Akamai-Kundenreferenz

Schulbezirk in den USA verhinderte Insiderbedrohungen

Ein großer Schulbezirk in Texas setzte Mikrosegmentierung von Akamai ein, um den East-West-Traffic zu schützen

Gesicherte Anwendungen

Interne Angriffe verhindert

Bereitgestellte Traffic-Ansicht

Führend im Bereich Bildung

Im Jahr 2022 erhielt ein großer Schulbezirk in Texas mit über 75.000 Schülern von der Texas Education Agency die Note „A“. Der Bezirk ist führend in der Bildungsqualität und bietet beispiellose Lernerfahrungen, mit denen die Schüler bestmöglich auf das spätere Leben vorbereitet werden sollen. Zu diesem Zweck konzentriert sich die Abteilung „Technology Operations“ des Bezirks darauf, eine erstklassige Infrastruktur aufzubauen und zu erhalten, um die Sicherheit digitaler Inhalte und Tools von heute und morgen für alle Stakeholder zu gewährleisten. Als der neue Leiter der Abteilung für Cybersicherheit eine Schwäche im Sicherheitsansatz des Bezirks erkannte, konnte diese Lücke mit Akamai Guardicore Segmentation geschlossen werden.

Verhinderung von Bedrohungen durch Insider

Der Schulbezirk in Texas verließ sich bisher auf Firewalls und Geofencing, um seine IT-Umgebung vor externen Bedrohungen zu schützen. Es fehlte jedoch eine Möglichkeit, interne Bedrohungen abzuwenden – insbesondere Insiderbedrohungen mit böswilliger Absicht. „Wer Zugriff auf ein System hatte, hätte auch ganz einfach auf jedes andere System zugreifen können“, erklärt der Manager of Systems Engineering des Bezirks.

Texas School District

Standort

Texas, USA

Branche

Öffentlicher Sektor

Lösung

Akamai Guardicore Segmentation

Akamai

Da der Schulbezirk keinen Einblick in die legitime Kommunikation zwischen internen Systemen hatte, konnte unrechtmäßiger, bösartiger East-West-Traffic nicht unterbunden werden. Die Abteilung „Technology Operations“ – bestehend aus Netzwerk- und System-Engineering sowie Cybersicherheit – erkannte die damit verbundene Bedrohungslage und die Notwendigkeit einer umfassenden Lösung zur Risikominderung. „Wir wären nachlässig, wenn wir keine Lösung zur Gewährleistung der vollen Sicherheit der Daten unserer Schüler und Mitarbeitenden einrichten würden“, fuhr der Manager fort.

Einfache schrittweise Einführung von Mikrosegmentierung

Nachdem der Bezirk seine Optionen geprüft hatte, entschied man sich für Akamai Guardicore Segmentation. „Es war eine der besten verfügbaren Lösungen für unsere Zwecke“, so der Manager.

Die Abteilung „Technology Operations“ überprüfte ihre Umgebung, um die Anwendungen und Systeme zu identifizieren, die von Akamai Guardicore Segmentation geschützt werden sollten. „Wir begannen zunächst mit unseren Tier-1-Anwendungen, es war jedoch unser Ziel, alles mit der Lösung zu schützen“, fuhr der Manager fort.

Mit der Unterstützung von Akamai trennte der Bezirk prioritäre Anwendungen wie Active Directory und SQL Server einfach und schnell mit präzisen Segmentierungsrichtlinien voneinander, um unerwünschten Datenfluss zwischen den Systemen zu vermeiden. Der Prüfungs- und Bereitstellungsprozess förderte die funktionsübergreifende Zusammenarbeit. „Es war eine gemeinsame Anstrengung, zu bestimmen, wie wir die einzelnen Elemente benennen, Abschirmungen einrichten und vieles mehr. Auf diese Weise hat uns Akamai Guardicore Segmentation eine gemeinsame Grundlage für eine enge Zusammenarbeit bereitgestellt.“

Sobald eine Abschirmung eingerichtet war, wurde der Schulbezirk auf mögliche Probleme aufmerksam gemacht. „Es konnte kein Traffic durchkommen, wenn wir es nicht erlaubten“, erklärte der Manager of Systems Engineering des Schulbezirks. Daher war der Bezirk sicher, dass die Lösung von Akamai diese Anwendungen sofort schützte.

„Sobald wir ein Gefühl für den ein- und ausgehenden Traffic einer Anwendung bekamen, gingen wir bei Bedarf in den Sperrmodus. Akamai Guardicore Segmentation bietet einen unkomplizierten Weg, um diesen Schutz in unserer gesamten Umgebung einzurichten“, so der Manager.

> Akamai Guardicore Segmentation bietet einen unbezahlbaren Einblick in unsere Umgebung und trägt dazu bei, dass unsere kritischen Systeme vor nicht autorisiertem East-West-Traffic geschützt sind.
>
> – Manager of Systems Engineering, Texanischer Schulbezirk

> „Wir lieben Akamai Guardicore Segmentation. Es ist einfach zu konfigurieren und zu verwalten und stellt eine wertvolle Lösung für jeden Schulbezirk dar, der sich vor internen Bedrohungen schützen möchte."
>
> — Manager of Systems Engineering, texanischer Schulbezirk

Mehr Transparenz in der gesamten Umgebung

Obwohl eine solche Abschirmung für einige Anwendungen nicht möglich ist, profitierte der Schulbezirk dennoch von der neuen Transparenz der Kommunikation zwischen diesen Anwendungen und anderen wie Active Directory. Alle Gruppen innerhalb der Abteilung „Technology Operations" können Datenflüsse von und zu jeder abgegrenzten Anwendung sehen, und erhalten so im Wesentlichen einen Einblick, was in allen Systemen in der Umgebung geschieht. „Akamai Guardicore Segmentation bietet einen aktuellen Überblick über den Stand der Dinge und eine einfache Möglichkeit, unerwünschten Traffic zu identifizieren. Darüber hinaus können wir die Lösung so konfigurieren, dass Traffic zugelassen oder bei Bedarf blockiert wird", so der Manager.

Diese Transparenz ermöglicht es den Teams für Netzwerk- und System-Engineering sowie Cybersicherheit, bei Bedarf zusammenzuarbeiten, um auftretende Probleme direkt zu lösen. „Wenn wir auf verdächtigen Traffic aufmerksam gemacht werden, liefert die Lösung von Akamai den Kontext, den wir benötigen, um eine Lösung zu finden, die unerwünschte Ereignisse verhindert und gleichzeitig gewährleistet, dass unsere Umgebung bedarfsgerecht funktioniert", erläutert der Manager.

Verhindern von unbefugtem Remote-Zugriff

Laut dem Manager of Systems Engineering des Schulbezirks hilft Akamai Guardicore Segmentation kontinuierlich dabei, Cyberangriffe abzuwehren: „Unsere Systeme werden regelmäßig von bösartigen IP-Adressen angegriffen. Die Lösung von Akamai bietet einen Überblick über ungewöhnliche Aktivitäten, wie z. B. ungewöhnliche Portaktivitäten auf einem Webserver, sodass wir den Zugriff und damit potenzielle Angriffe blockieren können."

Durch die nahtlose Zusammenarbeit mit anderen Sicherheitstools erhöht Akamai Guardicore Segmentation die Sicherheit des Bezirks weiter. Beispielsweise verwendet der Schulbezirk eine PAM-Lösung (Privileged Access Management), um externen Anbietern den erforderlichen Zugriff auf bestimmte Systeme zu ermöglichen. Statt den RDP-Zugriff (Remote Desktop Protocol) auf diese Server zu ermöglichen, muss die technische Abteilung des Bezirks die PAM-Lösung zur Remote-Verwaltung von Servern verwenden. Und Akamai Guardicore Segmentation hilft dabei, diesen RDP-Zugriff zu verhindern.

Wie der Manager of Systems Engineering des Schulbezirks erläuterte, verhindert diese kombinierte Sicherheitsmaßnahme, dass Mitarbeiter remote auf Server zugreifen können, wie es in der Vergangenheit noch möglich war: „Durch den Einsatz der Lösung von Akamai zum Blockieren des RDP-Zugriffs können wir sicherstellen, dass niemand eine Remote-Verbindung zu unserer Serverumgebung herstellt."

Sicherere Bereitstellung von Anwendungen

Stand heute hat der Schulbezirk Akamai Guardicore Segmentation auf 375 der 500 bestehenden Server implementiert und plant, jede Anwendung mit der Mikrosegmentierungslösung zu schützen. „Wir führen ständig neue Anwendungen ein – manchmal sogar eine pro Woche –, und sichern sie von Anfang an mit der Lösung von Akamai. Dies verleiht uns ein Gefühl der Sicherheit, wenn wir neue Anwendungen bereitstellen, da wir mit Akamai Guardicore Segmentation visualisieren können, wie unsere Apps funktionieren und kommunizieren", so der Manager of Systems Engineering des Bezirks.

 | Veröffentlicht: November 2024