AKAMAI-KUNDENREFERENZ

Anbieter von Kommunikationsinfrastruktur

Stoppt Ransomware frühzeitig mit Akamai

Verhinderung des potenziellen Verlustes von 1 Million US-Dollar

Verhinderung von potenzieller Shadow-IT

Transparenz im Bereich East-West-Traffic

Der Kunde

Der in den USA ansässige Anbieter von Kommunikationsinfrastruktur gewährleistet, dass Unternehmen und Menschen in der schnelllebigen Welt von heute miteinander verbunden bleiben. Er ist verantwortlich für ein breites Netz an Mobilfunkmasten und Glasfasernetzwerken, auf die sich seine Kunden im Alltag verlassen.

Die Herausforderungen

Eingeschränkte Transparenz und Kontrolle am Endpoint

Da im gesamten Unternehmen mehr als 6.000 Laptops verwendet werden, hatte das IT-Team zunehmende Bedenken hinsichtlich des Risikos der Flotte für die gesamte IT-Umgebung. Außerdem traten wiederholt Probleme im Zusammenhang mit Aktivitäten aus dem Bereich Shadow-IT durch die Poweruser des Unternehmens auf, die angegangen werden mussten.

Das Team für Endnutzerinformatik führte zwar einige Sicherheitsmaßnahmen ein, die aber an ihre Grenzen stießen. Keine dieser Maßnahmen konnte den Systemzugriff für Nutzer detailliert kontrollieren oder die Peer-to-Peer-Kommunikation einschränken, um die Verbreitung von Malware effizient aufzuhalten. Letztere stellte ein großes Problem für die Firma dar.

Um diese Lücken anzugehen, wollten die Verantwortlichen die Sicherheitsstrategie des Unternehmens verbessern. Dafür sollte eine Lösung eingeführt werden, die es erlauben würde, Transparenz und detaillierte Segmentierungskontrollen auf die Endgeräte der Mitarbeiter zu erweitern. Dies sollte es außerdem ermöglichen, laterale Netzwerkbewegungen zu beobachten und zu verhindern.

Auswahl der richtigen Lösung

Die Sicherheitsverantwortlichen hatten die Akamai Guardicore Segmentation bereits seit einiger Zeit in Betracht gezogen und sie interessierten sich für deren Nutzung für verschiedene Anwendungsfälle im Bereich der Cybersicherheit. Das Unternehmen entschied sich für ein stufenweises Vorgehen, um das große Potenzial der detaillierten Transparenz und der einfachen Erstellung von Richtlinien auszuschöpfen.

Anbieter von Kommunikations-infrastruktur

Standort
USA

Branche
Kommunikationsinfrastruktur

Lösung
Akamai Guardicore Segmentation

Die wichtigsten Vorteile

- Ransomware vorbeugen
- Shadow-IT stoppen
- Transparenz im Bereich East-West-Traffic

Da die softwaredefinierten Segmentierungsrichtlinien von Akamai nicht an die zugrunde liegende Infrastruktur gebunden sind, hatte der Provider die Möglichkeit, eine beliebige Menge an Sicherheitsinitiativen in Angriff zu nehmen. Die Laptopflotte der Mitarbeiter wurde jedoch als besonders risikobehaftet eingestuft, sodass das Team der Implementierung von Akamai-Agents an den Endgeräten Priorität einräumte.

Akamai Guardicore Segmentation

Nach dem Projektstart konnte die Einführung des optimierten Windows-Agent an den Computern des Unternehmens zügig erfolgen. Dies erhöhte die Transparenz in Bezug auf den Nutzerzugang und die Laptop-Aktivität auf Prozessebene.

Das IT-Sicherheitsteam war dann in der Lage, Sicherheitskontrollen für diese Endgeräte zentral zu initiieren und zu verwalten, was vollumfassend auf akkuraten Umgebungsdaten basierte. Dann wurden zeitnah verschiedene Richtlinien eingeführt, einschließlich eines Alarms in Bezug auf spezifische Microsoft-RDP-Aktivitäten (Remote Desktop Protocol), zum Beispiel fehlgeschlagener Anmeldeversuche.

Umfassende Transparenz in der Praxis

Schon kurz nach der Implementierung lieferte die für die Meldung ungewöhnlicher RDP-bezogener Aktivitäten konfigurierte Richtlinie zahlreiche Alarmmeldungen. Da ein fehlgeschlagener Anmeldeversuch auf den nächsten folgte, wurde schnell deutlich, dass Cyberkriminelle einen Brute-Force-Angriff versuchten.

Das IT-Sicherheitsteam beobachtete die Situation genau. Da die Angriffe andauerten, wurde beschlossen, RDP an allen Endgeräten mit einem Agent von Akamai zu blockieren. Mit nur wenigen Klicks wurde eine neue Segmentierungsrichtlinie geschaffen und in Kraft gesetzt, die RDP deaktivierte. So konnte der Angreifer gestoppt werden, bevor auch nur ein einziges Endgerät kompromittiert wurde.

Ransomware frühzeitig gestoppt

Bei der Nachbereitung erkannte das IT-Team schnell, dass alle Anzeichen auf einen großen und bekannten Ransomware-Akteur hindeuteten.

Wäre der Angriff erfolgreich gewesen, hätten die Angreifer wahrscheinlich versucht, mit ihren üblichen Taktiken fortzufahren und alles in ihrer Reichweite zu verschlüsseln, um dann eine Lösegeldforderung zu stellen. Aufgrund der Unternehmensgröße des Providers und der aktuellen Trends hätten die Cyberkriminellen schätzungsweise mehr als 1 Million US-Dollar gefordert. Dies hätte erhebliche zusätzliche Unterbrechungen und Ausfallzeiten mit sich gebracht, falls unternehmenskritische Ressourcen wie das ERP-System kompromittiert worden wären.

Dank dem schnell handelnden Sicherheitsteam und Akamai hatte der Angriffsversuch jedoch keinerlei Auswirkungen auf das Unternehmen.

Shadow-IT stoppen

Zusätzlich zum Schutz vor äußeren Bedrohungen konnte das Team mithilfe der Plattform auch interne Herausforderungen angehen. Vor der Implementierung von Akamai war es aufgrund der eingeschränkten Transparenz an den Endgeräten für manche Nutzer einfach, offizielle Prozesse zu umgehen und eigenständig Aktivitäten durchzuführen, die den Richtlinien des Unternehmens nicht entsprachen. Die neuen Einblicke und die Möglichkeit, Sicherheitskontrollen an Endpunkten durchzusetzen, erlaubte dem Team für IT-Sicherheit die Eindämmung von Shadow-IT. So konnten unter anderem DevOps-Angehörige daran gehindert werden, eigenständig neue Ressourcen zu erschließen, ohne im Vorfeld eine offizielle Genehmigung einzuholen.

Erweiterter Schutz mit Akamai

Für den Anbieter von Kommunikationsinfrastruktur ist der Schutz der Endpoints nur der Anfang. Das Unternehmen plant, neue Funktionen ausprobieren und Akamai für sein Rechenzentrum zu implementieren, seine Citrix-Umgebung zu sichern und den Zugriff durch Dritte für externe Anbieter zu kontrollieren.

Durch die flexible Beschaffenheit der Plattform kann das Team darauf vertrauen, dass es den Schutz vor Advanced Threats auf jeden Bereich der Umgebung erweitern kann – unabhängig davon, wie sich die Fusions- und Übernahmestrategie oder die Initiativen für die digitale Transformation in der Zukunft entwickeln werden.

Weitere Informationen finden Sie unter akamai.com/guardicore.

 | Support | Veröffentlicht: 05/23