

Wenn ein KI-Agent das Backup löscht

21.10.2026, 08:11 | IT, New Media & Software

Pressemitteilung von: *FAST LTA GmbH*



Der Schlüssel öffnet mehr als die Tür, für die er gedacht war.

Neun Sekunden bei PocketOS

PocketOS liefert Autovermietungen die Software, in der sie Reservierungen und Zahlungen verwalten. Ende April 2026 arbeitete dort ein KI-Coding-Agent an einer Routineaufgabe in der Testumgebung. Als Zugangsdaten nicht zusammenpassten, suchte der Agent selbst nach einem Ausweg. In einer Datei, die mit der Aufgabe nichts zu tun hatte, fand er einen API-Token, also einen digitalen Zugangsschlüssel. Angelegt war der Token, um Domains beim Cloud-Anbieter Railway zu verwalten, gültig war er für das gesamte Konto. Mit einem einzigen API-Aufruf löschte der Agent ein Speicher-Volume, in der Annahme, es betreffe nur die Testumgebung. Getroffen hat er das Volume der Produktionsdatenbank, eine Rückfrage gab es nicht.

Mit dem Volume verschwanden die Backups, denn Railway hatte die Backups auf Volume-Ebene im selben Volume abgelegt. Am Samstagmorgen fehlten den Autovermietern die Reservierungsdaten, Gründer Jer Crane rekonstruierte mit ihnen Buchungen, unter anderem aus Zahlungshistorien und E-Mails. Railway stellte später ein drei Monate altes Backup wieder her und hat den betroffenen Endpunkt inzwischen auf verzögertes Löschen umgestellt. Laut Crane bleiben große Datenlücken.

Zum Datenverlust führten zwei Konstruktionsfehler. Der Token hatte weit mehr Rechte, als seine Aufgabe verlangte, und die Backups waren mit denselben Rechten erreichbar wie die Produktion. Beide Fehler bestanden schon, bevor der Agent seine Aufgabe begann.

Nur wenige Unternehmen haben Abläufe für KI-Vorfälle

Wie deutsche Unternehmen auf solche Fälle vorbereitet sind, zeigt die am 7. Oktober vorgestellte KI-Sicherheitsstudie 2026 von BSI und TÜV-Verband. Forsa befragte dafür vom 22. Juni bis 31. Juli 2026 505 Unternehmen ab 20 Beschäftigten. 49 Prozent der Unternehmen setzen KI ein, weitere 9 Prozent planen es. Von diesen Unternehmen haben 11 Prozent eigene Abläufe für KI-bezogene Sicherheitsvorfälle, ein Viertel hat gar keine Regelung dafür. Eine Protokollierung oder Überwachung der KI-Nutzung gibt es laut Studie bei 40 Prozent der KI-Anwender. Jeder vierte von ihnen automatisiert mit KI bereits Arbeitsschritte, etwa die Rechnungserstellung. Dirk Stenkamp, Präsident des TÜV-Verbands, sagt dazu: „KI verschärft die Bedrohung von außen und schafft neue Risiken im eigenen Betrieb.“

Der gefahrenübergreifende Ansatz schließt Agenten ein

Für Einrichtungen, die unter das BSI-Gesetz fallen, ist der Fall auch eine Compliance-Frage. § 30 BSIG verpflichtet besonders wichtige und wichtige Einrichtungen zu Maßnahmen gegen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer Systeme. Diese Maßnahmen müssen auf einem „gefahrenübergreifenden Ansatz“ beruhen. Ob ein Angreifer die Daten löscht oder ein eigener Agent, ändert an der Pflicht nichts.

Zum Mindestumfang nach Absatz 2 gehören die „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall“ (Nr. 3) und Konzepte für die Zugriffskontrolle (Nr. 9). Ein Token, mit dem sich Produktion und Backups in einem Schritt löschen lassen, lässt sich mit beiden Punkten kaum vereinbaren.

Backups brauchen einen eigenen Rechtskreis

Agenten brauchen Schreibrechte, sonst automatisieren sie nichts. Für die Datensicherung folgt daraus eine Regel: Kein Konto und kein Token aus der Produktionsumgebung darf ältere Backup-Versionen löschen können, gleich ob ein Mensch es benutzt oder ein Agent.

Das beginnt bei einer Backup-Umgebung mit eigener Benutzerverwaltung und eigenen Administratorkonten. Innerhalb dieser Umgebung brauchen Backup-Versionen eine Aufbewahrungsdauer, die auch die Backup-Software nicht verkürzen kann, denn auch deren Zugangsdaten können in Skripten landen. Fällt auch diese Grenze, bleibt eine Kopie, die physisch vom Netz getrennt ist.

Silent Bricks trennen Backup-Versionen vom Netz

Silent Bricks sind ein On-Premises-Speichersystem für Backup und Restore, entwickelt in München und gefertigt in Deutschland. Die vorhandene Backup-Software, etwa Veeam oder Commvault, schreibt auf Silent Bricks als Backup-Ziel. Snapshots auf dem System bewahren die Backup-Versionen mit eigener, einstellbarer Aufbewahrungsdauer auf, unabhängig von den Zugriffsrechten der Backup-Software.

Ein Air Gap ist eine physische Trennung zwischen Datenträger und Netz. Solange sie besteht, erreicht kein Befehl die Daten, gleich mit welchen Zugangsdaten er abgesetzt wird. Der Silent Brick Max Air trennt sich nach Abschluss des Backup-Jobs galvanisch. Im getrennten Zustand sind weder Ports noch API-Endpunkte erreichbar, im manuellen Modus hebt nur eine Taste am Gerät die Trennung wieder auf. Der Silent Brick Pro lässt sich physisch aus dem Controller X entnehmen.

Die Inventur beginnt bei den Tokens

Ein Restore-Test beantwortet, ob sich Daten zurückspielen lassen. Fälle wie PocketOS fügen eine zweite Prüfung hinzu: Welche Konten und Tokens können die älteste Backup-Version löschen, und wo liegen sie? Taucht dabei ein Token auf, den ein Agent in einer Konfigurationsdatei finden kann, teilen Backup und Produktion dasselbe Risiko.

Welches Konto oder welcher Token in Ihrem Netz kann Ihre Backups löschen?

Im persönlichen Termin gehen wir mit Ihnen durch, welche Konten heute auf Ihre Backup-Versionen zugreifen und wie eine getrennte Backup-Umgebung mit Silent Bricks aussieht. Oder Sie besuchen einfach mal unser Webinar zum Thema “Backup ist nicht Restore”.

FAST LTA

Tölzer Str. 1
81379 München

Deutschland

Marek Birkenhauer (Online Marketing Manager)

Marek.Birkenhauer@fast-lta.de

Portrait

FAST LTA ist der Spezialist für Datensicherheit und Data-Privacy in Enterprise Storage sowie für Systeme, die lokalen KI-Betrieb ermöglichen. Die Kombination aus langlebiger und wartungsarmer Hardware, integrierter Software und Wartungsverträgen mit bis zu zehn Jahren Laufzeit sorgt für langfristig kostengünstigen Betrieb – von der Archiv- und Backup-Speicherung bis zum lokalen KI-Einsatz. Die Lösungen für sichere Datenspeicherung Made in Germany und digitale Souveränität des Münchner Anbieters haben sich in über 3.500 Installationen bewährt, unter anderem in Healthcare, öffentlicher Verwaltung, Dienstleistung sowie Industrie & Handel.

News-ID: 1327590 • Views: 147 (Stand: 28.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1327590/Wenn-ein-KI-Agent-das-Backup-loescht.html>