arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Backup-Lücke von Microsoft 365

Unternehmen nutzen Microsoft 365 als Grundlage für ihre Produktivität. Doch neben den Vorteilen solcher Produktivitätsplattformen wird immer wieder eine Lücke in der Datenschutzstrategie übersehen: das Prinzip der geteilten Verantwortung. Diese Nachlässigkeit setzt wichtige Geschäftsinformationen erheblichen Risiken aus, die sich in Ausfallzeiten und wirtschaftlichen Verlusten niederschlagen können.

Ein Risiko bei der Nutzung von Microsoft 365 besteht dann, wenn Unternehmen davon ausgehen, dass die integrierten Funktionen einen umfassenden Datenschutz bieten, der auch robuste Backup- und Wiederherstellungsfunktionen einschließt. Dieser Irrtum rührt daher, dass die die Sicherheit von Microsoft fälschlicherweise als Datenschutz und Datensicherung interpretiert wird. Tatsächlich bleiben Unternehmen aber anfällig für Datenverluste, die durch versehentliche Löschungen, Insider-Bedrohungen oder immer raffiniertere Ransomware-Angriffe entstehen.

Modell der geteilten Verantwortung
Microsoft verfolgt ein Sicherheitsmodell der geteilten Verantwortung, das präzise zwischen den Pflichten von Microsoft und den Aufgaben der Kunden unterscheidet. Microsoft ist für die Sicherheit und Verfügbarkeit der zugrunde liegenden Infrastruktur zuständig. Dazu zählen die physischen Rechenzentren, Netzwerkkontrollen und die Anwendungssoftware. Die Kunden hingegen sind verantwortlich für den Schutz, die Sicherung und Wiederherstellung ihrer Geschäftsdaten, die sich innerhalb der Microsoft 365-Umgebung befinden.

Die Schutzlücke, die sich aus der Fehlinterpretation der Verantwortlichkeiten ergibt, kann nur mit Backup-Lösungen von Drittanbietern geschlossen werden, die speziell für Microsoft 365-Umgebungen entwickelt wurden. Denn die Wiederherstellungsmöglichkeiten innerhalb von Microsoft 365 sind begrenzt: Der Papierkorb beispielsweise erlaubt eine Aufbewahrung von maximal 93 Tagen in SharePoint und OneDrive. Ein Schutz gegen endgültiges Löschen, gegen große Störungen in der Infrastruktur des Cloud-Anbieters oder gar gegen Ransomware ist das nicht.

Cyberkriminalität auf dem Vormarsch
Gezielte Cyberangriffe sind eine zunehmende Bedrohung für Microsoft 365. Im vergangenen Jahr verzeichnete Microsoft einen zehnfachen Anstieg passwortbasierter Angriffe. Die Kriminellen entwickeln ausgefeilte Kampagnen, die speziell auf Microsoft 365 abzielen, darunter Ransomware-Varianten zur Verschlüsselung cloudbasierter Informationen oder Kontoübernahmen, die den gesamten Mandanten eines Unternehmens kompromittieren können. Ohne eine unveränderliche Backup-Lösung sind betroffene Unternehmen gezwungen, entweder auf Lösegeldforderungen einzugehen oder sie riskieren, dauerhaft den Zugriff auf ihre geschäftskritischen Daten zu verlieren.

Neben Nutzerinformationen geraten auch andere Daten in Microsoft 365 zunehmend ins Visier, etwa Microsoft Entra-Gruppen, Benutzer, Rollen und Berechtigungen. Der Verlust solcher Identitäts- und Anwendungsobjekte kann verheerende Folgen haben, da eine Wiederherstellung ohne entsprechende Sicherungsmechanismen nahezu unmöglich ist. Es wäre vergleichbar mit dem Verlust sämtlicher Schlüssel zum eigenen Haus.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Fazit
Die Backup-Lücke in Microsoft 365 ist kein theoretisches Problem, sondern ein reales Geschäftsrisiko. Unternehmen, die auf Microsoft 365 vertrauen, müssen sich ihrer Rolle im Modell der geteilten Verantwortung bewusst sein und Schutzmaßnahmen ergreifen, die weit über die Standardfunktionen hinausgehen. Diese Herausforderungen erfordern ein Umdenken, weg von einem reaktiven und hin zu einem proaktiven Datenschutz. Nur durch das Erkennen der spezifischen Schwächen der Microsoft-Schutzmechanismen, ergänzende Backup-Lösungen wie beispielsweise von Arcserve, regelmäßige Tests und Validierungen sowie der Definition klarer Wiederherstellungsziele können Umgebungen wie Microsoft 365 vor einem Verlust von Daten bewahren.

Ein detaillierter Bericht mit Bedrohungsvarianten und Lösungsoptionen ist hier zu finden: https://www.arcserve.com/blog/microsoft-365-backup-gap-why-your-business-data-isnt-secure

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

Über Arcserve
Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen. Erfahren Sie mehr unter arcserve.com.

Unternehmenskontakt
Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
Alexandra Schmidt
+49 170 387 10 64
arcserve@tc-communications.de