

Was passiert tatsächlich, wenn Ransomware einen Unternehmensserver trifft?

Kurze Antwort: Wenn Ransomware einen Server trifft, deaktivieren Angreifer in der Regel zunächst dessen Dienste und verschlüsseln anschließend die Daten – dabei schneiden sie IT- und Sicherheitsteams vom Eingreifen ab und nutzen mitunter Dutzende oder sogar Hunderte kompromittierter Arbeitsstationen, um die Verschlüsselung remote durchzuführen.

Die ersten Anzeichen eines Angriffs

Eines der frühesten Anzeichen dafür, dass ein Server kompromittiert wurde, ist ein plötzlicher Dienstaussfall. Da Angreifer wissen, dass Ransomware Dateien während der Verschlüsselung versehentlich beschädigen kann, deaktivieren viele bewusst die auf einem Server laufenden Anwendungen, bevor der Verschlüsselungsprozess beginnt. Das bedeutet, dass Mitarbeiter oder Kunden, die auf dieses System angewiesen sind – sei es eine Gehaltsabrechnungsplattform, eine Webanwendung oder ein anderer geschäftskritischer Dienst – möglicherweise einen Ausfall bemerken, bevor jemand erkennt, dass ein Sicherheitsvorfall im Gange ist.

Verteidiger aussperren, während sich die Verschlüsselung ausbreitet

Sobald der Angriff im Gange ist, beginnt die Ransomware, die auf dem Server gespeicherten Daten zu verschlüsseln. Um zu verhindern, dass Sicherheitsteams oder Administratoren eingreifen, blockieren Angreifer häufig den Netzwerkzugriff auf den Server und isolieren ihn von den Personen, die normalerweise auf die Bedrohung reagieren würden. Diese Taktik verschafft dem Angreifer Zeit, die Verschlüsselung der Dateien abzuschließen, bevor Verteidiger handeln können.

Arbeitsstationen können die eigentliche Schwachstelle sein

Interessanterweise liegt die Gefahr nicht immer beim Server selbst. In vielen Fällen kompromittieren Angreifer eine große Anzahl von Mitarbeiter-Arbeitsstationen – manchmal 50, 70 oder mehr –, die bereits legitimen Zugriff auf den Server haben. Diese Arbeitsstationen werden dann gleichzeitig genutzt, um die Daten des Servers remote zu verschlüsseln. Da der Angriff von mehreren Endpunkten gleichzeitig ausgeht, stellen die mit dem Server verbundenen Arbeitsstationen oft eine größere Schwachstelle dar als die Serverinfrastruktur selbst.

Dieses Muster verdeutlicht, warum sich die Ransomware-Abwehr nicht ausschließlich auf Server konzentrieren darf. Endpunktsicherheit auf jedem Gerät mit Serverzugriff spielt eine entscheidende Rolle dabei, Angriffe zu stoppen, bevor sich die Verschlüsselung ausbreitet. Cyber Crucibles' FortressAI wurde entwickelt, um diese Verhaltensweisen bereits im frühesten Stadium zu erkennen und zu unterbrechen – unabhängig davon, ob die Bedrohung von einem Server ausgeht oder sich von verbundenen Arbeitsstationen ausbreitet.

<https://player.vimeo.com/video/1041172405?texttrack=de>

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

Revision #2

Created 2026-07-24 05:04:18 UTC by Dennis Underwood

Updated 2026-08-06 18:36:51 UTC by Dennis Underwood