Warum greift Ransomware freigegebene Dateien an, bevor sie meinen Desktop trifft?

Kurze Antwort: Wenn Ransomware einen einzelnen Arbeitsplatzrechner infiziert, ist dieser Rechner selten das eigentliche Ziel. Angreifer nutzen die Erstinfektion als Ausgangspunkt, um freigegebene Netzwerkressourcen zu erreichen, und verschlüsseln oder beschädigen den lokalen Desktop erst, nachdem sie bereits wertvollere Daten an anderer Stelle angegriffen haben.

Warum der Desktop die letzte Station ist, nicht die erste

Ein weitverbreiteter Irrglaube ist, dass es sich bei den Dateien eines bestimmten Mitarbeiters um das Ziel der Angreifer handelt, sobald Ransomware auf dessen Computer gelangt. In Wirklichkeit ist die Schadsoftware so programmiert, dass sie fast sofort über den lokalen Rechner hinausblickt. Sobald sie Fuß gefasst hat, beginnt sie, das Netzwerk nach erreichbaren Ressourcen mit größerem Wert zu durchsuchen, etwa Dateiservern, internen Wikis oder Datenbanken mit Kundendaten. Die Verschlüsselung oder Exfiltration dieser zentralen Daten ist das eigentliche Ziel, da sie einen weitaus größeren Teil der Organisation betrifft als der Ordner eines einzelnen Nutzers.

Die Lösegeldforderung erscheint zuletzt, nicht zuerst

Da Angreifer netzwerkweiten Daten Priorität einräumen, bevor sie das ursprünglich infizierte Gerät angreifen, ist der betroffene Mitarbeiter in der Regel die letzte Person, die etwas Ungewöhnliches bemerkt. Bis eine Lösegeldforderung auf dem Bildschirm dieser Person erscheint, haben die Angreifer typischerweise bereits die Verschlüsselung oder den Diebstahl von Daten in großen Teilen der Unternehmensinfrastruktur abgeschlossen. Diese Reihenfolge ist beabsichtigt. Sie ermöglicht es den Angreifern, maximalen operativen Schaden anzurichten, bevor jemand in der Organisation die Chance hat, den Einbruch zu erkennen oder darauf zu reagieren. Die sichtbare Lösegeldforderung ist im Grunde ein Signal dafür, dass der schwerwiegendere Schaden bereits im Verborgenen entstanden ist.

Was das für die Verteidigung bedeutet

Persönliche Fotos oder Dokumente, die lokal auf einem Desktop gespeichert sind, sind bei einem Ransomware-Angriff in der Regel das unwichtigste Ziel, auch wenn sie das sichtbarste Anzeichen dafür sein können. Eine wirksame Verteidigung muss dieses Muster berücksichtigen, indem sie sich darauf konzentriert, bösartige Aktivitäten so früh wie möglich zu erkennen und zu stoppen, bevor sie freigegebene Systeme erreichen können. FortressAI von Cyber Crucible wurde mit dieser Angriffssequenz im Hinterkopf entwickelt und zielt darauf ab, bereits in den frühen Phasen eines Einbruchs einzugreifen, anstatt erst zu reagieren, wenn die Verschlüsselung auf einzelnen Rechnern sichtbar wird.

https://player.vimeo.com/video/1043466243

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Revision #1
Created 2026-07-24 05:04:34 UTC by Dennis Underwood
Updated 2026-07-24 05:04:34 UTC by Dennis Underwood