AKAMAI-KUNDENREFERENZ

Staatliche Universität in den USA wählt Akamai, um kritische Gebäudetechnologien von 24 Campus zu schützen

Umfassende Netzwerktransparenz

Segmentierungsrichtlinien

Bedrohungserkennung und -Reaktion

Der Kunde

Eine große staatliche Universität in den USA

Die große staatliche Universität mit 24 Campus zählt mehr als 100.000 Studierende und über 17.000 Lehrkräfte und Mitarbeitende.

Die Herausforderung

Zentralisierung der Netzwerkinfrastruktur von mehr als 600 Gebäuden

Eine bekannte staatliche Universität in den USA wollte Gebäudeautomatisierungssysteme sicher in eine landesweite Smart-Campus-Initiative integrieren. Das für die physischen Anlagen und die OT-Systeme der Universität zuständige Team hatte Bedenken hinsichtlich der fehlenden Segmentierung zum Schutz der Geräte und Anwendungen. Auch die Entfernung des bestehenden Air Gaps des IT-Netzwerks der Universität bereitete Sorge. Das verantwortliche Team machte sich daher daran, die Gebäudeautomatisierungssysteme zu zentralisieren und die Sicherheit zu erhöhen.

Der Projektleiter der Universität erklärt: „Bis vor etwa zwei Jahren waren alle Campus relativ eigenständig. Wir stellten den Hauptanwendungsserver bereit, aber die einzelnen Campus-Controller befanden sich in IT-Netzwerken und waren nicht immer in separaten VLANs vom Rest des Campus-Traffics getrennt."

Dies bedeutete, dass sich ein erfolgreicher Angriff auf die Steuersysteme eines Gebäudes problemlos auf das komplette IT-Netzwerk eines Campus ausbreiten konnte oder umgekehrt.

Das Projekt hatte außerdem einen wirtschaftlichen Grund. „Die Universität wollte im Rahmen ihres Energiemanagements prüfen, wo wir Kosten sparen können", erklärt der Projektleiter. „Aufgrund der Eigenständigkeit der Systeme erhielten wir jedoch keinerlei Daten von den Campus."

Eine sichere Verbindung war nötig, damit Angreifer die entfernten Campus nicht als Hintertür nutzen konnten, um auf das Rechenzentrum zuzugreifen.

Große staatliche Universität

Branche
Bildung

Lösung
Akamai Guardicore Segmentation

Die wichtigsten Vorteile
- Laterale Netzwerkbewegung verhindern
- Ringfencing für Anwendungen

Akamai

Das ehrgeizige Projekt, mit dem alles in einer gemeinsamen Netzwerkinfrastruktur zusammengebracht werden sollte, umfasste mehr als 600 Gebäude auf 24 Campus. Das Facility Automation Team der Abteilung wurde mit der Durchführung des Projekts beauftragt.

Die Komplexität der Automatisierungssysteme der Universität und die Anzahl der beteiligten Anbieter erwies sich jedoch als eine weitere enorme Herausforderung.

„Wir verwalten Aufzugssysteme, Klimaanlagen, Schwingungsanalyse, Beleuchtung sowie die Stromverteilung und -messung. Hinzu kommen unsere wichtigsten Versorgungseinheiten, wie die Dampferzeugung, die Stromversorgung und die Abwasserbehandlung. Wir beschäftigen mehr als 260 Auftragnehmer für die Verwaltung aller dieser Systeme." Sie alle benötigen Zugriff auf das Netzwerk, ohne dessen Sicherheit zu gefährden oder die unterschiedlichen Kontrollsysteme zu stören.

> Ein Firewall-Management-System kann nicht mit [Akamai] konkurrieren.
>
> Projektleiter der Universität

Auswahl der richtigen Lösung

Gesucht: Transparenz des East-West-Traffics und zentralisierte Richtlinien

Tempered Networks, ein Sicherheitsanbieter, der sich auf intelligente Steuerungssysteme und IoT-Netzwerke spezialisiert hat, wurde mit der Verwaltung der North-South-Verbindungen zwischen den Campus und dem primären Rechenzentrum der Universität beauftragt. Die Universität hatte jedoch noch immer mehr als 300 Server im Rechenzentrum vor Sicherheitsverstößen zu schützen.

„Wir suchten nach Lösungen für die Verwaltung des East-West-Traffics, fanden aber keine, die ausreichend sauber und nutzerfreundlich waren", erinnert sich der Projektleiter der Universität.

Das Team stieß bei seiner Recherche auf Infection Monkey, das kostenlose Simulationstool für Infektionen und Angriffen von Akamai. Infection Monkey hilft Rechenzentrumsbetreibern, die Widerstandsfähigkeit ihrer Umgebungen gegen Angriffe und seitliche Bewegungen zu bewerten.

Das Team stellte fest, dass sich die mit Infection Monkey erkannten Probleme mit Akamai Guardicore Segmentation lösen lassen.

Es ist eine der wenigen auf Mikrosegmentierung spezialisierten Lösungen auf dem Markt. Es macht es den Betreibern von Rechenzentrum leicht, Sicherheitsrichtlinien zu entwickeln und zu implementieren, um die Kommunikation zwischen einzelnen oder logisch gruppierten Anwendungen zu steuern.

In seiner ersten Präsentation demonstrierte das Akamai-Team der Universität die einzigartigen Visualisierungsfunktionen der Plattform. Mithilfe von Akamai Guardicore Segmentation werden alle in der Umgebung ausgeführten Anwendungen einschließlich ihrer Abhängigkeiten sichtbar.

„Wir waren sofort überzeugt. Die Lösung bot genau das, was wir brauchten."

Akamai Guardicore Segmentation

Akamai statt interner Firewalls

„Bei einer zentralen Firewall-Verwaltung müssen die Regeln für jede Firewall individuell eingerichtet werden. Mit [Akamai] können wir eine Anwendungsgruppe erstellen und festlegen, dass die Systeme einer Gruppe nur untereinander kommunizieren."

Firewalls bergen außerdem Kosten-, Assets- und Verwaltungsprobleme. „Die Verwaltung all dieser Firewalls wäre schlichtweg ein Albtraum. Wir bräuchten vermutlich allein ein halbes Dutzend Mitarbeiter für die Implementierung und den reibungslosen Betrieb des Systems, und mindestens zwei weitere rein für die Verwaltung."

Darüber hinaus fehlt Firewalls die Flexibilität, Richtlinien auf Anwendungsebene festzulegen und zu ändern. „Mit [Akamai] können wir ermitteln, wie Systeme miteinander kommunizieren und warum dies erforderlich ist oder auch nicht. Firewalls bieten nicht die erforderliche Selektivität. Sie blockieren einfach den kompletten Traffic von Port zu Port.

Einfache, zentral verwaltete Mikrosegmentierung

Ein weiterer maßgeblicher Vorteil sind die Geschwindigkeit und Einfachheit, mit der wir Regeln erstellen und implementieren können.

„Bei der Inbetriebnahme hatten wir die Lösung auf ein paar Rechnern installiert und dann eine Richtlinie erstellt, mit der sich die Anbieter untereinander nicht sehen konnten. Der gegenseitige Zugriff der Anbieter wurde sofort blockiert. Das Produkt war damit genau das, wonach wir gesucht hatten“, erklärt der Projektleiter.

Für die Nutzung der Mikrosegmentierungstools und -methoden von Akamai braucht es keine Experten. „Dass alle Teammitglieder diese einfache Lösung nutzen konnten, war für mich ein wichtiges Kaufargument.“

Jenseits der Mikrosegmentierung: Erkennung und Reaktion

Die mit Akamai gewonnene Transparenz hatte den zusätzlichen Vorteil, dass betriebliche Anomalien innerhalb des Rechenzentrums sichtbar werden. „Einmal fanden wir einen fremden Druckerspooler-Dienst“, erinnert sich der Projektleiter. „Es stellte sich heraus, dass die Desktop-Sitzung eines Remote-Nutzers getrennt, aber nicht beendet worden war. Diese versuchte kontinuierlich, mit dem Druckserver des PC zu kommunizieren. Wenn ein solcher PC kompromittiert wird, kann er dem Angreifer Zugang zum Anwendungsserver verschaffen.“

Nachdem das Team Akamai nun aktiv nutzt, plant die Universität bereits weitere Verbesserungen der Sicherheit und Effizienz, die mit der Lösung möglich sind.

„Unser Ziel ist, zahlreiche Netzwerkfunktionen zu automatisieren, wenn ein Vorfall auftritt. Wenn wir beispielsweise eine nicht autorisierte MAC-Adresse oder einen Zugangspunkt von einem Gebäude erkennen, könnten wir mit [Akamai Guardicore Segmentation] einen Befehl an die Tempered Networks-Lösung senden, um das Gebäude zu sperren, und gleichzeitig den Betreiber benachrichtigen, um das Problem zu beheben und die Ursache zu ermitteln. Diese Erkennungsfunktion fehlte uns bisher.“

Mit der Plattform von Akamai gelang es dem Facilities Automation Team der Universität, den gewünschten Sicherheitsstatus schneller und einfacher zu erreichen, als es sich dies je hätte vorstellen können. „Wir hatten noch nie ein derart proaktives Tool, das permanent alles überwacht“, erklärt der Projektleiter.

Akamai übernimmt die Überwachung des East-West-Traffics des Rechenzentrums für das Team. „Unser Team soll sich auf seine tatsächlichen Aufgaben konzentrieren können, nämlich der Universität Energie und Geld zu sparen. Das ist nur möglich, wenn wir uns nicht ständig Gedanken um die Abläufe in unserem Rechenzentrum machen müssen.“

Das Team der Universität hatte nach einer einfachen Lösung für die Mikrosegmentierung gesucht. Akamai bot ihm dies und mehr.

„Es tut genau das, was es verspricht.“

> Das Team konnte nach der Installation sofort loslegen und Schutzregeln implementieren. Das hat den Kunden überzeugt.
>
> Projektleiter der Universität

Weitere Informationen finden Sie unter akamai.com/guardicore.

 | Support | Veröffentlicht: 06/23