Warum reichen Backup und Wiederherstellung nicht aus, um mit Ransomware umzugehen?

Kurze Antwort: Backups adressieren nur die letzte Phase eines Ransomware-Angriffs – die Verschlüsselung. Wenn die Verschlüsselung beginnt, haben Angreifer in der Regel bereits Zugangsdaten gestohlen und Ihre Daten exfiltriert. Die Wiederherstellung aus einem Backup stellt Ihre Dateien wieder her; sie ändert jedoch nichts an den Daten, die sich bereits in den Händen des Angreifers befinden.

Ransomware ist der letzte Schritt, nicht der erste

Ein typischer Angriff läuft in drei Phasen ab:

1. **Identitätsdiebstahl** – Zugangsdaten werden kompromittiert, um Zugriff zu erlangen.
2. **Datendiebstahl** – geistiges Eigentum, Kundendaten und andere sensible Informationen werden exfiltriert.
3. **Verschlüsselung** – Dateien werden gesperrt und ein Lösegeld gefordert.

Wiederherstellungsstrategien setzen erst in Phase drei an. Die Vertraulichkeitsverletzung und der Verlust der operativen Kontrolle haben zu diesem Zeitpunkt bereits stattgefunden.

Die tatsächlichen Kosten

Das größte geschäftliche Risiko durch Ransomware ist in der Regel nicht das Lösegeld selbst – es sind die Umsatzeinbußen durch einen längeren Ausfall sowie der daraus resultierende Reputationsschaden. Die Verhinderung der initialen Kompromittierung schützt vor beidem. Deshalb muss Prävention vor der Planung der Wiederherstellung stehen, nicht als Ersatz dafür.

Revision #1
Created 2026-07-24 04:32:21 UTC by Dennis Underwood
Updated 2026-07-24 04:32:21 UTC by Dennis Underwood