



Quelle: Rawrifi – stock.adobe.com

## Ransomware-Angriffe in der Cloud

**Ransomware bleibt eine der größten Cyber-Bedrohungen für Unternehmen. In einer Zeit, in der immer mehr Daten in die Cloud wandern, zielen auch die Angreifer vermehrt auf dieses Ökosystem ab. Alte Sicherheitskonzepte greifen allerdings angesichts der neuen Infrastrukturen oft zu kurz.**

Spätestens seit dem großangelegten Angriff mit der Schadsoftware WannaCry im Jahr 2017 ist Ransomware im breiten Bewusstsein angekommen, obwohl das Prinzip bereits davor existierte. Auch heute nutzen Kriminelle diesen Angriffsvektor immer wieder, um Lösegeld von Unternehmen zu erpressen. Erst kürzlich war der Landmaschinenhersteller [Fendt](#) von einer Attacke betroffen, die die Produktion lahmlegte. Im letzten Jahr erreichten die Vorfälle in den USA sogar einen neuen Rekord, da Angreifer in verschiedenste Branchen expandieren und kritische Infrastrukturen ins Visier nehmen.

Dieser Trend setzt sich auch 2022 ungehemmt fort. Auch die Lösegeldforderungen sind gestiegen. Laut IT-Governance liegt der durchschnittliche Preis für einen Entschlüsselungsschlüssel bei 140.000 US-Dollar. Doch die Gesamtkosten, die durch einen Angriff entstehen können, liegen weit darüber.

Ransomware-Bedrohungen entwickeln sich so rasant weiter, dass IT-Teams den Überblick verlieren. Ein weit verbreiteter Irrglaube ist, dass die Schadsoftware in der Regel durch Phishing-E-Mails übermittelt wird. Das mag zwar in vielen Fällen zutreffen, aber die neueste Art von Ransomware wird meist direkt aus dem Netzwerk heraus gestartet. Daher

verschiebt sich der Fokus jetzt auf die Überwachung von Aktivitäten innerhalb der Unternehmensnetzwerke, anstatt Nutzer davon abzuhalten, auf unbekannte Links zu klicken.

Eine weitere veraltete Annahme ist, dass häufige Backups die beste Wiederherstellungsstrategie sind. Im Fall von simplen Attacken mag das zutreffend sein. Aber versierte Angreifer, die es bereits geschafft haben, in ein Netzwerk einzudringen, haben nicht nur die Möglichkeit, Backups zu kompromittieren, sondern auch kritische Daten herauszufiltern und weiterzuverbreiten.

### Hintertüren schließen

Der häufigste Angriffspunkt ist das Remote-Desktop-Protokoll (RDP), eine Funktion von Microsoft Windows, die es einem Computer ermöglicht, sich mit anderen zu verbinden, um eine grafische Benutzeroberfläche für Anwendungen wie gemeinsame Whiteboards anzuzeigen. RDP-Schwachstellen treten immer häufiger auf, wobei viele von ihnen auf eine schlechte Konfiguration oder versäumte Patches zurückzuführen sind. Dank umfangreicher Recherchen können Eindringlinge ihre Angriffe immer gezielter durchführen, um maximalen Schaden anzurichten. Die zunehmende Präzision der Angriffe ist ein Grund dafür,

dass Lösegeldforderungen steigen, obwohl Unternehmen immer mehr proaktive Maßnahmen zum Schutz ergreifen.

Kriminelle tauchen immer dort auf, wo es etwas zu holen gibt: Da immer mehr Daten in die Cloud verlagert werden, folgen ihnen auch Ransomware. Wenn man bedenkt, dass Angreifer dort noch mehr Daten in die Hände bekommen können, wird klar, warum die Cloud für sie so verlockend geworden ist.

Aus diesem Grund ist ein ganzheitlicher Schutz für Endgeräte, Web-Verkehr und Cloud-Umgebungen unerlässlich. Mit einer Security Service Edge (SSE)-Strategie, die auch Funktionen zur Verhinderung von Datenverlusten (DLP) umfasst, können Sicherheitsteams die Datenexfiltration automatisch blockieren und so die heutzutage häufig auftretenden doppelten Erpressungsversuche durch Ransomware verhindern.

## Vertraue niemandem

Ein wirksames Mittel gegen Eindringlinge im eigenen Netzwerk ist eine Zero-Trust-Architektur, die auf dem Prinzip der geringstmöglichen Rechte basiert: Nutzer erhalten nur die für die Ausführung ihrer Aufgaben erforderlichen Zugriffsrechte oder Berechtigungen. Ein echter Zero-Trust-Ansatz verbindet einen Benutzer direkt mit der Anwendung, die er benötigt, ohne dass das Netzwerk jemals offengelegt wird.

Sicherheitsteams können Benutzer kontinuierlich authentifizieren und sie direkt mit Anwendungen verbinden, anstatt dem Datenverkehr aus einem internen Netzwerk oder einem Unternehmensgerät zu vertrauen. Die Sicherheitsrichtlinien werden für jede einzelne Transaktion neu geprüft, statt nur einmal beim Aufbau einer Verbindung, wie es bei klassischem VPN-Verbindungen typisch ist.

Mikro-Segmentierung ist ein weiteres zentrales Zero-Trust-Konzept. Es beinhaltet die Einschränkung des Zugriffs auf Anwendungen und Ressourcen, so dass Angreifer, die in eine Anwendung eindringen, anderen keinen Schaden zufügen können. Es bekämpft auch die „Land-and-Expand“-Techniken, die Eindringlinge verwenden, um von einem Zugangspunkt zu anderen Zielen im Netzwerk zu gelangen.

Die Verwendung legitimer RDP-Dienste und gültiger Anmeldeinformationen stellt Sicherheitsteams weiterhin vor die Herausforderung, zwischen vertrauenswürdigen und böartigen Aktivitäten zu unterscheiden. User and Entity Behavior Analytics (UEBA) und auf Anomalien basierende Kontrollen können dabei helfen, unnormales und potenziell gefährliches Verhalten zu erkennen und einzudämmen. Durch die Analyse gängiger Verhaltensweisen können

Sicherheitsexperten Basiswerte normaler Aktivitäten für den jeweiligen Kontext erstellen, um davon abweichende Anomalien oder verdächtige Handlungen direkt zu erkennen.

Versicherungs- und Finanznachrichten

# expertenReport



<https://www.experten.de/id/4924432/ransomware-angriffe-in-der-cloud/>