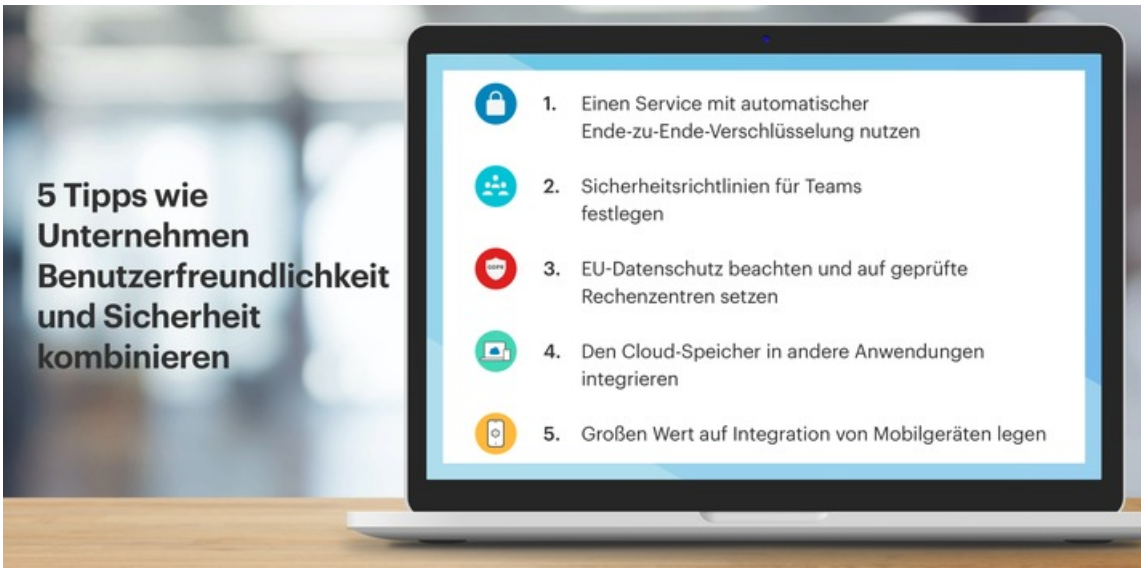
05.10.2020 – 16:21 Uhr

Cloud-Speicher: Fünf Tipps, wie Unternehmen Benutzerfreundlichkeit und Sicherheit kombinieren



Zürich (ots) -

Cloud-Speicher sind flexibel einsetzbare und skalierbare Speicherplätze. Längst nutzen nicht mehr nur Privatpersonen Cloud-Lösungen, um Fotos und andere Dateien abzulegen. Auch Unternehmen greifen gern auf dieses praktische Kollaborations-Werkzeug zurück. Doch geht diese Benutzerfreundlichkeit zu Lasten der Sicherheit?

Mit Hilfe von Cloud-Lösungen lassen sich im Prinzip unlimitierte Mengen an Daten standort- und geräteunabhängig sichern. Der Speicherplatz auf den eigenen Geräten und innerhalb der eigenen Infrastruktur wird so geschont. Dafür benötigt der Nutzer nur eine Internetverbindung und eine entsprechende Anwendung - innerhalb kürzester Zeit steht das zusätzliche Laufwerk auf Cloud-Basis zur Verfügung. Und nicht nur das: Über die Vergabe von Zugriffsrechten können die gespeicherten Dateien anderen Nutzer zur Verfügung gestellt werden. Das vereinfacht die Zusammenarbeit, nicht nur mit remote arbeitenden Kollegen, sondern auch mit Geschäftspartnern und weiteren externen Parteien.

Doch Cloud-Speicher sind in die Kritik geraten. Denn Public-Cloud-Tools werfen Fragen im Bereich Datenschutz auf, gerade dann, wenn der Speicher über Unternehmensgrenzen hinweg genutzt wird. Doch Sicherheitsbedenken müssen nicht sein. Im folgenden deshalb fünf Tipps, worauf Unternehmen achten sollten, damit der Cloud-Speicher benutzerfreundlich und sicher zugleich ist.

Tipp 1: Einen Service mit automatischer Ende-zu-Ende-Verschlüsselung nutzen

Traue keinem Cloud-Speicher blind - das ist eine Binsenweisheit und trotzdem werden im täglichen Geschäftsleben oft genug Dateien über gängige Cloud-Speicher geteilt, ohne sich vorab Gedanken über dessen Sicherheits-Features zu machen. Eine zuverlässige Sicherheit bei Cloud-Lösungen bietet Ende-zu-Ende-Verschlüsselung. Dabei erfolgen sowohl die Ver- als auch die Entschlüsselung clientseitig mit einem jeweils neu generierten Schlüssel für jede Datei-Version. Das bedeutet, nur der Eigentümer und von ihm autorisierte Benutzer können die Daten einsehen. Die Weitergabe der Schlüssel erfolgt über teilbare, verschlüsselte Ordner.

Tipp 2: Sicherheitsrichtlinien für Teams festlegen

Um die Kontrolle über die gespeicherten Daten zu behalten, ist es empfehlenswert, Richtlinienprofile einzurichten, um Nutzer zu organisieren und verschiedene Nutzungsregelungen für jede Profilgruppe festzulegen. Dabei geht es nicht nur darum, wer auf welche Datei zugreifen kann, sondern auch darum, beispielsweise eine 2-Stufen-Verifizierung zu nutzen, nur bestimmte Geräte zuzulassen oder Sitzungszeiten zu beschränken. Je detaillierter sich solche Sicherheitsrichtlinien definieren lassen, umso besser können Verantwortliche den Umgang mit Daten steuern.

Tipp 3: EU-Datenschutz beachten und auf geprüfte Rechenzentren setzen

Die Datenschutzgrundverordnung (DSGVO) verlangt, dass alle Unternehmen ihre Prozesse mit eingebautem Datenschutz ("privacy by design") und standardmäßigem Datenschutz "privacy by default") gestalten. Das gilt selbstverständlich ebenso, wenn Cloud Services zum Einsatz kommen. Der gewählte Cloud-Speicher muss den hohen Anforderungen des EU-Datenschutzes gerecht werden. Das heißt zum Beispiel, dass der Dienstleister geeignete Maßnahmen ergreift, um die ihm übertragenen Daten vor unrechtmäßiger Verarbeitung, Verlust oder Beschädigung zu schützen. Dazu gehören neben Verschlüsselungs- und Richtlinien-

Konzepten auch redundante Rechenzentren mit geeigneten physischen Sicherheitsmaßnahmen. Verschiedene offizielle Zertifizierungen helfen bei der Auswahl eines passenden Anbieters. Eine interessante Option für international arbeitende Unternehmen können Datenresidenzoptionen sein, wie sie etwa Tresorit bietet. Dadurch können Rechenzentren gezielt zugewiesen werden, um sicherzustellen, dass Daten in einem bestimmten Land gespeichert werden.

Tipp 4: Den Cloud-Speicher in andere Anwendungen integrieren

Kaum ein Tool kann sein volles Potenzial entfalten, wenn es nicht nahtlos in die vorhandene IT-Landschaft eingebunden werden kann. "Benutzerfreundlich" heißt heutzutage eigentlich auch "integriert und ohne zusätzlichen Aufwand verwendbar". Bei der Wahl eines Cloud-Speichers sollten Unternehmen deshalb vorab prüfen, ob dieser die benötigten Funktionen zu einer solchen Integration bietet. So kann beispielsweise eine Outlook-Anbindung wichtig sein, der Zugriff über einen Browser, automatische Upload-Optionen, der Offline-Zugriff, sichere Bereitstellung von Datei-Links oder definierte Schnittstellen.

Tipp 5: Großen Wert auf Integration von Mobilgeräten legen

Ortsunabhängig auf alle gespeicherten Daten zugreifen zu können - das ist eine der angenehmsten Seiten von Cloud-Speichern. Um diesen Vorteil optimal auskosten zu können, kommt es darauf an, dass der Cloud-Speicher verschiedene mobile Betriebssysteme unterstützt und zugleich höchste Datensicherheit garantiert. Wieder kommt hier beispielsweise Ende-zu-Ende-Verschlüsselung ins Spiel, dank der umständliche Mobile-VPN-Clients der Vergangenheit angehören. Zu einer sicheren Mobile Policy gehört es außerdem, verlorengegangene Mobilgeräte zu schützen: etwa durch die Möglichkeit Dateien aus der Ferne zu löschen, Geräte remote auszuloggen oder den Zugang zum Speicher durch Fingerabdruck oder mehrstufiger Verifizierung abzusichern.

Fazit: Cloud-Speicher sind einfach zu handhaben und zu installieren. Dadurch sind sie eine praktische Basis für team- und unternehmensübergreifende Zusammenarbeit, für das Teilen von Dokumenten und das Speichern von Daten. Damit dies nicht auf Kosten der Sicherheit und Compliance geht, sollten Unternehmen die Wahl des Cloud-Speichers allerdings nicht dem Zufall überlassen, sondern gezielt vorab notwendige und wünschenswerte Sicherheitsfeature evaluieren. Benutzerfreundlichkeit und höchste Sicherheitsstandards lassen sich heutzutage, mit der richtigen Lösung, sehr wohl kombinieren.

Autor: István Lám, CEO und Co-Founder von Tresorit

Über Tresorit

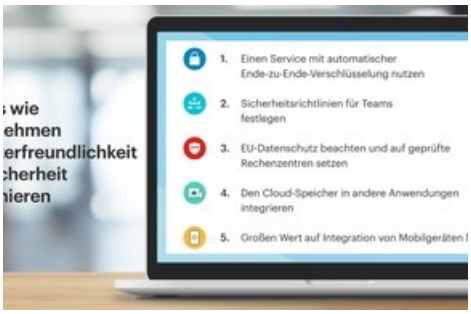
Tresorit ist eine Ende-zu-Ende verschlüsselte Zero-Knowledge-Content-Collaboration-Plattform (CCP). Ziel ist es, Daten von Personen und Organisationen mit der höchsten Klassifizierung in der Cloud zu schützen. Mit regionalen Standorten in Zürich, der Schweiz, Deutschland, Ungarn und den USA ist Tresorit auf dem Markt für Enterprise Cloud Storage und Content Collaboration Plattformen tätig. Tresorit ist die sicherste Art der Zusammenarbeit und verschlüsseln alles, um nichts zu wissen.Erfahren Sie mehr unter www.tresorit.com

Tresorit AG | Minervastrasse 3 | 8032 Zürich | Schweiz

Pressekontakt:

PIABO PR GmbH
Julia Loeser
E-Mail: tresorit@piabo.net
Phone: +49 30 2576 205 - 19
Markgrafenstraße 36
10117 Berlin | Germany

Medieninhalte



Cloud-Speicher: Fünf Tipps, wie Unternehmen Benutzerfreundlichkeit und Sicherheit kombinieren, Quelle: Tresorit / Weiterer Text über ots und www.presseportal.de/nr/148823 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/Tresorit AG"