Metaways: Diese Gefahren lauern in kostenlosen Public Clouds

Der IT-Dienstleister Metaways erläutert, warum gratis und sicher in der Cloud nicht zusammengehen.

Kostenfreie Public-Cloud-Angebote für Messaging, File Sharing oder Collaboration sind vor allem für kleine und mittelständische Unternehmen mit ihren schmalen IT-Budgets oft sehr verlockend. Doch sie bergen meist unkalkulierbare Sicherheitsrisiken. Der IT-Dienstleister Metaways nennt fünf Gründe, warum man von solchen Diensten lieber Abstand nehmen sollte.

1. Vermarktung der Nutzerdaten: Bei den meisten kostenfreien Public-Cloud-Diensten kommerzialisiert der Anbieter die Nutzerdaten – ein entsprechender Hinweis findet sich dann irgendwo im Kleingedruckten. Welche Daten nutzt der Mitarbeiter? Wann ist er bevorzugt online? Mit wem kommuniziert er? Mit diesen und ähnlichen Informationen werden exakte Nutzerprofile erstellt und an Anbieter verkauft, die auf gezielte Online-Werbung spezialisiert sind.

2. Drohender Rechteverlust an Inhalten: Viele Anbieter gehen sogar noch einen Schritt weiter und sichern sich in ihren Nutzungsbedingungen zusätzlich die Rechte an sämtlichen übertragenen Inhalten. Tauschen also beispielsweise Ingenieure technische Zeichnungen oder ähnliches aus, riskiert das Unternehmen, die Rechte an seinem geistigen Eigentum ungewollt an den Betreiber des Cloud-Dienstes zu übertragen.

3. Anfälligkeit für Cyber-Kriminalität: In Gratis-Public-Clouds wird in aller Regel sehr viel Infrastruktur von mehreren Nutzern gemeinsam verwendet. Das macht es sehr aufwändig, die Zugriffe zu überwachen. Und diesen Aufwand scheuen die Anbieter, steht er doch ihrem Geschäftsmodell entgegen – so viele Nutzer und damit so viele Daten wie möglich zu bekommen. Cyber-Kriminelle haben es dadurch leicht, an Passwörter oder Kreditkarteninformationen zu gelangen. Der Anreiz dafür ist gerade bei großen kostenfreien Cloud-Diensten besonders hoch – schließlich gibt es für die Hacker hier deutlich mehr Daten zu holen als bei einem kleinen Provider.

4. Gefahr von staatlichen Zugriffen: „Alle eure Daten gehören uns.“ Mit dieser Begründung forderte vor wenigen Wochen ein US-Gericht im Rahmen einer Ermittlung Zugriff auf Daten von Microsoft. Damit beansprucht der amerikanische Staat uneingeschränkten Zugriff auf alle Daten, die von US-Firmen gehostet werden. Diese Rechtsauffassung birgt die Gefahr, dass US-Behörden die großen amerikanischen Cloud-Dienste ohne jegliches Unrechtsbewusstsein auch für Industriespionage nutzen. Ein ähnliches Problem besteht aber auch in Deutschland. So muss jeder deutsche Internet-Provider, der mehr als 10.000 E-Mail-Konten beziehungsweise Kunden aufweist, eine sogenannte Sina-Box

installieren. Mit ihr wird im Falle eines richterlichen Beschlusses der E-Mail-Verkehr an die Behörden ausgeleitet. Damit sind auch große Cloud-Betreiber hierzulande der Gefahr staatlicher Zugriffe ausgesetzt. In kleineren Private Clouds besteht dieses Risiko dagegen nicht, da sie praktisch nie den Grenzwert von 10.000 E-Mail-Konten überschreiten.

5. Probleme mit der Compliance: Die Nutzungsbedingungen und Infrastrukturen von kostenlosen Public-Clouds macht es in den allermeisten Fällen praktisch unmöglich, gesetzliche Vorgaben zu erfüllen. Dazu gehört beispielsweise die allgemeine Pflicht bei Rechnungslegungsdaten nachzuweisen, auf welchen physischen Systemen sie sich befinden. Aber auch die speziellen Auflagen in regulierten Branchen – etwa der Schutz personenbezogener Daten bei Medizinunternehmen – lassen sich beispielsweise bei File-Sharing-Diensten nicht sicherstellen.

„Für nichts gibt es auch nichts. Ist ein Cloud-Produkt kostenlos, kann man davon ausgehen, dass der Nutzer das Produkt ist. Außerdem steht bei derartigen Angeboten meist eine hochautomatisierte Massenabfertigung der Datensicherheit im Weg“, sagt Cornelius Weiss, Team Leader Software Engineering bei Metaways in Hamburg. Wollen Unternehmen von den unbestreitbaren Vorteilen der Cloud-Technologie profitieren und gleichzeitig Datensicherheit gewährleisten, so der Experte, sollten sie sich deshalb an einen Dienstleister wenden, der ihre Schutzanforderungen individuell umsetzen kann. „Das ist aber nur in Private Clouds möglich, die der Dienstleister mit eigener Hardware beziehungsweise einem ihm bekannten Betreiber realisiert. Dann lassen sich sehr sichere Lösungen konzipieren. Aber umsonst geht das natürlich nicht.“