Akamai

WHITEPAPER

Neudefinition von Firewalls

Das überzeugende wirtschaftliche Argument für softwarebasierte Segmentierung

Zusammenfassung

Warum verlassen sich Netzwerk- und Sicherheitsteams bei der internen Netzwerksegmentierung immer noch auf ältere Firewalls? Da Anwendungen und Segmente, die durch Richtlinien geschützt sind, immer mehr Verbreitung finden, erweisen sich physische Firewall-Appliances als zu komplex, unflexibel und schlichtweg unwirksam, um die Sicherheitsherausforderungen der immer dynamischeren Hybrid-Cloud-Umgebung von heute zu bewältigen. Und sie sind viel teurer, als man denkt. Abgesehen von den immensen Vorlaufkosten für Firewalls und Hardware ergeben sich auch erhebliche nachgelagerte Kosten: durch Projektmanagement, Arbeitsaufwand, Wartung und das sehr reale Risiko einer längerfristigen Asset-Gefährdung aufgrund langwieriger Implementierungszeiten. Wenn moderne Unternehmen von den Vorteilen agiler DevOps-Methoden, schneller Anwendungsbereitstellung und der Cloud profitieren wollen, muss es eine bessere Möglichkeit geben, kritische Assets durch Segmentierung zu sichern. Und genau die gibt es jetzt: softwarebasierte Segmentierung. Sie ist einfacher, schneller, effektiver und – wie dieses Whitepaper deutlich zeigen wird – bietet optimale Sicherheit zu deutlich niedrigeren Gesamtbetriebskosten als herkömmliche Segmentierungsmethoden.

Einführung

Heute sehen wir drei Kräfte, die gemeinsam die Nachfrage nach präzisen Segmentierungsmethoden für Netzwerke und einzelne Assets steigern: Erstens erfordern agile DevOps-Methoden und andere schnelle Bereitstellungsmodelle eine beschleunigte Implementierung von Anwendungen in der Produktion. Und das erfordert zwangsläufig die Einrichtung sichererer Zonen mit präziseren Richtlinien. Zweitens migrieren Unternehmen in die Cloud und übernehmen hybride IT-Infrastrukturen. Hierbei werden ihre Anwendungen oft zwischen verschiedenen Umgebungen migriert, was den Traffic zwischen den Segmenten im gesamten Netzwerk erhöht. Und drittens schafft die schnelle Verbreitung von Anwendungen aufgrund agiler Entwicklung eine ständig wachsende Angriffsfläche für Hacker.

Firewalls für Segmentierung: die besten Jahre hinter sich

Unter diesen Bedingungen ist der bloße Einsatz von VLANs und Firewalls für die Segmentierung nicht mehr tragbar. Aus rein technischer Sicht ist die Konfiguration mehrerer VLAN- und Firewall-Installationen – und zwar so, dass sie mit der Anwendungsentwicklung Schritt halten – sowohl komplex als auch aufwendig. Außerdem ist das Ganze arbeitsintensiv und es werden zahlreiche Teammitglieder von wichtigeren Sicherheitsprojekten abgezogen. Die Bereitstellungszeit ist ein weiteres Problem, da hierdurch das Risiko einer langfristigen Gefährdung und Anfälligkeit von Assets steigt. Und vor allem ist die Implementierung extrem kostspielig – nicht nur aufgrund der Kosten für Firewalls und neue Hardware zur Unterstützung von zusätzlichem Traffic, sondern auch aufgrund der Kosten für die laufende Verwaltung, für Änderungen und für die Wartung von Installationen.

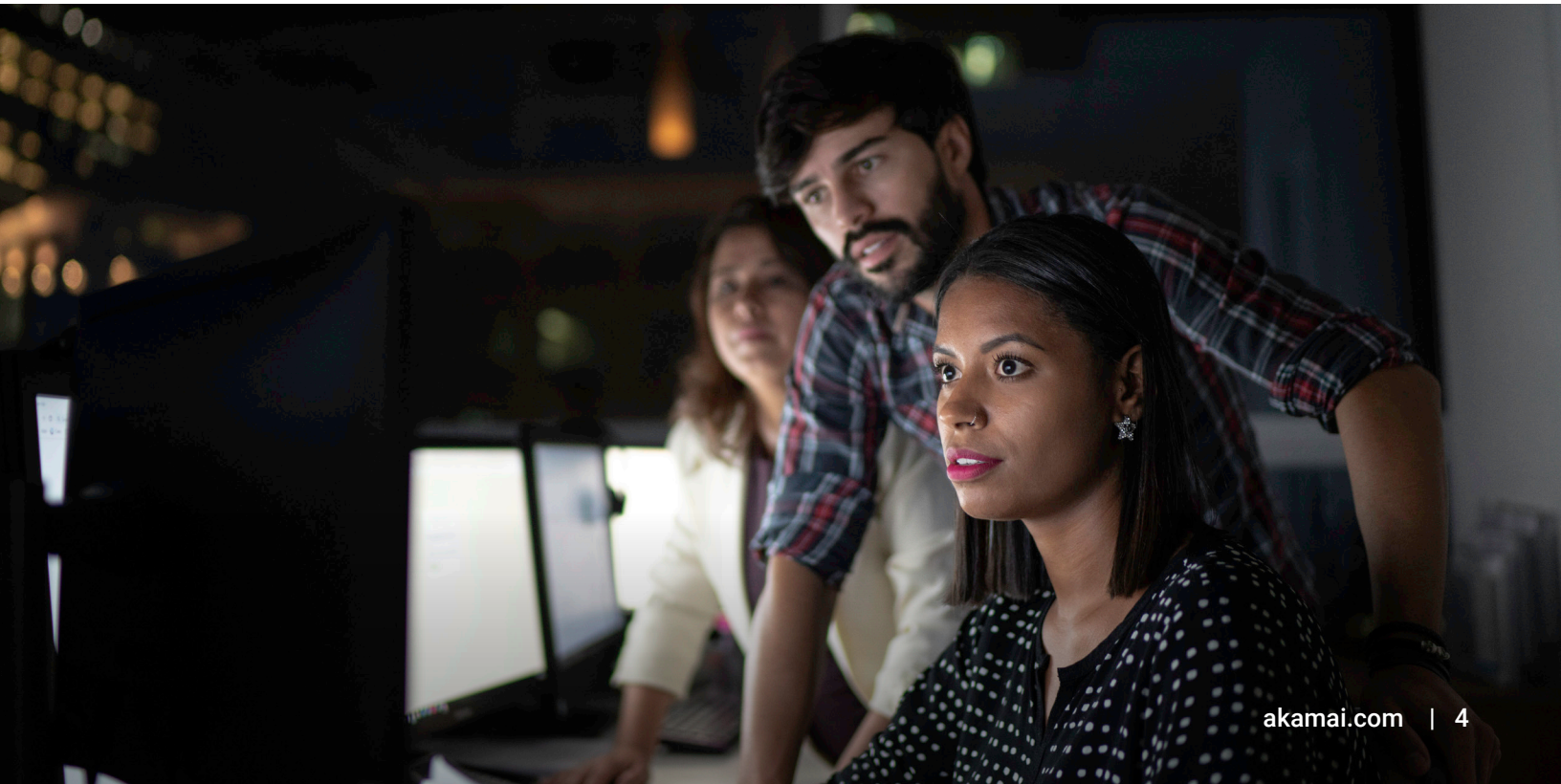
Einfach ausgedrückt: Herkömmliche Ansätze zur Netzwerksegmentierung stoßen an ihre Grenzen. Insbesondere wenn Unternehmen dynamische Cloud- und Hybridumgebungen nutzen möchten, schränkt der Einsatz interner Firewalls nicht nur ihre Flexibilität ein, sondern auch die Geschwindigkeit bei der Richtlinienerstellung und -durchsetzung und die Fähigkeit, den Betrieb sicher zu skalieren. Eine moderne, optimierte, kostengünstigere und letztendlich effektivere Alternative zur Segmentierung mit Legacy-Firewalls ist also wichtiger denn je. Und genau hier kommt softwarebasierte Segmentierung ins Spiel.

Eine moderne, optimierte, kostengünstigere und effektivere Alternative zur Segmentierung mit Legacy-Firewalls ist also wichtiger denn je.

Das Problem: die aufwendige und kostspielige Aufgabe der Firewall-Verwaltung

Bevor wir uns mit den Vorteilen der softwarebasierten Segmentierung befassen, ist es sinnvoll, sie mit dem Status quo zu vergleichen. Mit dem Wachstum eines Unternehmens nehmen auch die Anzahl der Anwendungen und die Menge des damit verbundenen Traffics zu – und so steigt auch die Nachfrage nach zusätzlichen Netzwerksegmenten und komplexeren Sicherheitsrichtlinien. Wenn Sie sich auf firewallgeschützte VLANs verlassen, muss jedes neu bereitgestellte VLAN jedem Switch-Trunk-Port hinzugefügt werden, über den der Traffic zwischen den Segmenten geleitet wird. Außerdem muss für jedes neue VLAN ein IP-Subnetzwerk erstellt werden. Für die Firewall muss eine individuelle Schnittstelle eingerichtet werden. Dann müssen Firewall-Richtlinien erstellt werden. Jede dieser Änderungen erfordert in der Regel Genehmigungen, Wartungsfenster und umfasst potenzielle Ausfallzeiten, was ein erhöhtes Risiko von Netzwerkunterbrechungen bedeutet.

Das Hinzufügen von VLANs und Firewalls erfordert einen mühsamen, mehrstufigen Prozess, an dem bis zu fünf Teams beteiligt sind, die separat für Switching, Routing, Firewall-Implementierung, ESXi-Server und die Erstellung von Sicherheitsrichtlinien verantwortlich sind. All das verlängert die Implementierungsdauer, setzt das Unternehmen längeren Risiken aus und führt zu höheren Kosten für Software, Hardware und Personal. Und aus Sicht der Techniker ist die Arbeit außerdem riskant und wenig lohnend: Hier wird mit viel Aufwand wenig erreicht und es werden Zeit und Ressourcen von anderen, wichtigeren Risikomanagement-Aufgaben abgelenkt. Leider eignen sich nur wenige Schritte im Änderungsmanagement-Prozess innerhalb der Firewall-VLAN-Umgebung für die Automatisierung.



Die Lösung: softwarebasierte Segmentierung in drei einfachen Schritten

Legacy-Netzwerk-Firewalls waren einfach nie für die präziseren, bandbreitenbegrenzten Anforderungen einer fein abgestuften internen Segmentierung gedacht. Softwarebasierte Segmentierung hat sich in den letzten Jahren als praktikable, schnellere, effektivere und kostengünstigere Alternative erwiesen, um der Nachfrage nach mehr und engeren Netzwerksegmenten in den heutigen dynamischen Umgebungen gerecht zu werden. Ein zentraler Aspekt der Implementierung einer softwarebasierten Segmentierung ist das Konzept einer „verteilten Firewall", die viel agiler und einfacher zu verwalten ist als eine herkömmliche Netzwerk-Firewall-Appliance.

> Softwarebasierte Segmentierung ermöglicht eine **10 oder 20 Mal schnellere Bereitstellung** als herkömmliche Firewalls – mit weniger Personal und praktisch ohne Ausfallzeiten oder Unterbrechungen.

Ein branchenführendes Beispiel für eine softwarebasierte Segmentierungslösung ist Akamai Guardicore Segmentation. Im Vergleich zum langwierigen, kostenintensiven und komplexen Prozess der VLAN-Firewall-Implementierung umfasst unsere Lösung für softwarebasierte Segmentierung nur drei Schritte:

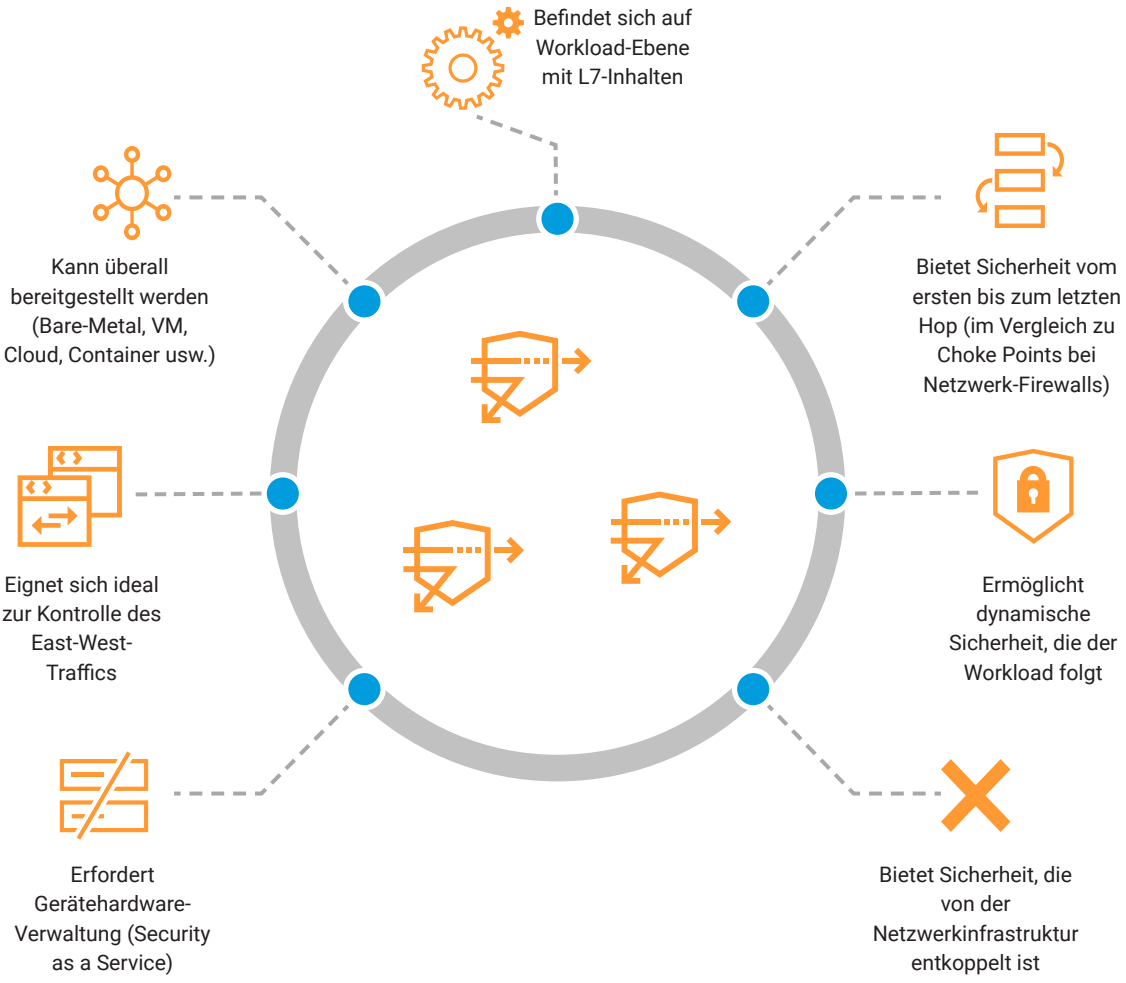
1. **Assets identifizieren und kennzeichnen:** Ein großes Hindernis, das mit herkömmlichen Firewalls einhergeht, ist die mangelnde Transparenz der zu schützenden Assets. Akamai Guardicore Segmentation umfasst eine Visualisierungsfunktion, mit der Verantwortliche alle Anwendungen, die in der Infrastruktur eines Unternehmens ausgeführt werden, sowie deren Abhängigkeiten identifizieren und kennzeichnen können.

2. **Visualisieren und nach Kennzeichnung gruppieren:** Wenn die kontextbezogene Transparenz erreicht ist, können Verantwortliche Anwendungen dann basierend auf ihren Kennzeichnungen in logischen Gruppen organisieren und die Abhängigkeiten zwischen ihnen abbilden. Unser Kennzeichnungsprozess ist sehr flexibel und ermöglicht es Ihnen, Anwendungen basierend auf Ihrem eigenen Geschäftskontext zu gruppieren – und zwar mit einer Terminologie, mit der Sie bereits vertraut sind.

3. **Richtlinien erstellen:** Verantwortliche können dann detaillierte Sicherheitsrichtlinien erstellen, die festlegen, welche Anwendungen miteinander kommunizieren dürfen – auf Grundlage der tatsächlich beobachteten Datenflüsse. Vorkonfigurierte Richtlinienvorlagen für häufige Anwendungsfälle vereinfachen den Prozess noch weiter. Anwendungen und Workflows werden nun effektiv voneinander segmentiert, unabhängig davon, wo in der Umgebung sie sich befinden.

Softwarebasierte Segmentierung lässt sich zehn oder sogar zwanzig Mal schneller bereitstellen als herkömmliche Firewalls – mit weniger Personal und praktisch ohne Ausfallzeiten oder Unterbrechungen. Sobald Sie den Visualisierungs- und Segmentierungsprozess gestartet haben, können Sie Ihr Netzwerk ganz einfach weiter unterteilen oder verschiedene Richtlinien basierend auf Kennzeichnungen hinzufügen, Prozesse automatisieren, Sicherheitsvorfälle beheben und schnelle Änderungen als Reaktion auf geschäftliche oder behördliche Anforderungen vornehmen.

Vorteile einer verteilten Firewall



Fallstudie: Großer Lebensmittelverarbeiter erzielt 85 % Einsparungen bei Segmentierung

Ein großer US-amerikanischer Verarbeiter von Schweinefleischprodukten musste 45 Anwendungen mit durchschnittlich fünf Servern pro Anwendung segmentieren, die an zwei Standorten bereitgestellt wurden. Ziel des Unternehmens war es, seine flachen Netzwerke bei minimaler Serviceunterbrechung zu beseitigen und so schnell wie möglich Richtlinien zu implementieren.

Nachdem sich die Verantwortlichen einige Alternativen angesehen hatten, entschieden sie sich für die softwarebasierte Segmentierungslösung von Akamai. Zwar waren Geschwindigkeit und Einfachheit der Implementierung ausschlaggebend für diese Wahl. Doch der entscheidende Faktor war eine Analyse, die über einen Zeitraum von drei Jahren Einsparungen von mehr als 900.000 US-Dollar (oder 85 %) gegenüber dem VLAN-Schutz eines führenden Firewall-Anbieters ergab. Im Einzelnen sind das die Folgenden:

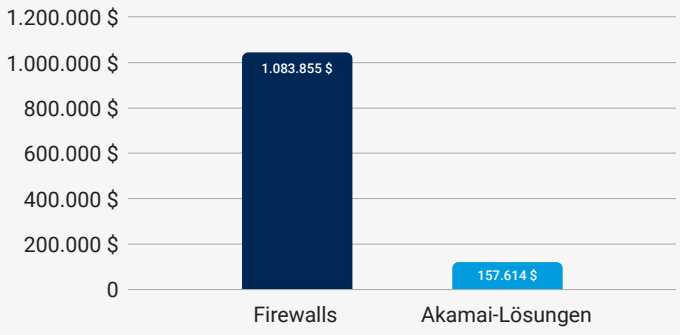
- Die Kosten für die Lizenzierung von Akamai Guardicore Segmentation waren um 55 % niedriger als die Hardwarekosten für eine VLAN-Firewall-Implementierung.
- Die Arbeitskosten, basierend auf einer Annahme von 2.000 US-Dollar pro Woche, waren bei Akamai um 93 % niedriger als bei einem VLAN-Projekt mit wesentlich längerer Dauer.

Darüber hinaus erfüllte Akamai die Kundenanforderung einer schnellen Richtlinienimplementierung und schützte in nur sechs Wochen 45 Anwendungen ohne Unterbrechung.

Gesamtbetriebskosten mit Firewall*
1.083.855 $

Gesamtbetriebskosten mit Akamai
157.614 $
-926.241 $

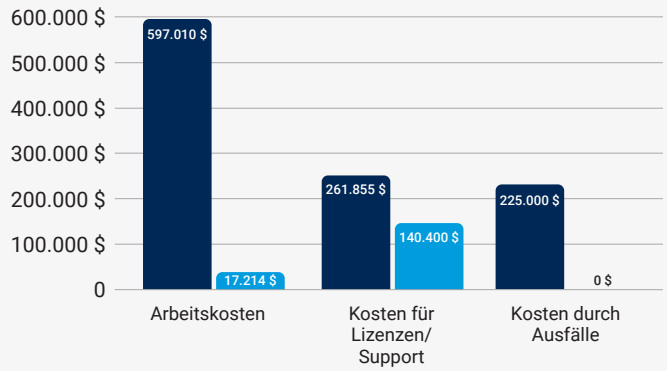
* Kosten über einen Zeitraum von drei Jahren



Arbeitskosten mit Akamai*
17.214 $
-579.796 $

Akamai-Kosten für Lizenzen/Support*
140.400 $
-121.455 $

Kosten durch Ausfallzeiten mit Akamai*
0 $
-255.000 $



Was das alles bedeutet

Softwarebasierte Segmentierung bietet drei wesentliche Vorteile gegenüber herkömmlichen Firewall-Methoden:

Effektivere Risikoreduzierung: Durch die schnelle Segmentierung von Anwendungen auf äußerst detaillierter Ebene führt die softwarebasierte Segmentierung zu einer deutlich reduzierten Angriffsfläche. Durch den Einsatz der Zero-Trust-Prinzipien – die eine strikte Authentifizierung sämtlicher Nutzer, Geräte oder Anwendungen erfordern, die versuchen, auf eine Netzwerkressource zuzugreifen – verhindert softwarebasierte Segmentierung die laterale Netzwerkbewegung von Bedrohungen innerhalb des Rechenzentrums oder der Netzwerkumgebung. Dadurch werden die Auswirkungen von Datenschutzverletzungen weiter reduziert, da Angreifer keine Prozesse mehr übernehmen können, selbst wenn sie erfolgreich den Netzwerkschutz geknackt haben. Außerdem können Unternehmen schneller Compliance mit Gesetzen erreichen, die eine eindeutige Isolierung kritischer, sensibler Anwendungen vom allgemeinen Netzwerktraffic erfordern.

Schneller zu optimaler Sicherheit: Kurz gesagt: Softwarebasierte Segmentierung erhöht die Sicherheit, beschleunigt die Bereitstellung flexibler DevOps-Anwendungen und sorgt dafür, dass jede Anwendung in der Produktion ordnungsgemäß geschützt wird. Außerdem sind weniger Ressourcen – ob technische oder personelle – in langfristigen Segmentierungsprojekten gebunden. So können Teams ihre Zeit auf andere, wichtigere Initiativen konzentrieren.

Erheblich reduzierte Gesamtbetriebskosten: Dies ist der eigentliche Gewinn und aus geschäftlicher Sicht wahrscheinlich der bedeutendste Vorteil. Softwarebasierte Segmentierung kann mit deutlich geringeren Investitionskosten (CapEx) erreicht werden, da hierfür statt Firewall-Appliances und zusätzlicher Hardware nur eine Softwarelösung erforderlich ist. Darüber hinaus werden die Betriebskosten (OpEx) im Laufe der Zeit deutlich gesenkt, da Arbeits- und Ressourceneinsparungen für die laufende Wartung und Verwaltung erzielt werden.

Allein anhand dieser Maßnahmen konnte der Ansatz von Akamai bei einem direkten Vergleich zwischen softwarebasierter Segmentierung und einer Firewall-Lösung für zehn Anwendungssegmente eine potenzielle Gesamteinsparung von 85 % erzielen – fast eine Million US-Dollar.

Zwar können Sie schon in der ersten Woche nach der Bereitstellung messbare Einsparungen erwarten, doch die Gesamtbetriebskosten (TCO) umfassen viel mehr als nur den Anschaffungspreis oder die laufenden Kosten. Auch wenn die Gesamtkosten nicht ohne Weiteres ersichtlich sind, führt softwarebasierte Segmentierung zu erheblichen Einsparungen, da Ausfallzeiten und Serviceunterbrechungen praktisch eliminiert werden. Darüber hinaus vermeiden Unternehmen finanzielle Verluste aufgrund von Datenschutzverletzungen sowie Strafen für die Nichteinhaltung von Vorschriften. Und sie verringern das Risiko von Reputationsschäden und Geschäftsverlusten infolge eines Verstoßes erheblich. IT-Teams und -Ressourcen können vom Firewall-Änderungsmanagement abgezogen und für produktivere Projekte eingesetzt werden. All diese Kostenfaktoren sorgen für niedrigere Gesamtbetriebskosten und bessere Geschäftsergebnisse für Unternehmen, die sich für eine softwarebasierte Segmentierungslösung entscheiden.

Fallstudie: Große globale Bank, die Compliance-Sanktionen ausgesetzt ist, sorgt mit Akamai Guardicore Segmentation für Abhilfe

Nach einem Audit, bei dem Sicherheitsrisiken in ihren flachen Netzwerken aufgedeckt wurden, und angesichts einer Reihe neuer Vorschriften, die eine strengere Segmentierung erforderten, leitete ein großes europäisches Finanzinstitut ein Segmentierungsprojekt ein, bei dem VLANs und Firewall-Regeln zum Einsatz kommen sollten. Dieses Projekt nahm viel Zeit in Anspruch und erforderte den Einsatz vieler Stakeholder und Teams, was Produktionsausfälle und unklare Richtlinien mit sich brachte. Infolgedessen zahlte die Bank Bußgelder für mangelnde Compliance sowie untragbar hohe Implementierungskosten.

Das IT-Team suchte also schnell nach alternativen Lösungen und war beeindruckt von dem Automatisierungsgrad, den Akamai in den Sicherheitsbetrieb der Bank einbringen konnte. Das Team implementierte Akamai Guardicore Segmentation über mehrere Regionen und IT-Infrastrukturtypen hinweg. Das Projekt dauerte weniger als drei Monate – zehnmal schneller als ursprünglich mit den herkömmlichen Segmentierungsmethoden angenommen. Die Bank hat nicht nur ihre Sicherheit verbessert, sondern auch die Compliance-Anforderungen für mehr als 10.000 Assets erfüllt. Die schnelle Bereitstellung führte zu einer beschleunigten Risikominderung sowie zu erheblichen Kosten- und Ressourceneinsparungen.

Große globale Bank

Projektziel:

Trennung von Entwicklung/Produktion/Nutzerakzeptanztests

Projektumfang:

1. Beschränkung des Traffics zwischen Produktions- und anderen Umgebungen
2. Bereitschaft für Anwendungs-Ringfencing

Legacy-Segmentierung

- Extrem langsame Fortschritte
- Auditprobleme, Bußgelder und Produktionsfehler
- Produktionsausfälle aufgrund von Anwendungsausfällen

Zeit: 2 Jahre mit Firewalls/VLANs

Auswirkungen von Akamai

- 10.000 nicht konforme Assets segmentiert
- Keine Anwendungsausfälle
- 10 Mal schnellere Implementierung
- Reduzierter manueller Aufwand mit DevOps

Zeit: 6 Monate **Mitarbeiter:** 3 Architekten

Fazit: Alles zusammengenommen

Firewalls sind nicht veraltet. Sie spielen auch weiterhin eine Rolle beim Schutz des lokalen Netzwerks. Doch in heutigen dynamischen Umgebungen ist dieses geschlossene Netzwerk ein etwas unklares Konzept. Um das notwendige Gleichgewicht zwischen Sicherheit und Agilität zu erreichen, müssen Unternehmen in der Lage sein, ihre digitalen Assets nicht nur auf der L4-Netzwerkebene, sondern auch auf der L7-Anwendungsebene zu schützen – genauer gesagt: auf Ebene einzelner Prozesse. Und zu diesem Zweck sind Firewalls nicht nur schlecht geeignet, sondern stehen auch dem Fortschritt im Wege. Der Versuch einer fein abgestuften Segmentierung mit Firewalls stellt eine enorme Belastung personeller, technischer und finanzieller Ressourcen dar.

Im Vergleich zu Firewalls hat sich gezeigt, dass softwarebasierte Segmentierung das Sicherheitsrisiko und die Amortisierungszeit deutlich reduziert und die Gesamtbetriebskosten deutlich niedriger ausfallen als bei herkömmlichen Ansätzen. Und das führt auch zu einem schnelleren ROI. Das ist keine futuristische Vision – softwarebasierte Segmentierung ist sofort verfügbar und liefert genau diese Vorteile für Unternehmen verschiedenster Branchen.

Eine Studie zu IT-Evolution

Die Geschichte der Technologie ist voll von ständiger Verbesserung, Vereinfachung und Kostensenkung. Und Segmentierung ist da keine Ausnahme.

Nehmen wir das Beispiel Datenspeicher, der sich in knapp zwei Jahrzehnten von Disketten zu Flash-Laufwerken, dann zu Network Attached Storage (NAS) und schließlich zu Cloudspeicher weiterentwickelt hat. Oder Computing-Laufzeit, die sich von Servern zu virtuellen Maschinen, Cloud Computing zu Containern und letztlich zu serverlosem Computing entwickelt hat. In beiden Fällen waren Kosteneinsparungen und höhere Flexibilität die wichtigsten Faktoren. Und natürlich wurde das Ganze durch schnelle Fortschritte in der Technologie möglich.

Die Evolution der Segmentierung weg von physischen Firewall-Appliances hin zu softwarebasierten verteilten Firewalls, die vom Netzwerk abstrahiert werden, ist ganz ähnlich. Die zugrunde liegenden Faktoren sind dieselben: geringere Kosten und erhöhte Flexibilität (was sich in einer schnellen Bereitstellung niederschlägt), während gleichzeitig die Effektivität von Sicherheitsrichtlinien kontinuierlich verbessert wird – durch einen präzisen Ansatz, der Zero Trust unterstützt.

Es ist an der Zeit, dass Netzwerk- und Sicherheitsteams ein neues Modell für den Schutz durch Segmentierung implementieren – ebenso, wie sie es in anderen Technologiesektoren getan haben. Denn die Segmentierung über physische Firewalls wird schon bald das Schicksal der Diskette ereilen.

Möchten Sie unsere Lösung in Aktion erleben?
Fordern Sie noch heute eine Demo an: akamai.com/guardicore