Akamai

WHITEPAPER

Der Zustand der Segmentierung im Jahr 2023

Das Überwinden von Bereitstellungshindernissen erweist sich als Vorteil

Inhaltsverzeichnis

Einführung

Leicht hatten es IT-Sicherheitsabteilungen noch nie. Heute jedoch gehen Angreifer immer raffinierter vor. Sie kombinieren Techniken, um immer größere Bedrohungen für immer häufigere Angriffe zu entwickeln. Damit setzten sie Sicherheitsteams stärker unter Druck als je zuvor. Kein Unternehmen kann ohne Onlinepräsenz arbeiten und ein erfolgreicher Angriff kann erheblichen, wenn nicht gar irreparablen Schaden für Reputation und Umsatz verursachen.

Wie die Ergebnisse in diesem Bericht zeigen, haben diese Angriffe inzwischen auch größere Auswirkungen. Damit erhöht sich der Druck auf Sicherheitsexperten, die richtigen Lösungen zu finden und die gesamte Umgebung zu schützen, ohne die allgemeine Performance oder die Innovationsfähigkeit zu beeinträchtigen.

Die Ergebnisse dieses aktuellen Berichts, der die Veränderungen gegenüber 2021 aufzeigt, sollen Aufschluss darüber geben, ob Segmentierung effektiv ist und als bevorzugte Lösung gelten kann. Die 1.200 Befragten waren sich mit überwältigender Mehrheit einig darüber, dass Segmentierung Assets effektiv schützt. Der Fortschritt bei ihrer Umsetzung für kritische Geschäftsanwendungen und -Assets war unter den Teilnehmern jedoch geringer als erwartet. Das größte Hindernis war in allen Regionen der Mangel an Fachwissen bei der Implementierung von Segmentierung. Dies deutet darauf hin, dass Teams möglicherweise zögern, ein Projekt zu starten, das die Performance beeinträchtigen könnte. Das gilt zumal angesichts der zunehmenden Komplexität von IT-Umgebungen.

Die gute Nachricht: Durchhaltevermögen zahlt sich aus. Für jene, die die meisten ihrer kritischen Assets segmentiert hatten, erwies sich die Segmentierung als überaus effektive Abwehrlösung. So konnten die Verantwortlichen Ransomware 11 Stunden schneller abwehren und eindämmen als diejenigen, die nur eine einzelne Ressource segmentiert hatten. Stellen Sie sich vor, welchen Unterschied diese 11 Stunden für Ihr Team, Ihre Kunden, den Ruf Ihrer Marke und Ihren Umsatz machen.

Ransomware-Angriffe und ihre Auswirkungen nehmen weiter zu

Die Zahl der (erfolgreichen und erfolglosen) Ransomware-Angriffe hat sich in den letzten zwei Jahren von durchschnittlich 43 im Jahr 2021 auf 86 im Jahr 2023 verdoppelt. Ein noch stärkerer Anstieg wurde zwischen dem 1. Quartal 2022 und dem 1. Quartal 2023 anhand von Daten gemessen, die auf den Leak-Websites von etwa 90 verschiedenen Ransomware-Gruppen erfasst wurden. Aus dem im August 2023 veröffentlichten Bericht Ransomware auf dem Vormarsch: Raffinierte Ausnutzungstechniken und Zero-Day-Angriffe geht hervor, dass die Ausnutzung von Zero-Day- und One-Day-Schwachstellen weltweit zu einem Anstieg der von Ransomware Betroffenen um 143 % geführt hat.

Es überrascht nicht, dass US-Unternehmen immer noch mit der größten Anzahl von Ransomware-Bedrohungen konfrontiert sind (Abbildung 1): IT-Sicherheitsteams und Entscheidungsträger in den USA verzeichneten in den letzten 12 Monaten durchschnittlich 115 Ransomware-Angriffe. Das sind mehr als in jedem anderen in der Umfrage erfassten Land.

Durchschnittliche Anzahl der Ransomware-Angriffe in den letzten 12 Monaten nach Ländern

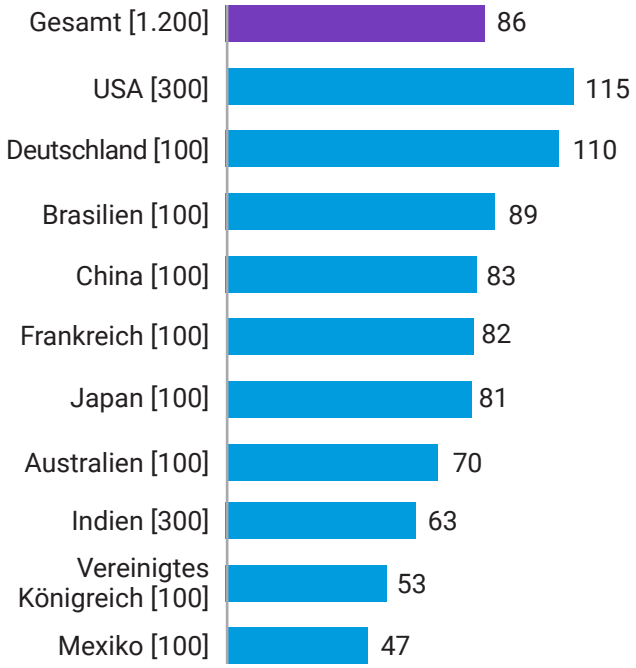

Abb. 1: Wie oft wurde Ihr Unternehmen in den letzten 12 Monaten von Ransomware angegriffen (unabhängig davon, ob die Angriffe erfolgreich waren oder nicht)? [1.200], gibt nur die durchschnittliche Anzahl der Angriffe in den letzten 12 Monaten an; aufgeschlüsselt nach Ländern.

Die USA sind eines der beiden Länder, in denen eine Segmentierung von mehr als zwei unternehmenskritischen Geschäftsbereichen am wenigsten wahrscheinlich war (Abbildung 2). Insofern könnte ihr Spitzenplatz bei Ransomware-Angriffen mit der niedrigen Platzierung bei der Implementierung von Segmentierung zusammenhängen.

Natürlich ist die hohe Zahl von Ransomware-Angriffen in den USA wohl auf unterschiedliche Faktoren zurückzuführen. Dazu gehören aufsehenerregende Großangriffe wie jener, den russische Cyberkriminelle 2023 auf Bundesbehörden verübt haben, oder die Verbreitung von IoT-Geräten in den USA (2 Milliarden mehr als der Zweitplatzierte China). Ransomware für IoT (R4IoT) nutzt anfällige IoT-Geräte wie IP-Kameras aus, um sich erst einmal festzusetzen und dann lateral in einem IT-Netzwerk zu bewegen. So machen sich die Angreifer unzureichende Sicherheitspraktiken zunutze, um unternehmenskritische Prozesse als „Geisel" zu nehmen.

Ransomware-Angriffe sind 2023 im Vergleich zu 2021 nicht nur weltweit häufiger, sondern auch erfolgreicher (Abbildung 3). Die Umfrageteilnehmer gaben an, dass Netzwerkausfälle, Datenverluste und Reputationsschäden zunehmen. All dies erhöht den Handlungsdruck für Sicherheitsteams erheblich. Die Auswirkungen dieses Drucks sehen wir auch bei der Strategie: Die Zahl der Unternehmen, die Strategien oder Richtlinien zur Cybersicherheit kontinuierlich aktualisieren, ist von 5 % im Jahr 2021 auf 13 % im Jahr 2023 gestiegen. Dies geschah nicht nur als Antwort auf Ransomware, sondern generell in Reaktion auf die ständige Veränderung der Angriffsfläche. Remote-Arbeitsmodelle und verteilte Anwendungen sowie die Migration von Daten in die Cloud sind nur zwei Faktoren, die sich tagtäglich auf die Sicherheitsstrategie auswirken.

Segmentierung von mehr als zwei Assets/Bereichen (nach Ländern)

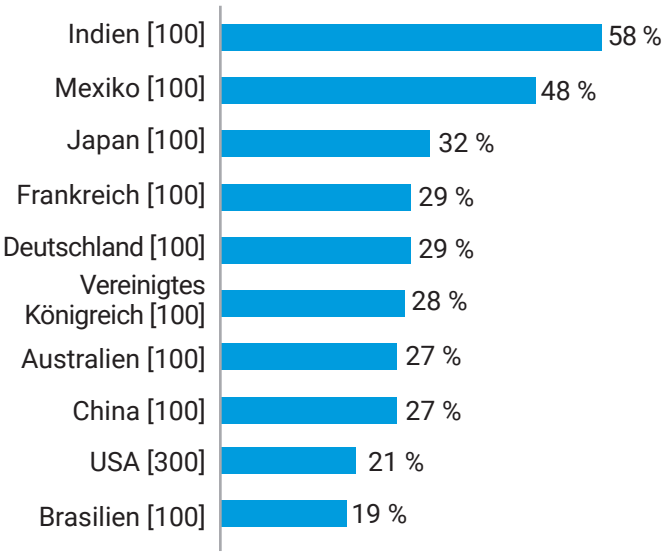

Abb. 2: Welche Assets decken die folgenden IT-Sicherheitsmaßnahmen jeweils ab? [1.200], zeigt nur Antworten für die Sicherheitsmaßnahme Segmentierung und Prozentsätze in Bezug auf die Nutzung von Segmentierung zum Schutz wichtiger Assets; aufgeschlüsselt nach Ländern.

Auswirkungen von Ransomware/Cyberangriffen

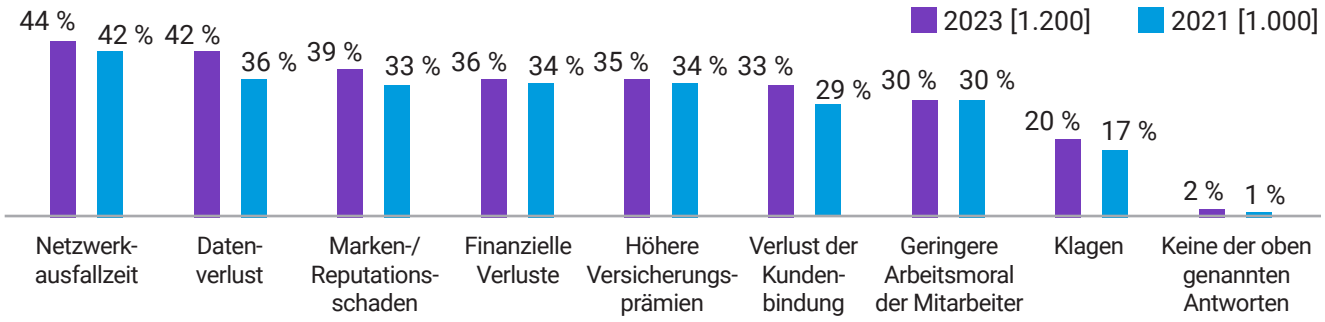

Abb. 3: Welche der folgenden Auswirkungen hatte es für Ihr Unternehmen, wenn es in der Vergangenheit Ransomware oder einen anderen Cyberangriff erkannt hat? [Basisgrößen in Diagramm], nicht alle Antwortoptionen werden angezeigt; aufgeschlüsselt nach historischen Daten.

Erkenntnisse nach Regionen

In Nord- und Südamerika ist die Wahrscheinlichkeit von Cyberangriffen höher: Die Gesamtzahl der Ransomware-Angriffe ist in Nord- und Südamerika mit durchschnittlich 96 Angriffen in den letzten 12 Monaten am höchsten. Zum Vergleich: In EMEA waren es 83 und in APAC 75 Angriffe.

Segmentierung und Mikrosegmentierung werden in APAC und Nord- und Südamerika als wichtiger angesehen als in EMEA: Dass die Netzwerksegmentierung äußerst wichtig ist, um die Sicherheit des Unternehmens sicherzustellen, sagen mehr IT-Sicherheitsteams und Entscheidungsträger in APAC (62 %) und Nord- und Südamerika (60 %) als in EMEA (53 %).

Befragte in Nord- und Südamerika gaben eher an, dass Mikrosegmentierung die oberste Priorität habe (41 %), als in APAC (35 %) oder EMEA (23 %).

Die Wahrscheinlichkeit, dass überhaupt Segmentierungen durchgeführt wurden, ist in EMEA-Ländern höher: Unternehmen sagen mit weit größerer Wahrscheinlichkeit in EMEA (10 %), dass keine geschäftskritischen Assets segmentiert wurden, als dies in APAC (4 %) oder Nord- und Südamerika (1 %) der Fall ist.

Die niedrigsten Implementierungsraten (das heißt: noch kein Bereich wurde segmentiert) wurden im Vereinigten Königreich festgestellt (23 %), wobei veraltete Ausrüstung als Haupthindernis angegeben wurde (46 %).

Unternehmen in APAC haben am meisten segmentiert: Der Anteil der Unternehmen, die mehr als zwei geschäftskritische Assets segmentiert haben, ist in APAC (36 %) höher als in EMEA (29 %) oder Nord- und Südamerika (26 %).

Unternehmen in allen Regionen stehen vor Herausforderungen: 97 % der Befragten in Nord- und Südamerika geben an, dass sie Probleme bei der Segmentierung ihres Netzwerks haben. Ähnlich hoch ist hier der Anteil in EMEA (94 %) und APAC (97 %).

Die EMEA- und APAC-Länder nennen fehlende Kompetenzen/Fachkenntnisse (38 % bzw. 43 %) als größtes Hindernis für die Segmentierung. Das größte Hindernis für Unternehmen in Nord- und Südamerika sind vermehrte Performance-Engpässe (41 %).

Mehr Unternehmen in Nord- und Südamerika sehen ihre Zero-Trust-Sicherheitsframeworks als ausgereift an: In Nord- und Südamerika erklärt ein größerer Anteil der Unternehmen, die Zero-Trust-Implementierung vollständig abgeschlossen und definiert zu haben (49 %), als in APAC (35 %) oder EMEA (33 %).

Segmentierung ist allgemein als wichtiger Teil von Zero Trust anerkannt

Die Befragten sind sich einig, dass Segmentierung wichtig ist, um die Sicherheit des Unternehmens zu gewährleisten, insbesondere bei der Abwehr von Malware. Branchenübergreifend glauben 93 % der Umfrageteilnehmer, dass Segmentierung wichtig ist, um schädliche Angriffe abzuwehren. In der verarbeitenden Industrie und im produzierenden Gewerbe liegt der Anteil sogar bei 99 %. Dies könnte darauf zurückzuführen sein, dass diese Branchen in ihrer Lieferkette stark auf Drittanbieter angewiesen sind, sodass Unterbrechungen Kaskadeneffekte mit massiven Auswirkungen für das Geschäft auslösen können.

Segmentierung ist auch ein wesentlicher Bestandteil eines Zero-Trust-Frameworks. Der am dritthäufigsten genannte Grund, warum das Unternehmen mit einem Segmentierungsprojekt begonnen hat, war die Entwicklung von Zero Trust: Fast alle Befragten, die überhaupt segmentiert haben, implementieren ein Zero-Trust-Sicherheitsframework oder haben es bereits implementiert (99 %). Allerdings haben nur zwei von fünf (40 %) der befragten Unternehmen das Zero-Trust-Framework vollständig definiert und abgeschlossen.

Weltweit strebt die Mehrheit der Befragten an, weiterzugehen und Mikrosegmentierung zu implementieren, um Anwendungs-Workloads auf einer granularen Ebene zu schützen: 89 % geben an, Mikrosegmentierung habe mindestens eine hohe Priorität, und 34 % nennen sie als ihre oberste Priorität. Darüber hinaus geben 97 % der IT-Sicherheitsteams und Entscheidungsträger an, dass sie mindestens von einem kleineren Teil ihrer Branche angewendet wird. Im öffentlichen Sektor liegt der Wert lediglich bei 80 % (ohne Gesundheitswesen). Dieser Unterschied könnte auf knappere Budgets und veraltete Infrastrukturen zurückzuführen sein, die einer Implementierung von Workload-Level-Schutz durch Mikrosegmentierung im Wege stehen.

Mikrosegmentierung

der IT-Sicherheitsteams und Entscheidungsträger geben an, dass Mikrosegmentierung mindestens von einem kleineren Teil ihrer Branche angewendet wird

Doch der öffentliche Sektor kann von der Implementierung moderner Sicherheitstechniken wie Mikrosegmentierung sehr profitieren. Da Systeme in diesem Sektor nicht unbedingt darauf ausgelegt sind, miteinander zu interagieren, fehlt es ihnen an Interoperabilität, was sowohl die Wahrscheinlichkeit menschlicher Fehler als auch die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs erhöht.

In Bezug auf Segmentierung geben 15 % der Befragten im öffentlichen Sektor an, dass keine Segmentierung vorhanden ist, obwohl 93 % ihre Bedeutung anerkennen. Dies entspricht dem niedrigsten Implementierungsniveau aller Sektoren, wobei Compliance-Anforderungen das größte Hindernis darstellen (52 %).

Segmentierung ist gut. Mikrosegmentierung ist besser.

Segmentierung ist ein Architekturansatz, bei dem ein Netzwerk in kleinere Segmente unterteilt wird, um Performance und Sicherheit zu verbessern.

Durch die Mikrosegmentierung wird ein Netzwerk auf der Ebene der einzelnen Workloads in Segmente unterteilt, sodass Sicherheitskontrollen und Servicebereitstellung für jedes einzelne Segment definiert werden können.

Implementierungen gehen langsam voran, doch Beharrlichkeit zahlt sich aus

Zwar gibt es eine breite Zustimmung für die These, dass Segmentierung der Schlüssel zur Abwehr von Angriffen ist. Die ernüchternde Realität ist jedoch, dass die Implementierung von Segmentierungen nur langsam vorankommt – langsamer als vielleicht erwartet. Nur 30 % der Unternehmen haben 2023 mehr als zwei kritische Geschäftsbereiche segmentiert (gegenüber 25 % im Jahr 2021), und 44 % haben vor zwei oder mehr Jahren ein Netzwerksegmentierungsprojekt gestartet, was darauf hindeutet, dass die Bemühungen zum Stillstand gekommen sind.

Langsame Implementierungen lassen sich am überzeugendsten durch die wesentlichen Hindernisse erklären, mit denen die Befragten konfrontiert sind: Mangel an Kompetenzen/Fachwissen für die Segmentierung (39 %), zunehmende Performance-Engpässe (39 %) und Compliance-Anforderungen (38 %; Abbildung 4). Fast alle Befragten berichteten unabhängig von Sektor, Branche oder Land über die gleichen Hindernisse (wenn auch in unterschiedlichem Ausmaß). Erwähnenswert ist, dass fehlende Kompetenzen/Fachwissen die häufigste Ursache für Verzögerungen bei Segmentierungsprojekten ist, während gleichzeitig im gesamten Bereich der Cybersicherheit die Fachkräfte rar sind. Da sich außerdem die Veränderungen auf diesem Gebiet so schnell vollziehen, sind Kompetenzlücken kaum zu vermeiden.

Trotz des langsamen Fortschritts nehmen die Segmentierungsraten insgesamt allmählich zu. Der Prozentsatz der Unternehmen mit segmentierten geschäftskritischen Anwendungen/Daten stieg von 2021 bis 2023 um 12 % und die segmentierten Server um 8 %.

Hindernisse beim Segmentieren des Netzwerks

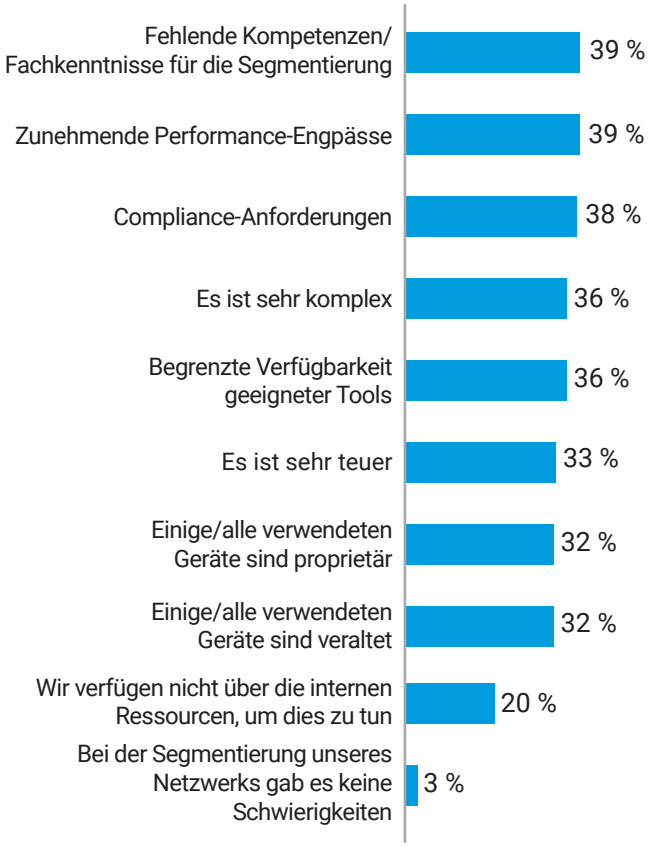

Abb. 4: Mit welchen Problemen war Ihr Unternehmen bei der Segmentierung des Netzwerks konfrontiert bzw. mit welchen Problemen rechnen Sie? [1.187], wurde nur Teilnehmern angezeigt, die ihr Netzwerk zu einem bestimmten Zeitpunkt segmentiert haben; nicht alle Antwortoptionen sind angegeben.

Die Erkenntnis: Segmentierung von sechs kritischen Geschäftsbereichen senkt das Risiko erheblich

Der Schutz und die Segmentierung von mehr Assets macht das Unternehmen sofort sicherer. Sicherheitsteams sind besser in der Lage, Angriffe zu erkennen und effektiver zu reagieren. Die Implementierung unausgereifter oder schlecht definierter Segmentierungsstrategien erhöht wahrscheinlich nur das Risiko eines Unternehmens. Für eine richtig durchgeführte Segmentierung lohnt es sich aber zweifellos, alle Hindernisse zu überwinden und die Implementierung vorzunehmen.

Unsere Ergebnisse zeigen, dass mit Segmentierung die Wiederherstellung nach einem Angriff 11 Stunden schneller erfolgt. Eine einfache Rechnung: Bei Unternehmen, die eine Segmentierung in sechs unternehmenskritischen Bereiche implementiert haben, dauert es durchschnittlich vier Stunden, bis ein Ransomware-Angriff vollständig gestoppt ist. Bei denjenigen, die nur ein Asset segmentiert haben, sind es 15 Stunden.

Mit Segmentierung beschleunigt sich auch die Eindämmung lateraler Bewegungen um 11 Stunden. Für diejenigen, die Segmentierungen über alle sechs unternehmenskritische Bereiche hinweg implementiert haben, dauert es durchschnittlich drei Stunden, die laterale Bewegung eines Ransomware-Angriffs signifikant zu begrenzen. Bei Unternehmen mit einer Segmentierung für nur ein Asset dauert dies durchschnittlich 14 Stunden.

Überlegen Sie, welchen Unterschied 11 Stunden für Ihr Team und für die Eindämmung von Kosten und Markenschäden in den beiden Szenarien machen.

Einen Angriff stoppen

4 Stunden

Die durchschnittliche Zeit, die benötigt wird, um einen Ransomware-Angriff vollständig zu stoppen (für diejenigen, die alle sechs Unternehmensressourcen segmentiert haben)

Für diejenigen, die nur ein Asset segmentiert haben: **15 Stunden**

Bewegung begrenzen

3 Stunden

Die durchschnittliche Zeit, die erforderlich ist, um die laterale Netzwerkbewegung eines Ransomware-Angriffs signifikant zu begrenzen (für diejenigen, die alle sechs Unternehmensressourcen segmentiert haben)

Für diejenigen, die nur ein Asset segmentiert haben: **14 Stunden**

Wie eine softwarebasierte Mikrosegmentierungslösung Herausforderungen meistert

Mikrosegmentierung ermöglicht nicht nur eine fortschrittlichere, detailliertere Segmentierung, sondern erleichtert auch die Implementierung.

Softwarebasierte Lösungen wie Akamai Guardicore Segmentation können schnell implementiert werden, ohne dass physische Änderungen am Netzwerk vorgenommen werden müssen. Sie müssen Ihren neuen Segmenten keine neuen IP-Adressen zuweisen oder sich Gedanken darüber machen, wo sich Ihre physischen Server und Geräte befinden könnten. Dies macht die Bereitstellung der Lösung wesentlich schneller und einfacher als infrastrukturbasierte Ansätze wie Firewalls und VLANs. Und da die Lösung einen eigenen proprietären Treiber für die Durchsetzung von Richtlinien verwendet, funktioniert sie nahtlos über alle Rechner und Betriebssysteme hinweg: von Bare-Metal-Servern bis hin zu Multicloud-Bereitstellungen, von Legacy-Technologien wie Windows Server 2003 bis hin zu den neuesten IoT/OT-Geräten und containerisierten Technologien. Das bedeutet, dass Sie nur eine einzige Lösung mit einer Schnittstelle verwalten, um Verbindungen, die von verschiedenen Betriebssystemen und Geräten in Ihrer gesamten Umgebung hergestellt werden, unabhängig von ihrem physischen Standort zu visualisieren und zu steuern.

Wie sie die Bereitstellung erleichtert

Die Mikrosegmentierung erzeugt zunächst eine interaktive Darstellung aller Verbindungen in Ihrer Umgebung, was eine wichtige Komponente zur Überwindung der wichtigsten Hindernisse für die Implementierung ist. Darüber hinaus hat Akamai in die Lösung Optionen zur aktiven Behebung von Performance-Engpässen und zum Umgang mit Compliance-Anforderungen integriert.

Performance-Engpässe entstehen nicht notwendigerweise infolge von technischen Belastungen eines Systems, die durch eine Segmentierungslösung verursacht werden. Vielmehr können sie aus Personalengpässen resultieren, die auftreten, wenn Geschäftsbereiche manuell segmentiert und Probleme in diesen Bereichen dann manuell behoben werden müssen. Bei Akamai arbeiten wir daran, dieses Problem – und das Problem fehlender Expertise als größtes Hindernis für die Implementierung – zu lösen, indem wir die Notwenigkeit einer manuellen Segmentierung reduzieren und technischen Support sowie Professional Services auf höchstem Niveau anbieten. Unsere Segmentierungsexperten arbeiten während des gesamten Implementierungsprozesses mit Ihnen zusammen, um sicherzustellen, dass Sie die Segmentierungsziele in Ihrer speziellen IT-Umgebung erreichen.

Unterstützung bei der Implementierung bietet auch die Lösung selbst: Die auf KI basierenden Richtlinienempfehlungen und vorkonfigurierten Richtlinienvorlagen für häufige Anwendungsfälle sparen Zeit und Klicks, vereinfachen den Workflow, verkürzen die Gesamtzeit bis zur Richtlinieneinführung und verhindern Fehlkonfigurationen aufgrund menschlicher Fehler. Für einen unserer Kunden konnten wir mit einem einzigen Ingenieur ein Projekt zur granularen Segmentierung, für das eine Dauer von zwei Jahren und Gesamtkosten von 1 Million US-Dollar veranschlagt waren, in nur sechs Wochen durchführen. Dadurch konnten die Gesamtkosten des Projekts um 85 % gesenkt werden. Das Beispiel macht deutlich, dass eine granulare Segmentierung schnell und einfach ohne Belastung durch Engpässe implementiert werden kann.

Wie sie Compliance erleichtert

Viele unserer Kunden verwenden unsere Lösung, um die Einhaltung verschiedener nationaler und internationaler Compliance-Auflagen wie PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, DSGVO zu gewährleisten und nachzuweisen. Diese Compliance-Auflagen verlangen in der Regel, dass die betreffenden Daten von anderen Systemen in Ihrer Umgebung getrennt werden. Während es kostspielig sein kann, dies mithilfe von Firewalls und VLANs zu erreichen, können Sie mit unserer softwarebasierten Lösung Segmente speziell für die bereichsinternen Daten erstellen. Außerdem können Sie durch Kommunikationsregeln steuern, was auf diese Daten zugreifen kann und was nicht. Mithilfe unserer visuellen Karte, die Ansichten nahezu in Echtzeit sowie Verlaufsansichten bietet, können Sie die Einhaltung dieser Auflagen nachweisen, indem Sie physisch aufzeigen, dass nur autorisierte Nutzer und Computer auf die betreffenden Daten zugreifen.

Mit der richtigen Lösung und dem richtigen Support verbessern Sie Ihre Sicherheitslage nachhaltig

Die Implementierung einer Segmentierung kann sehr schwierig sein. Doch dieser Bericht zeigt: Wer es schafft, sie effektiv umzusetzen, senkt sein Cyberrisiko erheblich. Eine ordnungsgemäße Segmentierung begrenzt die laterale Netzwerkbewegung von Bedrohungen und ermöglicht Ihnen, bei einem akuten Angriff schneller zu reagieren. Außerdem sind nach einem Angriff die Wiederherstellungsmaßnahmen gesichert und benötigen weniger Zeit.

Wenn Sie sich für eine Lösung entscheiden, die die häufigsten Herausforderungen bei der Implementierung einer Segmentierung bewältigen soll, und wenn Sie dabei mit den zur Verfügung gestellten Experten zusammenarbeiten, sind Sie optimal aufgestellt, um Ihre Sicherheitslage grundlegend zu verbessern. Und je mehr Geschäftsbereiche Sie segmentieren, desto größere Fortschritte erzielen Sie auch für Ihre Zero-Trust-Architektur, denn Sie reduzieren Ihr gegenwärtiges Risiko und errichten eine erste Verteidigungslinie gegen künftige Bedrohungen.

Die Umfrageteilnehmer

Wir haben 1.200 Entscheidungsträger im Bereich IT und Sicherheit in 10 Ländern befragt, um die Fortschritte zu messen, die Unternehmen bei der Sicherung ihrer Umgebungen erzielt haben. Dabei wurde der Schwerpunkt auf die Rolle der Segmentierung gelegt.

Es wurden Fragen zu den IT-Sicherheitsansätzen, Segmentierungsstrategien und zu den Bedrohungen gestellt, denen die Unternehmen 2023 ausgesetzt waren. Diese Ergebnisse geben uns Einblicke in die Veränderung der Sicherheitsstrategien seit 2021 und in die Bereiche, in denen noch Fortschritte erzielt werden müssen.

Befragt wurden Sicherheitsexperten und Entscheidungsträger aus den USA, Mexiko, Brasilien, dem Vereinigten Königreich, Frankreich, Deutschland, China, Indien, Japan und Australien. Alle arbeiteten für Unternehmen mit mehr als 1.000 Mitarbeitern und repräsentierten ein ausgewogenes Spektrum von Branchen und Sektoren.

Hinweis: Diese Stichprobe unterschied sich geringfügig von der des Jahres 2021. Stichprobengrößen – 2023: 1.200 ausgefüllte Umfragen, 2021: 1.000 ausgefüllte Umfragen. 2023 wurden auch Teilnehmer aus Australien, Japan und China befragt. Die Sektoren unterschieden sich leicht von 2021. 2023 richteten wir einen speziellen Fokus auf den digitalen Handel als eigenen Sektor.

Weitere Informationen zu Akamai Guardicore Segmentation

Akamai schützt Ihr Kundenerlebnis, Ihre Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Anwendungen und APIs zu schützen und Ihre Infrastruktur zu sichern. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn. Veröffentlicht: 10/23.

VansonBourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Das Unternehmens hat sich mit robusten und glaubwürdigen forschungsbasierten Analysen einen hervorragenden Ruf erworben. Die Analysen gründen auf strengen Forschungsprinzipien und der Fähigkeit, die Meinung von Entscheidungsträgern in technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und in allen wichtigen Märkten einzuholen. Weitere Informationen finden Sie unter www.vansonbourne.com.