Warum ist Ransomware so schwer zu stoppen und wiederherzustellen?

Kurze Antwort: Ransomware hat sich von einem einfachen Hacking-Trick zu einer ausgereiften, geschäftsähnlich organisierten kriminellen Operation entwickelt, die mehrschichtige Verschlüsselung und verschwindende Schlüssel nutzt, um eine Wiederherstellung ohne Zahlung nahezu unmöglich zu machen. Wer versteht, wie die Verschlüsselung und die Schlüsselverwaltung tatsächlich funktionieren, erkennt, warum Backups, Beschlagnahmungen durch Strafverfolgungsbehörden und schnelle Lösungen oft nicht ausreichen.

Wie sich Ransomware von einem Datenschutzverstoß unterscheidet

Bei einem Datenschutzverstoß geht es darum, Informationen unauffällig zu stehlen und später zu verkaufen, während Ransomware-Akteure ein anderes Ziel verfolgen: so lange unbemerkt im Netzwerk zu bleiben, bis maximaler Schaden angerichtet werden kann, und sich dann zu offenbaren. Sobald der Schaden angerichtet ist, spielt es für sie keine Rolle mehr, sich zu verstecken. Diese Operation wird zunehmend automatisiert und wie ein Unternehmen betrieben, komplett mit Zahlungsabwicklung und einem „Kundenservice" für Entschlüsselung, da Angreifer eine zuverlässige Methode benötigen, um im großen Maßstab Geld einzutreiben.

Der Verschlüsselungstrick hinter dem Angriff

Ransomware setzt in der Regel auf zwei zusammenwirkende Verschlüsselungsarten. Eine schnelle symmetrische Verschlüsselung (wie AES) sperrt die eigentlichen Dateien, während eine langsamere asymmetrische Verschlüsselung – dieselbe Methode, die auch zur Absicherung von Webverkehr verwendet wird – den symmetrischen Schlüssel selbst schützt. Dies ist eine etablierte kryptografische Technik, die aus legitimen Sicherheitssystemen entlehnt wurde. Bei Ransomware bedeutet dies jedoch, dass selbst wenn der Schlüssel einer einzelnen Datei irgendwie wiederhergestellt werden könnte, Angreifer zusätzliche Komplexität eingebaut haben, sodass die Entschlüsselung einer Datei oft von der Erzeugung eines neuen Schlüssels für die nächste abhängt

– wodurch Abkürzungen weitaus schwieriger sind, als es zunächst klingt.

Warum die Wiederherstellungsoptionen immer schwächer werden

Frühe Ransomware verwendete einen einzigen Schlüssel für viele Opfer, was es Verteidigern gelegentlich ermöglichte, ein Entschlüsselungstool zu extrahieren und zu verbreiten. Angreifer reagierten darauf, indem sie einzigartige, einmalig verwendete Schlüssel erzeugten, die niemals an einem wiederauffindbaren Ort gespeichert werden. Dies eliminiert die Option der qu

https://player.vimeo.com/video/1065143398

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

Revision #1
Created 2026-07-24 05:07:37 UTC by Dennis Underwood
Updated 2026-07-24 05:07:37 UTC by Dennis Underwood