

Was passiert tatsächlich in den Momenten während eines Ransomware-Angriffs?

Kurze Antwort: Die eigentliche Verschlüsselungsphase eines Ransomware-Angriffs ist bemerkenswert schnell und dauert nach Auslösung oft nur etwa 60 bis 90 Sekunden, obwohl Angreifer zuvor erhebliche, unbemerkte Zeit damit verbringen, sich innerhalb eines Netzwerks zu positionieren. Wenn sichtbare Symptome auftreten, entfaltet sich der Schaden bereits in Echtzeit – weshalb die Erkennung vor dem endgültigen Auslöser erfolgen muss, nicht danach.

Die Ruhe vor dem Angriff

Bevor Ransomware jemals aktiviert wird, verbringen Angreifer typischerweise Zeit damit, sich unbemerkt durch die Systeme eines Unternehmens zu bewegen, wertvolle Daten zu identifizieren, Backups zu deaktivieren und die Bedingungen für einen erfolgreichen Angriff zu schaffen. Diese Vorbereitungsarbeit kann unbemerkt bleiben, da der normale Geschäftsbetrieb wie gewohnt weiterläuft. Das Netzwerk kann bis zu dem Moment, in dem der Angreifer beschließt, die finale Phase einzuleiten, stabil und unauffällig erscheinen. Ähnlich wie eine unheimliche Stille kurz vor einem katastrophalen Ereignis kann diese ruhige Phase trügerisch sein, da sie nicht die bevorstehende Störung widerspiegelt.

Der rasante Beginn des Schadens

Einmal ausgelöst, kann sich ein Ransomware-Ereignis in weniger als zwei Minuten vollständig entfalten. In diesem kurzen Zeitfenster bemerken Mitarbeitende möglicherweise plötzliche Ausfälle: E-Mail funktioniert nicht mehr, Telefonsysteme verstummen, Anwendungen verhalten sich fehlerhaft oder Netzwerkverbindungen werden instabil. Dies sind Symptome einer Verschlüsselung und Systemkompromittierung, die gleichzeitig in der gesamten Umgebung stattfinden. Da der Prozess so schnell abläuft, bleibt in der Regel nicht genug Zeit, um manuell einzugreifen, sobald er begonnen hat.

Warum manche Systeme weiterlaufen

Ein beunruhigendes Detail vieler Ransomware-Vorfälle ist, dass nicht alles gleichzeitig ausfällt. Manche Dienste laufen möglicherweise normal weiter, während andere zusammenbrechen. Dies liegt oft daran, dass genau diese nicht betroffenen Systeme der Ort sind, an dem der Angreifer noch aktiv ist, und sie als Stützpunkt oder Ausgangsbasis nutzt. Dieses Muster zu erkennen ist wichtig, da die Annahme, ein Problem sei „nur teilweise“ vorhanden, ein falsches Sicherheitsgefühl erzeugen kann, während die Kompromittierung aktiv fortschreitet. Eine wirksame Prävention hängt davon ab, bösartige Aktivitäten zu erkennen und zu stoppen, bevor die finale, zerstörerische Phase beginnt, da nach der Auslösung nur ein extrem kurzes Zeitfenster zum Handeln bleibt.

<https://player.vimeo.com/video/1046658956?texttrack=de>

[Auf Vimeo ansehen](#) · Untertitel: English, Français, Español, العربية

Revision #2

Created 2026-07-24 05:04:04 UTC by Dennis Underwood

Updated 2026-08-06 18:36:49 UTC by Dennis Underwood