Was ist aus dem „dumm sammelnden" Modell der Sicherheitsbranche geworden?

Kurze Antwort: Jahrelang rieten Anbieter, dass lokale Endpunktverarbeitung veraltet sei, und setzten stattdessen auf leichtgewichtige Agenten, die Rohtelemetriedaten an Cloud-Analysen weiterleiten. Moderne speicherresidente Angriffe auf zentrale Betriebssystembibliotheken haben dieses Modell entlarvt — die Agenten laufen weiter, werden aber faktisch blind und stumm.

Warum das Modell übernommen wurde

Es war günstiger zu entwickeln. Kernel-Level-Engineering ist schwierig und teuer; das Versenden von Telemetriedaten in die Cloud ermöglichte es Anbietern, kostengünstige Endpunktsoftware auszuliefern, große Cloud-Speicherpools zu monetarisieren und Cloud-KI-Fähigkeiten zu vermarkten. Das Modell war auf Entwicklungsökonomie optimiert, nicht auf Verteidigung.

Warum es jetzt scheitert

Diese Agenten sind vollständig auf native Betriebssystemkomponenten angewiesen, um zu funktionieren und Daten zu sammeln. Wenn Angreifer diese Komponenten im Speicher kompromittieren, stürzt der Agent nicht ab — er läuft weiter und meldet nichts, sodass ein Dashboard anzeigt, alles sei in Ordnung, während Daten exfiltriert werden.

Es gibt zudem dokumentierte, gezielte Sabotage: Angreifer und, in einigen verifizierten Fällen, Wettbewerber, die eigene Schwächen verschleiern wollen, nutzen aktiv diese Bibliotheksabhängigkeiten aus, um Endpunktschutzmaßnahmen zwangsweise zu beenden oder zu sabotieren.

Die architektonische Sackgasse

Um dies zu beheben, müssten etablierte Anbieter cloud-first-Telemetrie-Pipelines aufgeben und für lokale Verarbeitung auf Kernel-Ebene am Edge neu aufbauen — ein mehrjähriges Vorhaben. Aktuelle Übernahmen und Venture-Investitionen zeigen, dass sich die Branche stattdessen weiter in Richtung Cloud-Analysen und zentralisierter Data Lakes bewegt.

Revision #1
Created 2026-07-24 04:41:22 UTC by Dennis Underwood
Updated 2026-07-24 04:41:22 UTC by Dennis Underwood