AKAMAI-KUNDENREFERENZ

Börsennotiertes Fertigungsunternehmen standardisiert Sicherheitskontrollen und spart Zeit mit Akamai Guardicore Segmentation

Das Fertigungsunternehmen benötigte eine sichere, globale Lösung

- Umfassende Netzwerktransparenz
- Übergreifende Segmentierung von IT-Infrastrukturen
- Reaktion auf Ransomware-Bedrohungen

Der Kunde

Dieses führende Fertigungsunternehmen ist an der NYSE börsennotiert und auf Märkten auf der ganzen Welt tätig.

Die Herausforderung

Schutz eines globalen Unternehmens

Die Gruppe für IT-Sicherheit ist verantwortlich für verschiedene Standorte auf der ganzen Welt, von denen die meisten sowohl als Büros als auch als Fertigungsanlagen genutzt werden. Um eine starke Sicherheitsstrategie zu gewährleisten, musste das Team Sicherheitskontrollen in dem gesamten Unternehmen standardisieren und über die weit verteilten Standorte hinweg durchgehenden Schutz bieten.

„Wir wollten unser offenes, flaches Netzwerk auf eine segmentierte Architektur umstellen, die auf Best Practices basiert“, erklärt der für das Segmentierungsprojekt verantwortliche Infrastrukturarchitekt.

Wie viele Firmen verwendete dieses Herstellerunternehmen zunächst Firewalls für das Projekt.

Die Verwaltung einer Vielzahl von auf der Infrastruktur basierenden Regeln und Änderungen auf der Ebene der Workstations sowie Upgrades überall im Netzwerk wurde schnell sehr zeitraubend, sogar an einem einzigen Standort. Zusätzlich blieb trotz der verbesserten Sichtbarkeit die Beschränkung auf spezifische Bereiche bestehen, sodass es schwer war, eine volle, zentralisierte Übersicht über Netzwerkaktivitäten und die Abhängigkeiten zwischen den Ressourcen zu erreichen.

Unautorisierte laterale Netzwerkbewegung stoppen

Firewalls boten zwar einige grobe Segmentierungskontrollen, scheiterten aber an einem anderen zentralen Problem des Sicherheitsteams – der nicht verwalteten Peer-to-Peer-Kommunikation. Daher war es essenziell, Schutz und Sichtbarkeit in diesen spezifischen Bereich auszudehnen. Diesen Bereich nicht anzugehen hätte bedeutet, dass das Unternehmen für Pass-the-Hash-Angriffe, Ransomware und andere Bedrohungen angreifbar gewesen wäre, deren Verbreitung auf lateraler Netzwerkbewegung zwischen Endpunkten basiert.

Fertigungsunternehmen

Standort
USA

Branche
Fertigungsindustrie

Lösung
Akamai Guardicore Segmentation

Die wichtigsten Vorteile

- Verringert die Ausbreitung von Malware durch laterale Netzwerkbewegung
- Bietet einen detaillierten Überblick
- Sichert Endpunkte durch Segmentierung
- Erleichtert die Vorfallsreaktion

Auswahl der richtigen Lösung

Nach mehreren schwerfälligen Firewall-Kontroll-Implementierungen erfuhr das Team von Akamai Guardicore Segmentation und diskutierte intern über die Vorteile und Möglichkeiten einer Segmentierung der neuen Generation.

Für alle neuen Lösungen, die für eine Implementierung infrage kamen, war umfassende Recherche erforderlich, sodass das Team auch mehrere Alternativen auswertete. Nach einem gründlichen Prüfungsverfahren entschied sich das Team schließlich für Akamai Guardicore Segmentation. „Kein anderer Anbieter außer Akamai bot uns eine Komplettlösung mit Traffic-Überwachung, flexibler Kennzeichnung und einer umfassenden Transparenz auf Anwendungsebene durch nur einen einzigen Agent auf einem Client“, so der Infrastrukturarchitekt.

> Mit nur einem einzigen Agent pro Gerät haben wir das Problem eines Endpoint-Angriffs jetzt für immer gelöst.
>
> Infrastrukturarchitekt, Fertigungsunternehmen

Akamai Guardicore Segmentation

In der ersten Phase des Projekts implementierte das Unternehmen Akamai Guardicore Segmentation auf ca. 2.000 Workstations. Das IT-Sicherheitsteam lernte sofort eine neue Ebene der Transparenz in Bezug auf das Netzwerk und die Kommunikationswege kennen, sobald die Lösung installiert war.

Neue Einblicke und Segmentierung im Einsatz

„Mit den Traffic Maps von Akamai hat sich unsere Transparenz um 1.000 % verbessert und umfasst die Kommunikation von PC zu PC“, so der Infrastrukturarchitekt.

Durch die Möglichkeit, die Aktivität eines einzelnen Computers aufzuschlüsseln und dabei die allgemeine Aktivität auf Anwendungsebene zu verstehen, konnte das Unternehmen seine Sicherheitsentscheidungen basierend auf einer besseren Informationsgrundlage treffen. Zum Beispiel hatten einige Nutzer Anwendungen für ihre privaten Drucker auf ihren Firmen-Laptops installiert. Es stellte sich heraus, dass viele dieser Anwendungen das Firmennetzwerk kontinuierlich nach unterstützten Geräten absuchten. Basierend auf diesem neuen Einblick durch die von Akamai bereitgestellte Transparenz konnte das Team die Scans stoppen.

Akamai Hunt: Akamai Guardicore Segmentation zur Erkennung von Bedrohungen

Mit diesem neuen Verständnis der Netzwerkaktivität konnte das Unternehmen externe Cyberkriminelle aufhalten. Bald nach der Implementierung der Plattform entdeckte der Akamai Hunt-Service beispielsweise eine Ressource, die mit einer Datei mit Merkmalen einer bekannten Malware namens GoldenSpy kommunizierte. Das Hunt-Team informierte das IT-Sicherheitsteam des Unternehmens über die erkannte Bedrohung. Dem Kunden wurden auch eine Analyse des Umfangs des Befalls, der potenziellen Risiken (Zuordnung von Ergebnissen mit MITRE-Informationen über GoldenSpy) und der Forensik (mithilfe von Insight) sowie Empfehlungen für interne Untersuchungen und Schadensbegrenzung bereitgestellt. Dann verwendete das Unternehmen die Richtlinienkontrollen von Akamai, um das befallene System zu isolieren und die Malware daran zu hindern, sich durch laterale Netzwerkbewegung auf andere Geräte auszubreiten.

Standardisieren und Zeit sparen

Dieses Unternehmen kann nun auch Richtlinien erstellen und zentral verwalten, einschließlich einer zentralen globalen Workstation-Richtlinie. Es hat außerdem die Flexibilität, vereinzelte Ausnahmeregelungen zu erstellen, wenn ein Anwendungsfall dies verlangt. Dies gewährleistet eine einheitliche Durchsetzung überall dort, wo ein Agent von Akamai implementiert ist. Außerdem sinkt das Risiko für Konfigurationsfehler und Verzögerungen.

Auch die Zeit für die Erstellung von Richtlinien hat sich in dem Unternehmen erheblich verkürzt. Eine Änderung an den Firewall-Kontrollen vorzunehmen, konnte zum Beispiel mehrere Tage dauern, bevor die neue Plattform in Betrieb genommen wurde. Mit der Verwendung der neuen Vorlagen für Richtlinien von Akamai als Orientierungshilfe kann das IT-Sicherheitsteam auch für die komplexesten Anwendungsfälle in weniger als einer Stunde Sicherheitskontrollen erstellen und sie innerhalb von Sekunden auf die gesamte installierte Basis anwenden.

Die Zukunft mit Akamai

Der anfängliche Fokus des Projekts lag auf der Standardisierung der Sicherheitskontrollen für Endpoint-Segmentierung und -Zugriff. Inzwischen gibt es jedoch Pläne, weitere Anwendungsfälle mit Akamai anzugehen. Die Entscheidungsträger diskutieren über eine Erweiterung des Schutzes, um auch Server und kritische Anwendungen, wie beispielsweise das ERP-System des Unternehmens, einzubeziehen.

Was auch immer zukünftige Pläne umfassen mögen – das ursprüngliche Projekt ist für das Fertigungsunternehmen bereits ein Erfolg und hat die Angriffsfläche und das Risiko für die Workstations des Unternehmens erheblich reduziert. Das Team ist jetzt viel zuversichtlicher in Bezug auf die Sicherheitsstrategie des Unternehmens bei Angriffen, die sich lateral von Endpoint zu Endpoint bewegen. Der Projektleiter erklärt: „Mit nur einem einzigen Agent pro Gerät haben wir dieses Problem jetzt für alle Zeiten gelöst und können nun an einer Workstation ohne Richtlinien innerhalb von 30 Sekunden die vollen Sicherheitskontrollen implementieren."

> Mit den Traffic Maps von Akamai hat sich unsere Transparenz um 1.000 % verbessert und umfasst nun auch die Kommunikation von PC zu PC.
>
> Infrastrukturarchitekt, Fertigungsunternehmen

Weitere Informationen finden Sie unter akamai.com/guardicore.

 | Support | Veröffentlicht: 06/23