Zscaler™ Workload Segmentation zur Abwehr von Ransomware

Sicherung der Ost-West-Kommunikation zwischen Anwendungen zur Verhinderung lateraler Bewegungen von Bedrohungen

Harry Sverdlove
Chief Technologist, Secure Workload Communication, Zscaler

Inhalt

Einleitung: US-Gesundheitswesen erneut im Visier von Ransomware-Angriffen

Im Krisenjahr 2020 blieb auch die Cyber-Sicherheit nicht vor Erschütterungen verschont. Erst kürzlich warnten die Cybersecurity and Infrastructure Agency (CISA), das Federal Bureau of Investigation (FBI) und das US-Gesundheitsministerium vor einem erhöhten Risiko im Gesundheitssektor durch eine Ransomware-Kampagne, der bereits mehrere Krankenhäuser in den USA zum Opfer gefallen waren.

Solche Angriffe sind nicht neu. 2019 wurden in den USA über 140 Ransomware-Angriffe auf staatliche Behörden und medizinische Einrichtungen gemeldet. Ransomware-Angriffe haben im Laufe der vergangenen zehn Jahre an Häufigkeit, Raffinesse und Effektivität zugenommen.

Bei Ransomware-Angriffen werden wichtige Dateien oder das ganze Betriebssystem eines Unternehmens verschlüsselt, sodass die User nicht mehr auf das System zugreifen können. Erst nach Zahlung eines Lösegelds (normalerweise in einer Kryptowährung) wird dem Opfer ein entsprechender Schlüssel zur Entsperrung der Ressourcen übermittelt. Es handelt sich also um finanziell motivierte Angriffe, die von organisierten Cyberkriminellen durchgeführt werden. In seltenen Fällen sollen diese Angriffe lediglich die Infrastruktur des Opfers außer Betrieb setzen. In aller Regel dienen sie rein der Erbeutung von Lösegeld.

Wie funktioniert Ransomware?

Damit Ransomware wirksam ist, muss sie so viele Systeme wie möglich innerhalb eines Netzwerks beeinträchtigen. Wenn beispielsweise nur eins von Tausenden von Systemen verschlüsselt und deaktiviert wurde, wird das Opfer mit hoher Wahrscheinlichkeit lediglich dieses eine System aus dem Netz nehmen und neu aufbauen. Je mehr Systeme oder Dateien betroffen sind, desto eher ist das Opfer geneigt, das Lösegeld zu zahlen. Den Empfehlungen der Strafverfolgungsbehörden und Cyber-Sicherheitsexperten zum Trotz, dass Opfer von Ransomware-Angriffen *niemals* ein Lösegeld zahlen sollten, ist in der Praxis die Versuchung groß, das Problem mit einer schnellen Zahlung zu beheben. Die Alternative wäre, täglich Millionenverluste durch Ausfallzeiten hinzunehmen und die Dateien in wochen- oder gar monatelanger Arbeit manuell wiederherzustellen.

Bei der aktuellen Kampagne gegen den US-Gesundheitssektor wird eine Phishing-E-Mail an Mitarbeiter des Unternehmens geschickt, auf die der Angriff abzielt. Die E-Mail enthält entweder einen Schadcode (als Anhang) oder einen Link zu einer schädlichen bzw. kompromittierten Website, auf der die Malware-

Nutzlast gehostet wird. Die Malware gehört zur TrickBot-Familie (und den damit verbundenen Trojanern BazarLoader/BazarBackdoorn).

TrickBot ist dann in der Lage, sich heimlich in verschiedene Windows-Prozesse zu installieren, eine Hintertür zu einem Command-and-Control-Server (C&C) einzurichten, zusätzliche Komponenten herunterzuladen, gängige Tools zur Katalogisierung des Netzwerks anzuwenden und sich schließlich im gesamten Netzwerk zu verbreiten. TrickBot verfügt zudem über spezifische Module, die sich über einen SMB-Exploit oder über Remote Desktop Protocol (RDP) auf Domain Controllern ausbreiten können.

Auf jedem von TrickBot infizierten Computer wird die Ransomware Ryuk (bzw. ihr Nachfolger Conti) heruntergeladen und gestartet. Sie ist in der Lage, sowohl lokale als auch auf Filesharing-Plattformen gespeicherte Netzwerkdateien zu verschlüsseln.

Ransomware-Angriffe folgen immer dem gleichen Muster:

1. Ein User wird zum Herunterladen und Ausführen einer schädlichen Loader-Datei verleitet (bzw. sie wird über ein Exploit ohne Wissen des Users installiert und ausgeführt).
2. Die Loader-Datei kontaktiert einen Server (oder andere Schadsysteme), um weitere Komponenten herunterzuladen.
3. Das Netzwerk wird zur Identifizierung weiterer Systeme und Filesharing-Plattformen überwacht.
4. So viele Systeme wie möglich werden infiziert, insbesondere Domain Controller und andere kritische Infrastrukturen.
5. Dateien werden verschlüsselt, um das System bzw. die Systeme entweder vollkommen außer Betrieb zu setzen oder den Zugriff auf bestimmte Daten zu verhindern.

Kleine Abweichungen im Ablauf und die Anwendung zusätzlicher Mittel zur Verschleierung und Zerstörung ändern nichts daran, dass das Grundmuster immer identisch ist.

Maßnahmen gegen Ransomware

Empfehlungen zur Abwehr von Ransomware-Angriffen beziehen sich zumeist auf den ersten und fünften Schritt der oben beschriebenen Angriffssequenz. Für den ersten Schritt wird empfohlen, durch Anwendung von E-Mail-Filtern und User-Schulungen zu verhindern, dass verdächtige Downloads oder Web-Links angeklickt werden. Das ist zwar nicht falsch, aber offensichtlich völlig unzureichend, wie die zunehmende Anzahl erfolgreicher Ransomware-Angriffe belegt. Angreifer wenden immer raffiniertere Taktiken an, sodass es zunehmend schwerer fällt, schädliche E-Mails von legitimen zu unterscheiden. Darüber hinaus nutzen sie andere Möglichkeiten, User auszutricksen – z. B. durch das Kompromittieren von Websites, die von den Opfern häufig besucht werden (eine Methode, die als Waterholing bezeichnet wird).

Die Empfehlung für den fünften Schritt lautet, einen zuverlässigen Backup- und Recovery-Plan einzurichten, sodass ein kompromittiertes und verschlüsseltes System im Ernstfall schnell gelöscht und wiederhergestellt werden kann. Diese Empfehlung ist sinnvoll, zumal sie auch die Notfallwiederherstellung nach Systemausfällen vereinfacht. Dabei ist allerdings zu bedenken, dass Ransomware-Angriffe erstens immer raffinierter werden und auch Sicherungskopien in Mitleidenschaft ziehen können. Und zweitens: Haben Sie schon einmal versucht, ein einziges System wiederherzustellen – geschweige denn einen Domain Controller oder Hunderte von Systemen, die über ein ganzes Unternehmen verteilt sind? Das ist eine äußerst mühselige Arbeit, die mehrere Wochen dauern kann, und Datenverluste sind dabei unvermeidlich.

Zscaler Workload Segmentation setzt beim zweiten bis vierten Schritt an. Wenn die schädliche Nutzlast ihren C&C-Server nicht kontaktieren kann oder verhindert wird, dass sie das Netzwerk überwacht und sich auf andere Systeme verbreitet, kann der Angriff im Idealfall ganz vereitelt oder zumindest sein Umfang minimiert werden.

Hier ist ein Zero-Trust-Ansatz zur Überprüfung des lateralen Traffics am effektivsten. Zero Trust bedeutet, dass nur befugte Entitäten – also z. B. Anwendungen, User und Geräte – mit anderen befugten Entitäten kommunizieren können. Dieser Ansatz beruht auf der Annahme, dass das Netzwerk selbst mitsamt seiner Adressen/Ports/Protokolle inhärent unsicher ist. Ob eine Kommunikation als vertrauenswürdig eingestuft wird, hängt nicht nur vom Kommunikationspfad (wie wird kommuniziert?), sondern auch von den beteiligten Entitäten (wer kommuniziert?) ab.

In den meisten Netzwerken wird die Kommunikation zwischen Systemen innerhalb desselben Netzwerks unzureichend kontrolliert. Mindestens 87 Prozent der zugelassenen Pfade in den meisten Unternehmensnetzwerken werden entweder nicht genutzt oder nicht benötigt. Dieser Kontrollmangel ist darauf zurückzuführen, dass herkömmliche Firewalls nicht das notwendige Maß an Granularität bieten, um den Traffic tatsächlich auf der Grundlage der Entitäten zu beschränken, die diese Verbindungen nutzen. Einmal angenommen, ein Unternehmen arbeitet mit Active Directory und für die Kommunikation zwischen Domain Controllern und Clients werden die Ports 88 und 135 benötigt. Mit einer herkömmlichen Firewall kann der Traffic bestenfalls basierend auf den IP-Adressen des Netzwerks und dieser Ports eingeschränkt werden. Dadurch lässt sich nicht verhindern, dass ein Schadcode über genau diese Adressen und Ports mit dem Controller kommuniziert, um Informationen zu sammeln oder einen Exploit zu platzieren.

Next-Generation Firewalls (NGFWs) können den Traffic zwar auf Abweichungen von den erwarteten Mustern überprüfen. Sie lassen sich jedoch umgehen, indem Schadcode mithilfe entsprechender Syntax als „legitim“ getarnt wird. Hinzu kommt, dass NGFWs verdächtigen Code erst erkennen, wenn die Verbindung

bereits zustande gekommen ist. Bei bestimmten Exploits ist der Schaden zu diesem Zeitpunkt längst angerichtet. Weiter ist zu bedenken, dass die Bereitstellung von NGFWs an jeder Verbindungsstelle zwischen Systemen nicht nur mit hohen Kosten verbunden ist, sondern auch zu beträchtlichen Netzwerkverzögerungen führen kann – das gilt für physische Netzwerke ebenso wie für virtualisierte Cloud-Umgebungen.

Zscaler Workload Segmentation (ZWS) verfolgt einen anderen Ansatz zur Mikrosegmentierung, der Netzwerksicherheit durch Überprüfung der Identität aller kommunizierenden Anwendungen und Dienste gewährleistet. Dadurch wird unbefugte und schädliche Software auch dann an der Kommunikation gehindert, wenn sie Adressen, Ports und Protokolle verwendet, die von herkömmlichen Firewalls als vertrauenswürdig eingestuft und zugelassen werden – und sogar dann, wenn sie die Paketprüfung innerhalb der NGFW durch Tarnung mit „legitimer“ Syntax umgehen kann.

Der Einsatz identitätsbasierter Mikrosegmentierung im Unternehmensnetzwerk bietet viele weitere Vorteile, darunter eine einfachere Bereitstellung (keine Änderung der Infrastruktur erforderlich), Policy-Komprimierung und einfachere Verwaltung (wesentlich weniger Richtlinien erforderlich), automatisch skalierende Richtlinien (da die Richtlinien auf der Identität und nicht auf den Netzwerkadressen basieren) und verbesserte Netzwerktransparenz durch Einblick in die Kommunikation zwischen Anwendungen statt nur zwischen Adressen. Aus rein sicherheitstechnischer Sicht würde die identitätsbasierte Sicherheit von ZWS im oben beschriebenen Fall verhindern, dass eine schädliche Loader-Datei zusätzliche Komponenten herunterlädt, systeminterne Software zur Überwachung und Katalogisierung des Netzwerks ausnutzt und weitere Systeme über RDP oder PSEXEC infiziert.

Zuverlässige Abwehr durch Unterbrechung der Angriffssequenz

Die Schulung von Usern zur Abwehr von Phishing-Angriffen und eine Backup-Strategie für die Notfallwiederherstellung sind sinnvolle Strategien, die jedoch alleine nicht zur Verhinderung erfolgreicher Ransomware-Angriffe ausreichen. In beinahe allen Phasen eines Ransomware-Angriffs spielt die unbefugte Kommunikation schädlicher oder kompromittierter Software eine Rolle. Herkömmliche Firewalls können dagegen nichts ausrichten. Die identitätsbasierte Segmentierung mit ZWS hingegen verhindert zuverlässig die Ausbreitung von Ransomware in der IT-Umgebung. Damit sind Unternehmen Ransomware-Angriffen nicht mehr wehrlos ausgeliefert.

Hinweis: Ryuk und Conti werden von Zscaler Threat Library und Cloud Sandbox erkannt.
Weitere technische Angaben dazu erhalten Sie hier.