Warum werden Ransomware-Angriffe von Jahr zu Jahr häufiger?

Kurze Antwort: Ransomware-Angriffe nehmen zu, weil sich Cyberkriminelle Gruppen von unorganisierten, opportunistischen Akteuren zu disziplinierten Operationen entwickelt haben, die Automatisierung nutzen, um viele Opfer effizient anzugreifen und schnell Zahlungen zu erpressen.

Vom chaotischen Start-up zur organisierten Operation

Als Ransomware erstmals zu einer weitverbreiteten Bedrohung wurde, waren viele Angreifer unerfahren. Eine Welle neu arbeitsloser Personen versuchte sich während der Pandemie an Cyberkriminalität, oft mit uneinheitlichen Ergebnissen. Wie in jeder aufstrebenden Branche überlebten diese frühe Marktbereinigung nur die organisierteren und leistungsfähigeren Akteure. Im Laufe der Zeit begannen diese Gruppen weniger wie verstreute Gelegenheitsakteure und mehr wie strukturierte Unternehmen zu agieren, die auf konstante Einnahmen ausgerichtet sind.

Bis 2024 hat sich diese Reife in einer starken Abhängigkeit von Automatisierung niedergeschlagen. Etablierte Ransomware-Operationen setzen mittlerweile automatisierte Tools ein, um weniger erfahrene Teilnehmer in ihre Angriffe einzubinden und dabei effiziente, wiederholbare Prozesse beizubehalten. Dies hat es ihnen ermöglicht, ihre Aktivitäten weit über das hinaus zu skalieren, was ein kleines Team versierter Hacker manuell erreichen könnte.

Die richtige Dosierung des Angriffs für maximale Auszahlung

Ein wesentlicher Teil dieser Entwicklung besteht darin, zu lernen, wie ein Angriff richtig dimensioniert wird. Ist ein Eindringen zu geringfügig, kann ein gut vorbereitetes IT-Team die Systeme einfach wiederherstellen und muss nichts zahlen. Ist ein Angriff zu umfangreich und löscht die gesamte Unternehmensinfrastruktur, bleibt möglicherweise kein tragfähiges Unternehmen mehr übrig, das überhaupt eine Lösegeldzahlung leisten könnte. Moderne Ransomware-Gruppen zielen auf einen Mittelweg ab: genug Störung, um ein Unternehmen zu einer schnellen Zahlung zu

drängen, ohne so viel Schaden anzurichten, dass eine Wiederherstellung oder Verhandlung irrelevant wird.

Warum Automatisierung den Anstieg antreibt

Sobald ein Angriffsprozess automatisiert werden kann, geben sich Cyberkriminelle nicht mehr damit zufrieden, jeweils nur ein Opfer zu verfolgen. Mithilfe von Tools, die künstlicher Intelligenz, maschinellem Lernen und robotergestützter Prozessautomatisierung ähneln, können sie Dutzende oder Hunderte von Organisationen parallel ins Visier nehmen. Viele Opfer entscheiden sich dafür, Vorfälle nicht öffentlich bekannt zu machen, sodass Angreifer einen Erpressungszyklus abschließen und zu neuen Zielen übergehen können. Dieses skalierte, wiederholbare Geschäftsmodell – und nicht eine einzelne neue Technologie – ist der Hauptgrund, warum Ransomware-Angriffe weiter zunehmen.

https://player.vimeo.com/video/1043463561

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

Revision #1
Created 2026-07-24 05:06:29 UTC by Dennis Underwood
Updated 2026-07-24 05:06:29 UTC by Dennis Underwood