und erfahren Sie, wie Sie die Kontrolle über Ihre Office-365-Daten übernehmen können.

BEISPIEL 01



Ihr Entwicklungsteam hostet unternehmenskritische Projektdateien sowohl auf OneDrive for Business als auch auf SharePoint Online und Sie müssen auf Dateien aus einem Projekt zugreifen, das vor einigen Jahren realisiert wurde. Leider hat einer Ihrer Kollegen versehentlich den Ordner Ihres Teams gelöscht, zusammen mit allen Dokumenten, die Sie für eine bevorstehende Produkteinführung benötigen. In Ihrer Verzweiflung überprüfen Sie schnell den Papierkorb, um die gelöschten Dateien wiederherzustellen. Nur um festzustellen, dass die Dokumente auch hier ebenfalls nicht mehr vorhanden sind.

Annahme:

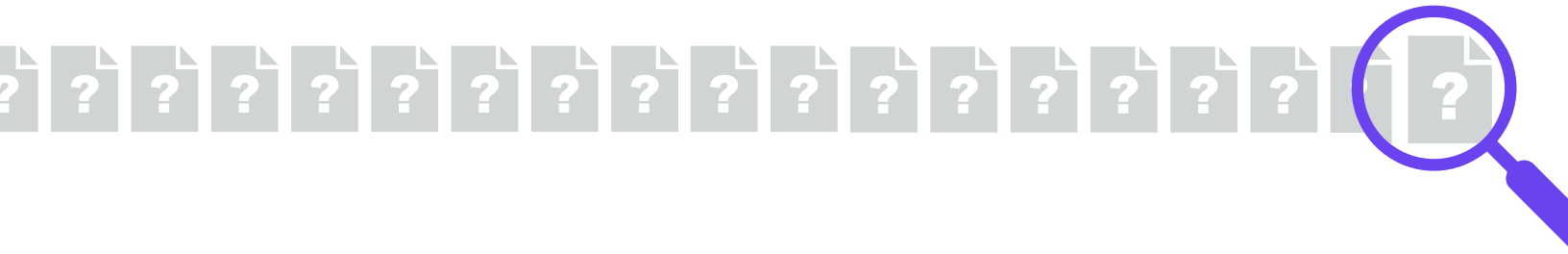
Office 365-Elemente werden von Microsoft zur langfristigen Aufbewahrung gesichert.

Realität:

Elemente in Office 365 werden nur 90 Tage im Papierkorb gespeichert, können aber jederzeit vorzeitig geleert werden, so dass die Daten nicht wiederherstellbar sind. Und selbst wenn Daten abrufbar sind, ist die Point-in-Time-Wiederherstellung für Microsoft nicht möglich, so dass Sie keine andere Wahl haben, als die neueste Version im Papierkorb mit allen Änderungen wiederherzustellen, auch wenn Sie das gar nicht wollen. Darüber hinaus variieren die Speicherrichtlinien für jede Anwendung in der Cloud-Plattform, was den Prozess der Wiederherstellung gelöschter Elemente noch umständlicher macht.

Ergebnis:

Hunderte von Stunden (und viel Geld!) verschwendet durch die Suche nach nicht wiederherstellbaren Dokumenten und die Überarbeitung verlorener Dateien.



BEISPIEL 02

Sie erhalten eine E-Mail vom stellvertretenden Personalchef, der sie dringend dazu auffordert persönliche Daten zu verifizieren, damit Sie eine Rückerstattung Ihrer Krankenversicherung ausbezahlt bekommen können. Die E-Mail enthält einen Link, den Sie anklicken und dort ihre Bankverbindung und personenbezogene Daten bestätigen sollen. Genau in dem Moment als Sie auf „senden“ drücken, überdenken Sie die Angelegenheit noch einmal und zweifeln an einer solchen Maßnahme der Personalabteilung. Sie gehen sofort zur E-Mail zurück, um deren Echtheit zu überprüfen und festzustellen, dass die Absenderadresse ein Phishing-Konto ist und Sie Opfer eines Betrugs geworden sind.

Annahme:

Office 365-Anwendungen sind vor externen Cyber-Bedrohungen geschützt.

Realität:

Die Kontrolle der Office 365-Daten liegt in Ihrer Verantwortung, einschließlich des Schutzes Ihrer Exchange Online E-Mails vor Ransomware, Malware und Hackern. Ohne eine Datenschutzlösung eines Drittanbieters haben Sie keine Möglichkeit, auf eine separate Kopie Ihrer Daten zuzugreifen, wenn ein Mitarbeiter auf eine E-Mail reagiert, auf die er nicht reagieren sollte.

Ergebnis:

Externe Sicherheitsangriffe und Datenschutzverletzungen können verheerende Auswirkungen auf ein Unternehmen haben, was zu erheblichen finanziellen Einbußen und irreparablen Schäden an Ihrer Markenreputation führen kann. Darüber hinaus können Sie für teure Bußgelder im Zusammenhang mit der Einhaltung gesetzlicher Vorschriften und Datenschutzrichtlinien verantwortlich gemacht werden, wenn interne und Kundeninformationen betroffen sind.

BEISPIEL 03

Einer Ihrer Mitarbeiter ist vor einem Jahr aus dem Unternehmen ausgeschieden und das Konto wurde gelöscht, um Lizenzkosten für inaktive Benutzer zu sparen. Leider hat dieser Mitarbeiter unerwartet rechtliche Schritte gegen Ihr Unternehmen eingeleitet, und Sie sind verpflichtet, Informationen über den Streitfall vorzulegen.

Annahme:

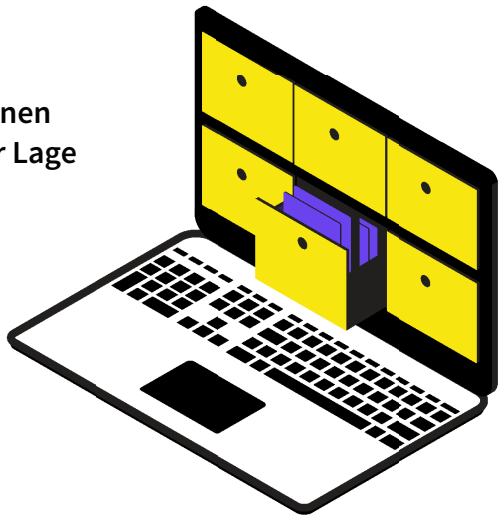
Office 365 hat eine integrierte Datensicherung.

Realität:

Viele Unternehmen sind motiviert, alte Nutzerkonten zu löschen, um die finanzielle Belastung durch die Zahlung von Lizenzgebühren für gekündigte Mitarbeiter oder solche, die das Unternehmen verlassen haben, zu vermeiden. Dies kann bei Rechtsstreitigkeiten zu Problemen führen, da das Löschen eines Benutzers bedeutet, dass seine persönliche SharePoint-Website und sein OneDrive-Konto ebenfalls für immer verloren sind. Und obwohl Litigation Hold ein von Microsoft eingesetzter Schutzmechanismus ist, um das Risiko von Datenverlusten zu verringern, kann es nicht an die Stelle der Datensicherung von Drittanbietern treten, um Compliance-Anforderungen und -Vorschriften zu erfüllen.

Ergebnis:

Rechtliche Schritte können lähmend sein, wenn Sie Anwaltskosten und die Folgen oder Bußgelder, mit denen Sie konfrontiert werden können, wenn Sie nicht in der Lage sind, die notwendigen Informationen bereitzustellen. Sie wissen nie, wann Sie E-Mails oder andere Dokumentationen vorlegen müssen, also ist die Vorhaltung der Informationen der einzige Weg, um Ihr Unternehmen vor Risiken zu bewahren.



arcserve®

eBook

SCHÜTZEN SIE IHRE OFFICE 365-DATEN MIT ARCSERVE!

Microsoft bietet Backups als Teil eines Shared-Responsibility-Modells an. Das heißt: Microsoft ist einerseits für die physische Sicherheit ihrer Rechenzentren und Softwarefehler verantwortlich, Sie aber andererseits für den Schutz Ihrer Daten vor menschlichen Fehlern, internen und externen Sicherheitsbedrohungen und programmatischen Problemen.

Mit Arcserve Unified Data Protection (UDP) wird der Schutz von Office 365 zur Realität und Sie profitieren von den umfassendsten Datenschutzfunktionen, die für Office 365 verfügbar sind, einschließlich:

- vollständigem Support für Ihre unternehmenskritischen Office-365-Anwendungen: Exchange Online, SharePoint Online und OneDrive for Business;
- Point-In-Time-Backup und granulare Wiederherstellung;
- Deduplikation und Kompression mit starker AES-Verschlüsselung;
- flexiblem Storage-Support und Lizenzierungsoptionen, die Ihren Geschäftsanforderungen angepasst sind; sowie
- optimierte, einheitliche Verwaltungsoberfläche für eine integrierte Disaster-Recovery- und Backup-Lösung.

Übernehmen Sie mit Arcserve die Kontrolle über Ihre Office 365-Daten! Schützen Sie das Unbezahlbare!