Akamai

WHITEPAPER

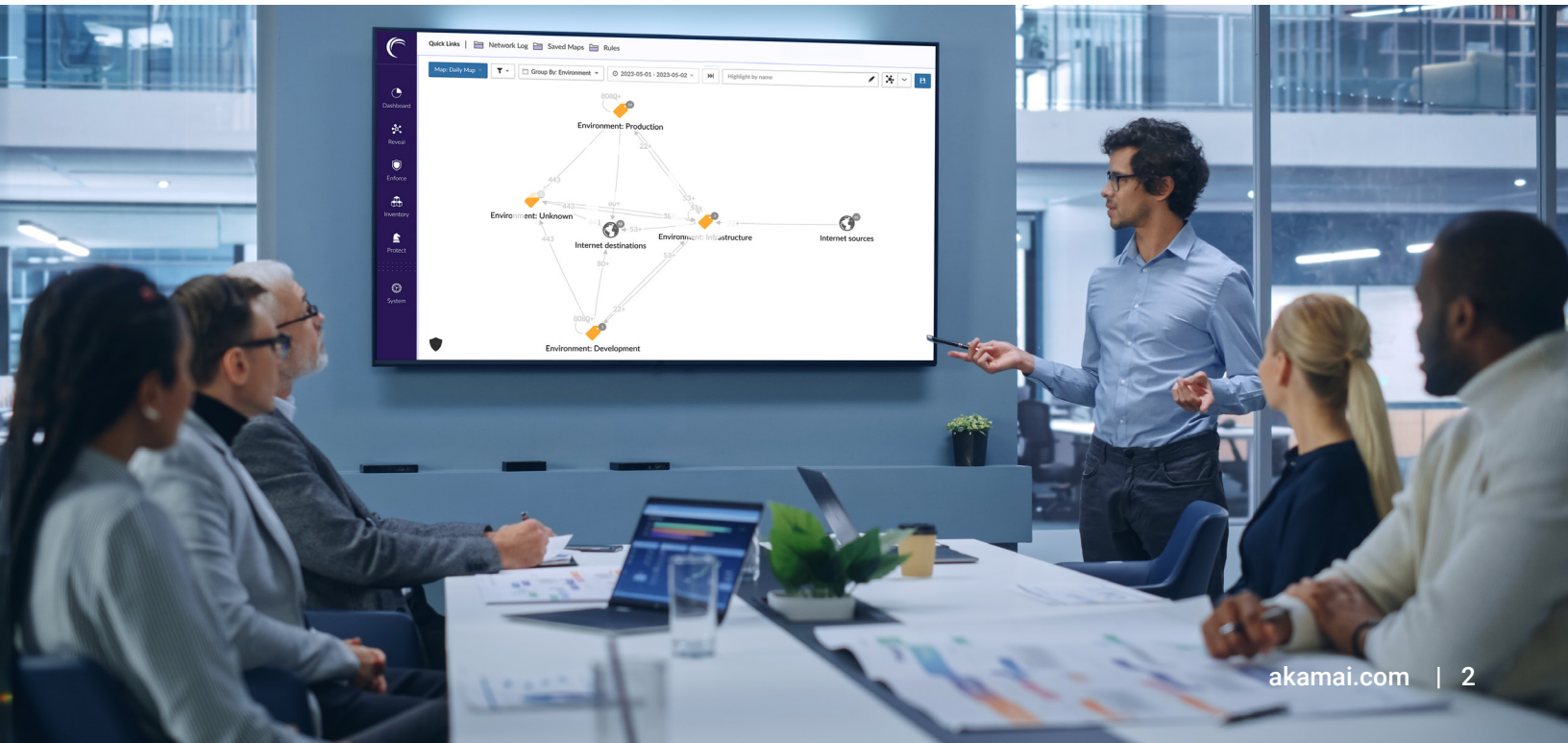
Softwarebasierte Segmentierung für Betreiber von Rechenzentren

Für Betreiber von Rechenzentren mit mehreren Mandanten ist die Segmentierung von Computing-Umgebungen nicht nur wichtig, sie ist die Basis ihres Betriebsmodells. Erstens müssen sie ihre eigene Infrastruktur von den Umgebungen ihrer Kunden trennen und bestimmte Ressourcen teilen, während sie gleichzeitig den Zugriff auf andere Ressourcen verhindern. Zweitens müssen sie eine „Kreuzkontamination" – egal ob unbeabsichtigt oder schädlich – in den jeweiligen Umgebungen ihrer Kunden verhindern. Dazu gehört auch, zu verhindern, dass erfolgreiche Angriffe oder Malware-Infektionen von der Umgebung eines Kunden auf andere Umgebungen übergreifen. Schließlich ist innerhalb der eigenen betrieblichen Anwendungen ein angemessenes Maß an Trennung erforderlich, um die Auswirkungen eines potenziellen Angriffs zu begrenzen. Bei einem genaueren Blick auf die operativen Netzwerke der Anbieter von Rechenzentren wird klar, dass es drei Szenarien gibt, in denen eine effiziente Segmentierung die Sicherheit erheblich verbessern und die Kosten senken kann.

1. **Trennung von operativen Netzwerken** (DCIM, BMS usw.) vom Unternehmensnetzwerk (den internen Systemen des Anbieters, die auch die Fakturierung beinhalten) und von den Kundennetzwerken

2. **Reduzierung des Risikos von lateralen Bewegungen innerhalb des operativen Netzwerks,** das über viele Systeme verfügt, in denen Fehler schwer zu beheben sind, und das Risiken birgt, wenn es nicht ordnungsgemäß segmentiert ist

3. **Schaffung einer effizienten und sicheren Verbindung zwischen Kundennetzwerken** , wie z. B. die DMZ, wo sich das nutzerdefinierte Portal befindet, das sicheren Zugriff auf Daten aus operativen Netzwerken (z. B. Lesen des Stromstatus) und Unternehmensnetzwerken (zum Lesen der Fakturierungsinformationen) benötigt



Diese Aspekte werden heute über sehr komplexe, langsam zu implementierende und ineffiziente Netzwerkkonstrukte, VLANs, Zwischennetzwerke usw. abgewickelt. Durch die Implementierung einer softwaredefinierten Lösung ohne komplexe Netzwerkkonfigurationen sind erhebliche Kosteneinsparungen möglich und die Konnektivität kann engmaschiger und zuverlässiger gesteuert werden.

Darüber hinaus fällt es den Kunden schwer, ein hohes Maß an Segmentierung innerhalb ihrer Anwendungen (gehostet oder vor Ort) zu implementieren und aufrechtzuerhalten. Dies bietet Betreibern von Rechenzentren die wichtige Möglichkeit, ihr internes Wissen, ihre Tools und Betriebsmodelle im Bereich Segmentierung zu nutzen, um ihren Kunden Managed Services zu bieten und im Zusammenhang mit einer Segmentierungspraxis eine sehr attraktive Einnahmequelle zu schaffen. Darüber hinaus ist der Betreiber – durch die Möglichkeit, Sicherheitsrichtlinien mit der richtigen Methodik, den richtigen Tools und den richtigen Prozessen auf Kundenstandorte auszuweiten – in der Lage, auf die nicht gehosteten Anwendungen zuzugreifen und Einblicke in sie bereitzustellen, wodurch die sichere Migration in das gehostete Rechenzentrum beschleunigt und so zum Kerngeschäft beigetragen werden kann.

Equifax: Ein Worst-Case-Szenario

Wenn Sie sich fragen, was „im schlimmsten Fall“ bei schwacher, ineffektiver oder nicht vorhandener Segmentierung der Umgebung passieren könnte, ist der in der Vergangenheit häufig publizierte Equifax-Vorfall von 2017 ein erstklassiges Beispiel. Der Angriff führte zur Kompromittierung der hochsensiblen, personenbezogenen Daten von 143 Millionen US-Bürgern. Laut der Untersuchung des U.S. Government Accountability Office (GAO) brachen die Angreifer zunächst in das Konfliktlösungsportal des riesigen Kreditbüros ein, indem sie im Webframework Apache Struts eine Schwachstelle ausnutzten, die die Bezeichnung CVE 2017-5638 trägt. Nach dem Eindringen konnten Sie die Systeme des Unternehmens im Wesentlichen 76 Tage lang ausnutzen. Im GAO-Bericht wurde diese Freiheit der lateralen Bewegung auf eine fehlende Segmentierung zurückgeführt, die einfach einen beliebigen Zugriff auf Datenbanken ermöglicht – eine nahezu unbegrenzte Angriffsfläche.

Die Frage ist, wie man diese Art von Segmentierung am effektivsten, effizientesten und wirtschaftlichsten erreichen kann. Betreiber nutzten in der Vergangenheit herkömmliche Firewalls oder VLANs, um Umgebungen innerhalb einer Architektur mit mehreren Mandanten oder Nutzern zu trennen. Die Implementierung und Aufrechterhaltung solcher Maßnahmen ist jedoch üblicherweise mühsam, sehr manuell, zeitaufwendig und teuer. Darüber hinaus sind diese Techniken alles andere als zuverlässig und können eine erhebliche Menge an Angriffsfläche offenlegen. Die Effizienz von Lösungen, die für die Netzwerkverteidigung entwickelt wurden, ist besonders in Rechenzentren ein Problem, da die meisten dieser Umgebungen eine Vielzahl von virtuellen Maschinen, Hypervisoren, Containern und sogar Cloud-Komponenten umfassen und Workloads automatisch dynamisch starten und enden. Weiterhin ist es wichtig, zu bedenken, dass eine Segmentierung mit VLANs Ausfallzeiten bei einer Anwendung erfordert, was für kritische, operative Kontrollen das Aus bedeuten kann.

Aus all diesen Gründen befassen sich Betreiber gemeinsamer Umgebungen genauer mit modernen, softwaredefinierten Segmentierungstechniken, einschließlich Mikrosegmentierung. Fortschritte auf dem Gebiet der Mikrosegmentierungstechnologien haben sie zu einer praktikablen Option für alle Arten von Unternehmen und zur wohl besten Wahl für die Umsetzung eines Zero-Trust-Sicherheitsmodells gemacht. Ein genau so wichtiger Punkt ist, dass Mikrosegmentierung mit den richtigen Tools und ein wenig durchdachter Planung schneller und einfacher als die vorher genannten Methoden implementiert werden kann und leichter zu verwalten und zu warten ist. Aktuelle Tests haben gezeigt, dass Mikrosegmentierung im Vergleich zur herkömmlichen Firewall-Implementierung um bis zu 30 Mal schneller bereitgestellt werden kann. Ein weiterer entscheidender Vorteil: Softwaredefinierte Segmentierung erfordert keine Änderungen am Netzwerk oder Ausfallzeiten der Anwendungen. Durch diese Zeiteinsparungen und Effizienzsteigerungen verursacht der gesamte Implementierungszyklus deutlich geringere Kosten.

Die Fallstricke konventioneller Ansätze

Um die Vorteile einer softwaredefinierten Segmentierung oder Mikrosegmentierung zu verstehen, ist es nützlich, sich zu Vergleichszwecken einige der Nachteile und Einschränkungen von Standardtechniken anzusehen, die sowohl lokal als auch in der Cloud eingesetzt werden. Das kann eine Kombination aus physischen oder virtuellen Firewalls und Netzwerkkonfigurationen wie VLANs umfassen. Im Allgemeinen verschlingen diese Methoden erhebliche Ressourcen und sind arbeitsintensiv. Das Erstellen von Sicherheitsrichtlinien ist ein umständlicher Prozess. Ergänzungen und Änderungen müssen manuell vorgenommen werden, was die betriebliche Effizienz beeinträchtigt und das Risiko einer Schwachstelle erhöht.

Insbesondere interne Firewalls sind teuer in der Anschaffung und komplex in der Einrichtung. Sie stören außerdem den normalen Traffic, verändern Muster und verursachen „Hairpinning“, was letztendlich die System-Performance beeinträchtigt. Wie in der Branche gerade festgestellt wird, eignen sich Firewalls nicht für die Segmentierung innerhalb des Rechenzentrums – einige Anbieter sagen, dass Firewalls dort einfach nicht eingesetzt werden sollten.

Eine der schwierigsten Herausforderungen bei der Einführung einer Segmentierung in eine vorhandene, laufende Produktionsumgebung besteht darin, dass herkömmliche Methoden Ausfallzeiten von Anwendungen erforderlich machen. Ausfallzeiten verursachen Kosten. Sie können nur innerhalb bestimmter Zeitfenster geschehen und sind oft sogar gar nicht möglich.

Eine weitere Herausforderung, die es zu beachten gilt, ist, dass die Erstellung einer internen Segmentierung gute Kenntnisse über Abhängigkeiten zwischen East-West-Anwendungen erfordert. Solche Einblicke stehen in der Regel nicht zur Verfügung. Ohne eine einfache Methode zur Zuordnung von Anwendungsabhängigkeiten ist die Segmentierung einer Industrieumgebung extrem schwierig und riskant.

Warum softwaredefinierte Segmentierung effektiver ist

Betriebseffizienz, verbesserte Sicherheit: Die softwaredefinierte Segmentierung ist den ineffizienten traditionellen Techniken überlegen und – was der wichtigere Punkt ist – führt in Umgebungen mit mehreren Nutzern zu mehr Sicherheit. Wie der Name schon sagt, übernimmt die softwaredefinierte Segmentierung das Konzept der Netzwerksegmentierung und setzt es ohne Infrastrukturänderungen um. Dabei werden Sicherheitsrichtlinien für einzelne oder logisch gruppierte Anwendungen festgelegt, unabhängig davon, wo sie sich im hybriden Rechenzentrum befinden. Diese Richtlinien bestimmen, welche Anwendungen miteinander kommunizieren können und nicht – echtes Zero Trust.

Keine manuellen Änderungen oder Ausfallzeiten: Für die softwaredefinierte Segmentierung sind keine Änderungen am Netzwerk erforderlich, und es müssen keine VLANs erstellt werden, wodurch erheblich Betriebskosten gespart werden. Es sind auch keine Ausfallzeiten der Anwendung oder Änderungen aufgrund einer Migration in ein neues VLAN erforderlich. Das ist wichtig. In vielen Anwendungen, bei denen Ausfallzeiten sehr teuer oder sogar unmöglich sind, ist dies die einzige Möglichkeit, diese wichtige Sicherheitsmaßnahme bereitzustellen.

Umfassende Transparenz: Darüber hinaus bieten fortschrittliche softwaredefinierte Segmentierungslösungen, die die Herausforderungen der Segmentierung von East-West-Traffic bewältigen sollen, ein integriertes Sichtbarkeitstool, das die Segmentgrenzen und Anwendungsabhängigkeiten identifiziert. Dadurch ist der Prozess sehr effizient, und operative Fehler bei der Erstellung der Richtlinien werden beseitigt.

Automatisierung von Richtlinien und Kontrollen: Durch die softwaredefinierte Segmentierung können Richtlinien auch dynamisch angewendet werden, sodass Workloads automatisch der richtigen Richtlinie zugeordnet werden, wenn sie beginnen und enden. Dadurch werden erhebliche Mengen von Ressourcen eingespart, da kein manuelles Verschieben und keine Ergänzungen oder Änderungen erforderlich sind.

Infrastrukturunabhängig: Ein wichtiger Vorteil der softwaredefinierten Segmentierung ist, dass sie infrastrukturunabhängig ist. Dasselbe Tool bietet Transparenz und Segmentierung in jeder Infrastruktur: Bare Metal, virtualisiert, PaaS, Cloud, Container, usw. Alles mit einer Verwaltungskonsole und einem einzigen Workflow. Dies führt zu einer erheblichen operativen Freiheit, in der Sicherheitsstandards ohne Einschränkungen der zugrunde liegenden Infrastruktur umgesetzt werden können.

Mehr Umsatz, stärkere Beziehungen: Vor allem aber bietet dies den Betreibern von Rechenzentren eine große Chance. Während sie die interne Segmentierung verwalten und bereitstellen, können sie die Schulungen, Tools und Prozesse nutzen, um ihren Kunden einen besonders wichtigen Managed Service zu bieten: Die Segmentierung nicht nur der gehosteten Anwendungen, sondern auch der Anwendungen, die sich am Kundenstandort oder in der Cloud befinden, und das mit demselben Tool und über dieselbe Verwaltungskonsole. Dies bedeutet nicht nur potenziell mehr Umsatz, sondern auch eine stärkere Abhängigkeit vom Betreiber, was zu längeren Beziehungen und höheren Gewinnen führt.

Warum Akamai?

Um diese Vorteile nutzen zu können, muss eine Lösung zur softwaredefinierten Segmentierung eine Reihe von grundlegenden Kriterien erfüllen. Sie muss einen umfassenden Einblick auf Prozessebene in alle Anwendungen ermöglichen, die in der Computing-Umgebung ausgeführt werden, und die Fähigkeit haben, alle Datenströme zwischen ihnen abzubilden. Die Flexibilität, Assets für die Erstellung von Richtlinien korrekt zu kennzeichnen und Kennzeichnungen automatisch zu ändern, wenn Workloads automatisch skaliert werden, ist ebenfalls entscheidend für eine effiziente Bereitstellung und Verwaltung. Und die Lösung muss plattform- und infrastrukturunabhängig sein. Richtlinien müssen ihren jeweiligen Anwendungen folgen können und in mehreren Umgebungen konsistent funktionieren. Schließlich sollte die Lösung ein automatisiertes und vereinfachtes Betriebsmodell für die Erstellung, Verwaltung und Durchsetzung von Richtlinien ermöglichen.

Nur Akamai Guardicore Segmentation erfüllt all diese Kriterien. Die softwaredefinierte Segmentierung ist unsere Kernfunktion. Die Lösung bietet eine beispiellose grafische Visualisierung aller Assets in der Umgebung und der Abhängigkeiten zwischen ihnen – ob Bare Metal, virtuelle Maschinen, Public Cloud, Container oder IoT-Geräte. Diese hohe Transparenz beschleunigt den Prozess der Identifizierung, Gruppierung und Erstellung von Sicherheitsrichtlinien um Mikrosegmente von Anwendungen erheblich.

Weitere Informationen hierzu finden Sie unter akamai.com/guardicore.