Kann Ransomware weiterhin auf Daten zugreifen, die in Cloud-Diensten wie OneDrive oder Google Drive gespeichert sind?

Kurze Antwort: Ja. Während Cloud-Speicher früher für Ransomware unerreichbar war, haben Angreifer ihre Methoden angepasst und können nun cloudbasierte Daten durch Techniken wie Laufwerkszuordnung (Drive Mapping) und, heute noch häufiger, den Diebstahl von API-Schlüsseln und Sitzungstoken angreifen.

Wie sich Ransomwares Vorgehen bei Cloud-Daten verändert hat

Als die Remote-Arbeit einen raschen Wandel hin zu Cloud-Speichern auslöste, mussten sich sowohl Unternehmen als auch Cyberkriminelle gleichzeitig an die neue Umgebung anpassen. In den frühen Phasen dieses Wandels konnte Ransomware in der Regel keine Dateien auf Cloud-Plattformen erreichen – lagen die Daten in der Cloud statt auf einem lokalen Server, ließen Angreifer sie meist unangetastet, da ihnen ein direkter Zugriffsweg fehlte.

Das änderte sich, als Angreifer lernten, Cloud-Speicher wie ein Amazon-, OneDrive- oder Google-Drive-Konto manuell mit einem infizierten System zu verbinden. Sie taten dies, indem sie den Cloud-Speicher als lokalen Laufwerksbuchstaben einbanden – ähnlich wie ein USB-Gerät auf einem Computer als eigenes Laufwerk erscheint. Sobald der Cloud-Speicher auf diese Weise eingebunden war, waren die cloudbasierten Dateien der Verschlüsselung genauso ausgesetzt wie Dateien auf einer lokalen Festplatte.

Die größere Bedrohung heute: gestohlene Schlüssel und Token

Mit der Reifung der Cloud-Nutzung verlagerten sich auch die Taktiken der Angreifer erneut. Anstatt Laufwerke manuell einzubinden, gehen viele nun gezielt gegen API-Schlüssel und Sitzungstoken vor – Zugangsdaten, die direkten, programmgesteuerten Zugriff auf Cloud-Konten und -Daten

gewähren. Der Erwerb eines solchen Tokens ist vergleichbar mit dem Diebstahl eines Passworts, bietet jedoch oft einen breiteren und schnelleren Zugriff auf Cloud-Ressourcen als ein gestohlenes Passwort allein.

Diese Verlagerung ist bedeutsam, denn dieselbe Geschwindigkeit und Skalierbarkeit, die Cloud-Computing für legitime IT-Teams wertvoll machen, stehen nun auch Angreifern zur Verfügung. Unter den Kunden von Cyber Crucible erlebte im vergangenen Jahr mehr als die Hälfte einen versuchten Diebstahl eines Cloud-Sitzungstokens, mit dem Ziel, die aktive Sitzung eines Nutzers zu übernehmen, während weniger als 9 % einen tatsächlichen Datenkompromiss verzeichneten. Dies deutet darauf hin, dass Angreifer den Diebstahl von Zugangsdaten und Token als primären Einstiegspunkt priorisieren, wobei Datendiebstahl ein sekundäres Ziel darstellt.

Sind Cloud-Daten automatisch sicher?

Cloud-Speicher garantiert keinen Schutz vor Ransomware oder Datendiebstahl. Er verändert lediglich die Methode, die Angreifer anwenden müssen, um an diese Daten zu gelangen – wobei sich das primäre Risiko hin zur Kompromittierung von Zugangsdaten und Sitzungstoken verschiebt, statt zur direkten Dateiverschlüsselung.

https://player.vimeo.com/video/1047006345

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

---

Revision #1
Created 2026-07-24 05:01:48 UTC by Dennis Underwood
Updated 2026-07-24 05:01:48 UTC by Dennis Underwood