Akamai-Kundenreferenz

US-amerikanisches Gesundheitsunternehmen wehrte auf eine intelligente Art und Weise 4.000 Cyberangriffe an einem Tag ab

Network Engineers setzten auf Layer-7-Transparenz und intelligente Richtlinien mit Mikrosegmentierung, um Cyberrisiken zu verringern

Vereitelte Ransomware

Erhöhte Transparenz

Verbesserte Richtlinien

Sicherstellung wichtiger Gesundheitsleistungen für Patienten

Stellen Sie sich vor, Sie müssten ein Netzwerk schützen, das sich direkt auf das Leben der Patienten auswirkt, und gleichzeitig den immer komplexeren Cyberangriffen einen Schritt voraus sein. Vor dieser Herausforderung stand ein mittelständisches Gesundheitsunternehmen. Das Network-Engineering-Team sah sich mit wachsenden Ransomware-Bedrohungen und mangelnder Transparenz konfrontiert. Daher wandte sich das Team an Akamai Guardicore Segmentation, um die Sicherheitslage des Unternehmens zu verbessern.

Ausweitung der Zero-Trust-Architektur

Das Unternehmen hatte eine ehrgeizige Vision: Die IT-Umgebung sollte durch die Einführung von Zero-Trust-Prinzipien gestärkt werden und die HIPAA- und SOC-2-Compliance-Anforderungen erfüllen. Da viel auf dem Spiel stand, setzte sich das Network-Engineering-Team unter anderem folgende Ziele:

- Aufrechterhaltung des Betriebs kritischer Anwendungen auch bei Sicherheitsvorfällen
- Verringerung der Auswirkungen von Ransomware-Angriffen durch Eindämmung ihrer Verbreitung
- Erreichen einer detaillierten Netzwerktransparenz, die weit über herkömmliche Firewalls hinausgeht

Das Unternehmen benötigte eine kostengünstige, skalierbare Mikrosegmentierungslösung, bei der die bestehende IT-Infrastruktur nicht umgestaltet oder ersetzt werden musste. Außerdem sollte die Lösung so einfach sein, dass sie von einem kleinen Team verwaltet werden kann, und sie sollte skalierbar sein, um mit dem Unternehmen wachsen zu können.

Ein Network Engineer erklärt: „Ransomware zielt auf die Gesundheitsversorgung ab. Je schneller wir diese Bedrohungen isolieren und beseitigen können, desto besser."

Healthcare Company

Standort

USA

Branche

Gesundheitswesen und Life Sciences

Lösung

Akamai Guardicore Segmentation

Akamai

Die Suche nach der richtigen Mikrosegmentierungslösung

Nachdem das Unternehmen eine Containerisierung schnell verworfen hatte, wurden Mikrosegmentierungslösungen evaluiert. „Wir wollten die gleichen Vorteile wie bei den Firewalls der nächsten Generation, nämlich Transparenz auf der Anwendungsebene“, erklärt der Netzwerkingenieur.

Bei der Evaluierung zahlreicher Lösungen stieß das Unternehmen auf Akamai Guardicore Segmentation. Eine überzeugende Demo, gepaart mit praktischem Support durch die Ingenieure von Akamai, gaben den Ausschlag. Die Lösung erfüllte alle Kriterien, darunter:

- **Erhöhte Transparenz:** Layer-7-Untersuchung und umfassende Einblicke in das Netzwerk
- **Einfache Bereitstellung:** Softwarebasierte Mittel ohne zusätzliche Hardware
- **Ausfallsicherheit:** Kein einziger Single Point of Failure im Kernnetzwerk
- **Flexibilität:** Unterstützung für verschiedene Betriebssysteme

Laut dem Vice President of IT Infrastructure and Information Security ist Akamai Guardicore Segmentation für kleine Teams besonders vorteilhaft. „Gleich nach der Implementierung haben wir Vorteile hinsichtlich Transparenz und Kontrolle festgestellt.“

„Wir müssen nicht mehrere East-West-Firewalls anschaffen und verwalten, was enorme Kosteneinsparungen mit sich bringt, und erhalten außerdem ein Maß an Transparenz, das uns Firewalls nicht bieten können“, fügt der Manager of IT Infrastructure hinzu.

Ransomware frühzeitig gestoppt

Die beeindruckenden Ergebnisse zeigten sich sofort. Durch eine bessere Eingrenzung der Anwendungen und die Einführung der sofort umsetzbaren Ransomware-Präventionsrichtlinien von Akamai Guardicore Segmentation konnte das Team bereits am ersten Tag 4.000 Cyberangriffe neutralisieren. Mit der Lösung können die Richtlinien sogar an die spezifischen Anforderungen des Unternehmens angepasst werden.

„Für die allgemeinen Richtlinien haben wir den Alarmmodus verwendet, um Vorfälle zu melden, ohne Ausfallzeiten zu verursachen. So können wir Richtlinien kontinuierlich verfeinern“, so der Network Engineer.

> “Akamai Guardicore Segmentation hat uns nicht nur geholfen, unsere Probleme mit Ransomware zu beheben – wir konnten sogar unsere Cybersicherheit verbessern.
>
> – Network Engineer

> „Den ‚Zero-Trust-Gipfel' zu erklimmen ist eine unglaubliche Herausforderung. Mit Akamai Guardicore Segmentation haben wir nicht nur diesen Gipfel schnell erklommen, sondern auch die Kosten und Komplexität reduziert."
>
> — Vice President of IT Infrastructure and Information Security

Einzigartige Layer-7-Erkenntnisse

Laut dem Manager of IT Infrastructure bietet Akamai Guardicore Segmentation wertvolle Einblicke in den Traffic zwischen verschiedenen Anwendungen. Das war für das Team eine wahre Fundgrube an Daten. Das Team konnte nun über die Layer-4-Protokolle hinaus detaillierte Daten untersuchen: Nutzer-IDs, Befehlszeileneingaben und sogar Dienstkorrelationen.

„Unser Netzwerkteam kann den Traffic untersuchen, um Probleme zu beheben, und unserem Sicherheitsteam die Informationen zur Verfügung stellen, die es zur vollständigen Untersuchung von Vorfällen benötigt", so der Network Engineer.

Diese Transparenz erwies sich bei einem unerwarteten Richtlinienverstoß als sehr nützlich. Ein neuer Mitarbeiter schloss einen PC direkt an die Kundenendgeräte (Customer Premises Equipment, CPE) seines Netzbetreibers statt an einen LAN-Port an, der durch einen Router für den internen Gebrauch abgeschirmt war. Dies war ein absolutes No-Go, da das CPE dem PC eine öffentliche IP zuwies, was ihn anfällig für öffentliche Internet-Scans machte.

Der Network Engineer des Unternehmens führt aus: „Akamai Guardicore Segmentation hat das Problem sofort erkannt, sodass wir den PC isolieren konnten und die Situation nicht eskaliert ist. So kamen wir auch auf die Idee, eine Richtlinie zu erstellen, die solche Vorfälle in Zukunft verhindern soll."

Intelligentere Kennzeichnung, bessere Richtlinien

Dank der intuitiven Kennzeichnung und Erstellung von Richtlinien konnte das Network-Engineering-Team den Traffic leicht zuordnen und Sicherheitsregeln durchsetzen. „So konnten wir sehen, was für unsere Umgebung am besten geeignet ist", so der Network Engineer. „Das war sehr beeindruckend und in diesem Ausmaß völlig unerwartet – dadurch konnten wir auch Richtlinien effizient erstellen."

Das Team konnte beispielsweise den Zugriff auf Druckserver einschränken und nur vertrauenswürdige Zonen zulassen – ein schneller Erfolg, der die allgemeine Sicherheitslage des Unternehmens verbesserte. „So konnten wir sofort Probleme angehen, die am leichtesten zu beheben waren", so der Ingenieur weiter.

Stärkeres Vertrauen durch Transparenz

Mit welchem Vorteil wir nicht gerechnet hatten? Dass wir einen klaren Überblick über den internen Traffic und das Anwendungsverhalten erhalten haben. Diese neu gewonnene Transparenz verbesserte nicht nur die Zusammenarbeit mit den Anwendungseigentümern, sondern auch die Wartungsfenster. So kann z. B. das Team den Anwendungseigentümern zeigen, ob ihr Traffic blockiert wird.

„Früher stellten Fehlerbehebung und Zukunftssicherheit ein Problem dar. Jetzt können wir bei Umstellungen sicher feststellen, wann der Traffic von alten auf neue Server übertragen wird. So konnten wir Altsysteme mit Sicherheit außer Betrieb nehmen“, so der Network Engineer.

Der Vice President of IT Infrastructure and Information Security des Unternehmens fasst zusammen: „Akamai Guardicore Segmentation hat bereits Wirkung gezeigt und ist zu einem wichtigen Aspekt unserer Sicherheit geworden. Ich freue mich darauf, diese Lösung unternehmensweit zu implementieren.“

 | Veröffentlicht: Februar 2025