Akamai

E-BOOK

Bereitstellungshindernisse zum Schutz kritischer Banksysteme überwinden

Globaler Bericht zum Zustand der Segmentierung

Inhaltsverzeichnis

Einführung

Der Schutz der Finanzdienstleistungsbranche hat IT-Sicherheitsteams schon immer vor besondere Herausforderungen gestellt. Inzwischen gehen Angreifer jedoch noch raffinierter vor. Sie kombinieren Techniken und steigern so das Ausmaß und die Frequenz der Bedrohungen. Damit setzen sie die Sicherheitsteams der Finanzdienstleister stärker unter Druck als je zuvor. Finanzdienstleister sind in ihrem Geschäft auf ihre digitale Präsenz angewiesen 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 – es muss die gesamte Umgebung geschützt und die allgemeine Performance beibehalten werden, ohne eine Offenlegung großer Mengen an sensiblen Daten zu riskieren.

Die befragten Finanzdienstleister (an der Umfrage beteiligten sich Vertreter der Regionen USA, LATAM, EMEA und APAC) sind sich über die Effektivität der Segmentierung beim Schutz von Assets weitgehend einig. Insgesamt jedoch sind die Fortschritte bei der Bereitstellung von Segmentierung für kritische Geschäftsanwendungen, Server und Assets geringer als erwartet. Das größte Hindernis für Finanzdienstleister sind zunehmende Engpässe. Das deutet darauf hin, dass Teams möglicherweise auf Bedrohungen reagieren, ohne über ausreichend Zeit oder Unterstützung zu verfügen, um die sich aus Änderungen ergebenden Auswirkungen auf die Performance vollständig zu verstehen und abzumildern.

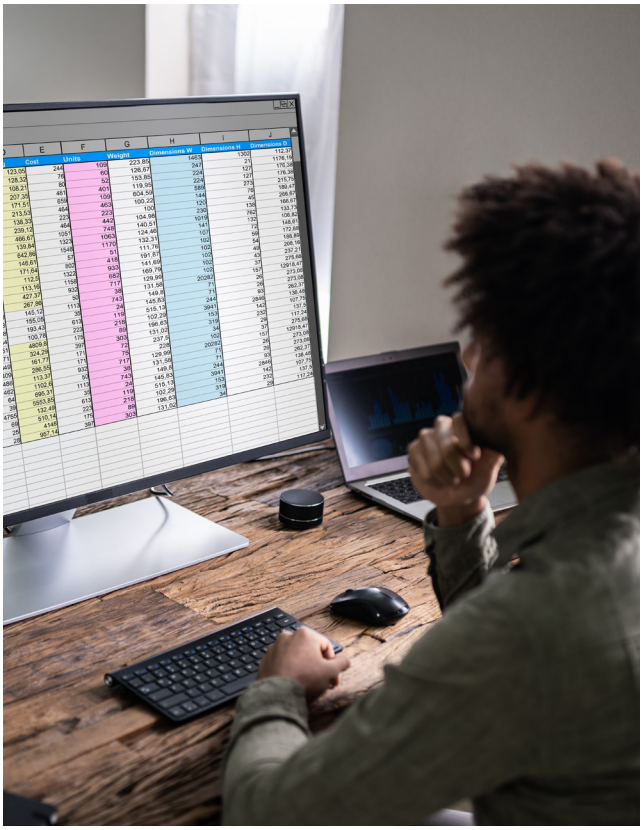
Die gute Nachricht: Durchhaltevermögen zahlt sich aus. Für jene, die die meisten ihrer kritischen Assets segmentiert hatten, erwies sich die Segmentierung als überaus effektive Abwehrlösung. So konnten die Verantwortlichen Ransomware 13 Stunden schneller abwehren und eindämmen als diejenigen, die nur eine einzelne Ressource segmentiert hatten. Stellen Sie sich vor, welchen Unterschied diese 13 Stunden für Ihr Team, Ihre Kunden und Ihre Reputation machen.

Das Ergebnis: Beim Thema Segmentierung geht es insgesamt langsam voran, doch wer durchhält, reduziert sein Risiko enorm.

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.

Die Mikrosegmentierung ist eine Sicherheitstechnik, mit der Sie ein Netzwerk logisch in verschiedene Sicherheitssegmente unterteilen können, bis hin zur individuellen Workload-Ebene. Sicherheitskontrollen und Servicebereitstellung können dann für jedes einzelne Segment definiert werden.



Ransomware-Angriffe und ihre Auswirkungen nehmen weiter zu

Die Zahl der (erfolgreichen und erfolglosen) Ransomware-Angriffe bei Finanzdienstleistern hat in den letzten zwei Jahren von durchschnittlich 43 im Jahr 2021 auf 62 im Jahr 2023 zugenommen. Das entspricht einem Anstieg um fast 50 %. Zwar gelten die Sicherheitsmaßnahmen der Branche als zuverlässig, doch die Zahlen offenbaren eine kritische Anfälligkeit, die nicht übersehen werden darf. Es ist offensichtlich, dass der Finanzdienstleistungssektor nicht immun gegen die Bedrohung durch Ransomware ist und sich keineswegs in Sicherheit wiegen kann.

Finanzdienstleister in der APAC-Region waren im Durchschnitt am häufigsten das Ziel von Ransomware-Angriffen (73). Am niedrigsten lag die Zahl der Angriffe in LATAM (48, Abbildung 1).

Durchschnittliche Anzahl der Ransomware-Angriffe im Finanzdienstleistungssektor in den letzten 12 Monaten nach Region

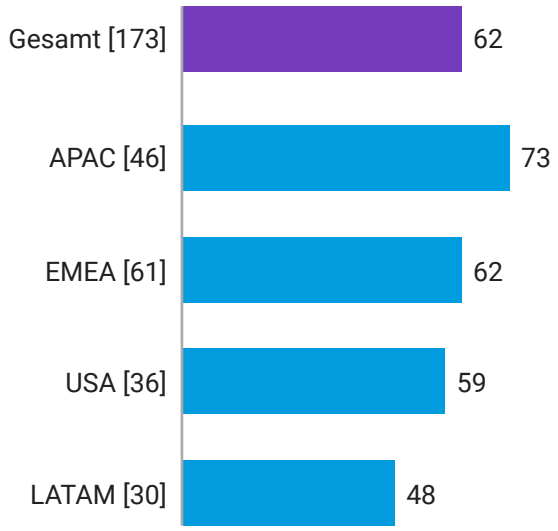


Abb. 1: Wie oft wurde Ihr Unternehmen in den letzten 12 Monaten von Ransomware angegriffen (unabhängig davon, ob die Angriffe erfolgreich waren oder nicht)? Das Diagramm zeigt die durchschnittliche Anzahl von Angriffen in den letzten 12 Monaten, aufgeschlüsselt nach Region (Basiszahlen angegeben), nur Daten des Finanzdienstleistungssektors.

Da die meisten Finanzdienstleister weltweit tätig sind, könnte die gestiegene Zahl gezielter Angriffe in der APAC-Region darauf zurückzuführen sein, dass Hacker sich von APAC-Zielen höhere Erträge versprechen. Dies bedeutet jedoch nicht, dass Finanzdienstleister in anderen Regionen sicherer sind. Es ist lediglich so, dass sie eher Opfer von lateralen Angriffen werden, die ihren Ursprung an anderer Stelle haben.

Darüber hinaus war bei den Befragten in LATAM die Wahrscheinlichkeit am größten, dass ihr Finanzinstitut mehr als zwei Assets segmentiert hat. Am zweithäufigsten war dies in der APAC-Region der Fall. Dies zeigt, dass Finanzinstitute in APAC angesichts der Anzahl der Ransomware-Angriffe, denen sie ausgesetzt sind, möglicherweise versuchen, ihre Segmentierung zu steigern.

Unternehmen im Finanzdienstleistungssektor, die mehr als zwei Assets/Bereiche segmentiert haben, nach Region

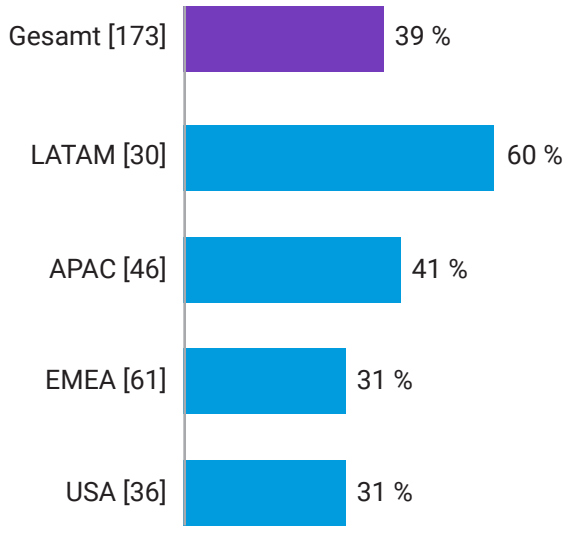


Abb. 2: Welche Assets decken die folgenden IT-Sicherheitsmaßnahmen jeweils ab? Das Diagramm zeigt nur Antworten für die Sicherheitsmaßnahme Segmentierung und Prozentsätze in Bezug auf die Nutzung von Segmentierung zum Schutz wichtiger Assets; aufgeschlüsselt nach Region (Basiszahlen angegeben), nur Daten des Finanzdienstleistungssektors.

Ransomware-Angriffe kamen 2023 im Vergleich zu 2021 weltweit nicht nur häufiger vor, sie waren auch erfolgreicher (Abbildung 3). Die Umfrageteilnehmer gaben an, dass Netzwerkausfälle und Datenverluste zugenommen haben. All dies erhöht den Handlungsdruck für Sicherheitsteams erheblich. Auch der Anteil der Befragten, die höhere Versicherungsprämien meldeten, ist gestiegen, wobei hier der für die USA ermittelte Wert (56 %) besonders zu Buche schlägt. Daran zeigt sich, welchem Risiko Finanzinstitute ausgesetzt sind, die ja häufig nicht nur Daten zu Einzelpersonen, sondern auch zu Unternehmen besitzen.

Die Auswirkungen dieses Drucks sehen wir auch bei der Strategie: Die Zahl der Finanzdienstleister, die Strategien oder Richtlinien zur Cybersicherheit kontinuierlich aktualisieren, ist von 3 % im Jahr 2021 auf 18 % 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.

Auswirkungen von Ransomware/ Cyberangriffen auf Finanzdienstleister

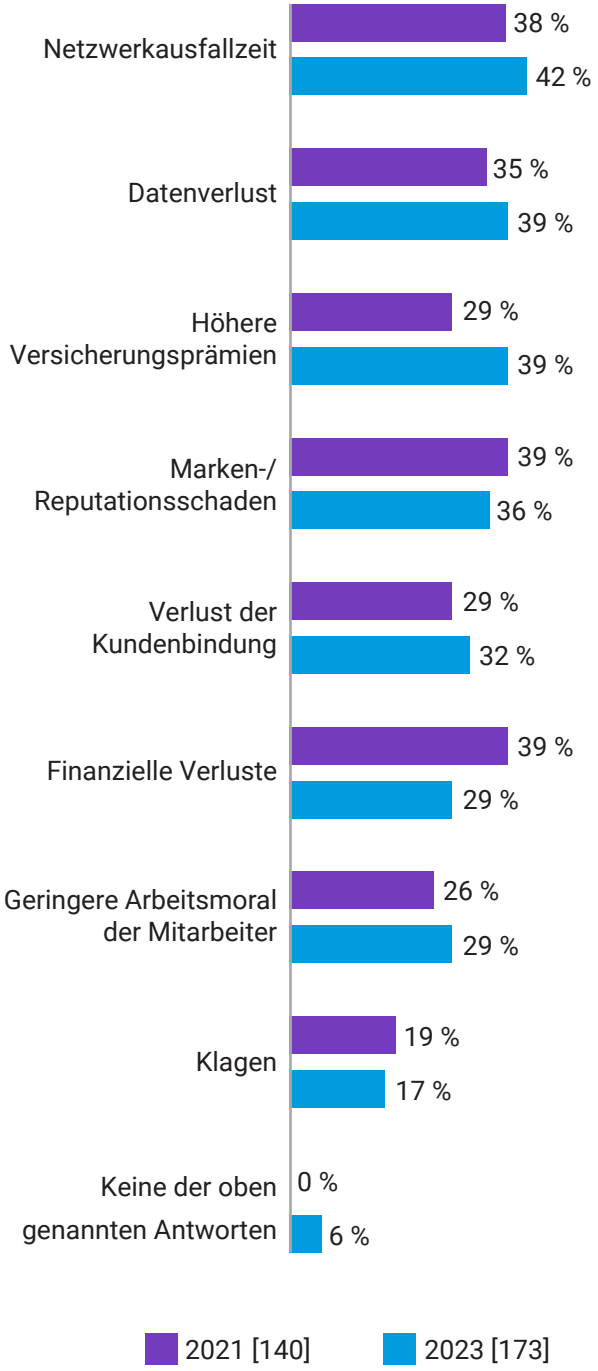


Abb. 3: Welche der folgenden Auswirkungen hatte es für Ihr Unternehmen, wenn es in der Vergangenheit Ransomware oder einen anderen Cyberangriff erkannt hat? Das Diagramm zeigt die Basisgrößen nach Jahr, aufgeschlüsselt nach historischen Daten, nur Daten des Finanzdienstleistungssektors, nicht alle Antwortoptionen sind angegeben.

Segmentierung als Eckpfeiler von Zero Trust

Die Befragten aus dem Finanzdienstleistungssektor sind sich einig, dass Segmentierung wichtig ist, um die Sicherheit des Unternehmens zu gewährleisten, insbesondere bei der Abwehr von Malware: 66 % geben an, dass Segmentierung äußerst wichtig ist, und 92 % sind der Meinung, dass sie ein entscheidender Faktor für die Abwehr schädlicher Angriffe ist.

Segmentierung ist auch ein wesentlicher Bestandteil eines Zero-Trust-Frameworks. Als häufigsten Grund für den Start eines Segmentierungsprojekts nannten die Unternehmen die Entwicklung von Zero Trust: Fast alle befragten Unternehmen, die überhaupt Segmentierungen vorgenommen haben, implementieren ein Zero-Trust-Sicherheitsframework (99 %) oder haben dies bereits getan. Allerdings haben weniger als die Hälfte (47 %) der Befragten ihr Zero-Trust-Framework so weit abgeschlossen und definiert, dass es als ausgereift gelten kann.

Die Mehrheit der befragten Finanzdienstleister möchte diese Entwicklung weiter fördern und Mikrosegmentierung implementieren, um Anwendungs-Workloads auf einer granularen Ebene zu schützen: 88 % geben an, Mikrosegmentierung habe mindestens eine hohe Priorität, und 39 % nennen sie als ihre oberste Priorität. Mit der höchsten Wahrscheinlichkeit sehen die Befragten in LATAM darin die höchste Priorität (50 %), am wenigsten häufig ist dies bei Unternehmen der EMEA-Region der Fall (31 %). Die Tatsache, dass die befragten Unternehmen in LATAM hier eher eine Top-Priorität sehen, spiegelt sich in ihrer Performance wider (Abbildung 1). Es zeigt sich, dass Unternehmen, die eine Mikrosegmentierung priorisieren, davon profitieren können.

Darüber hinaus geben 99 % der IT-Entscheidungsträger in diesem Sektor an, dass zumindest eine Minderheit ihrer Branche Mikrosegmentierung umgesetzt hat und dass es sich um eine Lösung handelt, die zumindest in Grundzügen allen bekannt ist.

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 39 % der Finanzdienstleister haben 2023 mehr als zwei kritische Geschäftsbereiche segmentiert (gegenüber 26 % im Jahr 2021), und 45 % 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: erhöhte Performance-Engpässe (41 %), fehlende Kompetenzen/Fachkenntnisse für die Segmentierung (39 %) und Compliance-Anforderungen (35 %). Zwar sind fehlende Kompetenzen/fehlendes Fachwissen die häufigste Ursache für Verzögerungen bei Segmentierungsprojekten. Zur erwähnen ist aber auch, dass 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.

Bei einer Aufschlüsselung nach Regionen (siehe Abbildung 4) gibt es jedoch Unterschiede in Bezug auf die Hindernisse, die am ehesten zu erwarten sind. Dies zeigt, dass bestimmte Probleme genauso stark, wenn nicht sogar stärker, durch lokale Gegebenheiten (zum Beispiel mangelnde Kompetenzen in den USA, Compliance-Bedenken in APAC) verursacht werden können als durch globale Probleme.

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 17 %, und die Zahl der segmentierten Server stieg ebenfalls um 17 %. Diese Steigerungen übertreffen die durchschnittlichen branchenübergreifenden Steigerungsraten (12 % bzw. 8 %). Darin zeigt sich: Die IT-Abteilungen der Finanzdienstleiser sind eher als die meisten anderen in der Lage, auftauchende Hindernisse zu überwinden. Ein Grund dafür könnte sein, dass die oben angesprochenen strengen Compliance-Anforderungen ein immer höheres Sicherheitsniveau erfordern. Ein weiterer Faktor können die höheren Versicherungsprämien sein, die Finanzdienstleister schultern müssen – Versicherer könnten ihren Kunden besondere Anforderungen auferlegen, damit bestimmte Probleme so schnell wie möglich behoben werden können.

Hindernisse, die bei der Segmentierung von Netzwerken im Finanzdienstleistungssektor aufgetreten sind – die drei wichtigsten Hindernisse nach Region

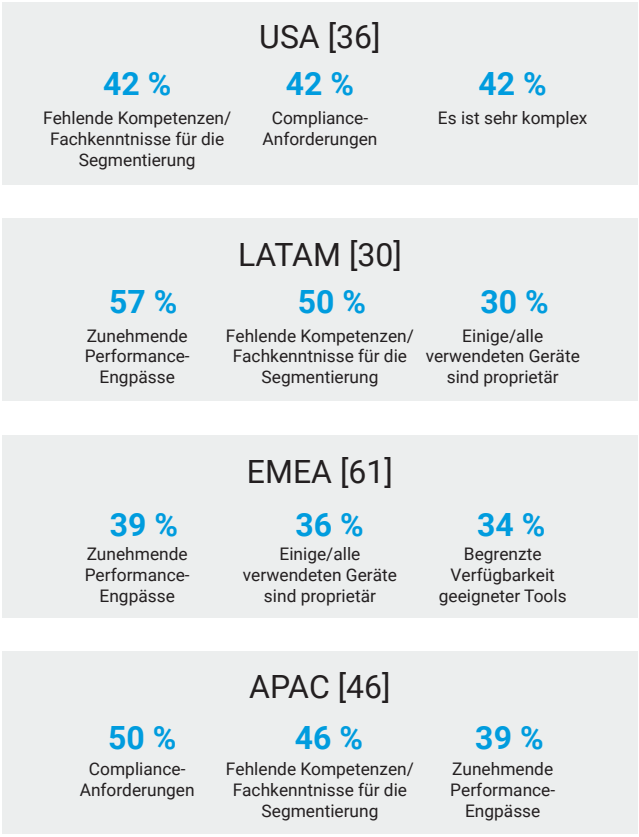


Abb. 4: Mit welchen Problemen war Ihr Unternehmen bei der Segmentierung des Netzwerks konfrontiert bzw. mit welchen Problemen rechnen Sie? Das Diagramm zeigt die Basisgrößen nach Region; die Frage wurde nur denjenigen angezeigt, die ihr Netzwerk zu einem bestimmten Zeitpunkt segmentiert haben; angegeben sind nur die drei am häufigsten gewählten Antworten nach Region; nur Daten des Finanzdienstleistungssektors.

Unternehmen, die sechs kritische Geschäftsbereiche segmentiert haben, haben ihr Risiko erheblich verringert

Der Schutz und die Segmentierung von mehr Assets macht Finanzdienstleister sofort sicherer. Sicherheitsteams sind besser in der Lage, Angriffe zu erkennen und effektiver zu reagieren. Die Implementierung unausgereifter oder schlecht definierter Segmentierungsstrategien erhöht lediglich das Risiko. Eine richtig durchgeführte Segmentierung verbessert dagegen die Cyberresilienz und sorgt dafür, dass Ransomware und Sicherheitsverletzungen nicht auf kritische Systeme und Daten übergreifen können. Dadurch werden aus Cyberangriffen resultierende größere Geschäftsausfälle verhindert.

Unsere Ergebnisse zeigen, dass mit Segmentierung die Wiederherstellung nach einem Angriff 13 Stunden schneller erfolgt.
Eine einfache Rechnung: Bei Finanzdienstleistern, die eine Segmentierung in sechs geschäftskritischen Bereichen implementiert haben, dauert es durchschnittlich drei Stunden, bis ein Ransomware-Angriff vollständig gestoppt ist. Bei Unternehmen mit einer Segmentierung für nur ein Asset dauert dies 16 Stunden.

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

Bedenken Sie, welchen Unterschied diese je nach Szenario zusätzlich benötigten 11–13 Stunden für Ihr Team, den entstehenden Markenschaden und die anfallenden Kosten machen.

Einen Angriff stoppen

3 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: **16 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

Finanzdienstleister sind bestrebt, die Skalierbarkeit zu verbessern, vorhandene Investitionen zu nutzen, Kosten zu optimieren und die Agilität und Flexibilität zu verbessern. Daher migrieren sie Workloads in die Cloud, wobei sie häufig On-Premise-Rechenzentren mit Private oder Public Clouds kombinieren. Softwaredefinierte Segmentierungslösungen wie Akamai Guardicore Segmentation haben sich als flexibler, effizienter und kosteneffektiver Ansatz für die Sicherheit auf Anwendungsebene erwiesen. Dieser Ansatz ermöglicht eine deutlich schnellere Implementierung, eine vereinfachte Wartung und eine effektive Abwehr von Bedrohungen. Er lässt sich schneller und einfacher implementieren als infrastrukturbasierte Ansätze wie Firewalls und VLANs. Dadurch gibt er Finanzdienstleistern die Möglichkeit, umfassende Sicherheitsziele zu erreichen und gleichzeitig die zunehmenden Geschäftsanforderungen zu erfüllen und mit modernsten Technologien innovative Kundenerlebnisse zu bieten. Darüber hinaus funktioniert er nahtlos in verschiedenen Systemen und Umgebungen und bietet zentralisierte Verwaltung und Kontrolle, von Bare-Metal-Servern bis hin zu Multicloud-Bereitstellungen und Legacy-Systemen. Somit bietet der Ansatz eine einheitliche Lösung für die Visualisierung und Steuerung von Verbindungen in der gesamten Umgebung, unabhängig vom physischen Standort.

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.

So vereinfacht Mikrosegmentierung die Compliance

Viele unserer Kunden verwenden unsere Lösung, um die Einhaltung verschiedener Compliance-Anforderungen wie PCI-DSS, SWIFT, Sarbanes-Oxley, DSGVO und DORA zu gewährleisten und nachzuweisen. Diese gesetzlichen 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

Segmentierung kann komplex sein. Wie dieser Bericht jedoch zeigt, erzielen Unternehmen, die Segmentierung erfolgreich implementieren, Verbesserungen in den Bereichen Netzwerksicherheit, Netzwerk-Performance und Compliance. Außerdem vereinfachen sie die Verwaltung ihrer Netzwerke. 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.

Erkenntnisse nach Regionen

Segmentierung und Mikrosegmentierung sind in EMEA und den USA wichtiger als in LATAM: Dass die Netzwerksegmentierung äußerst wichtig ist, um die Sicherheit des Unternehmens sicherzustellen, sagen mehr IT-Sicherheitsverantwortliche in EMEA (70 %) und den USA (60 %) als in LATAM (57 %).

50 % der befragten Unternehmen in LATAM nannten Mikrosegmentierung als oberste Priorität, mehr als die Befragten in den USA (42 %), APAC (41 %) und EMEA (31 %).

Die Wahrscheinlichkeit, dass gar keine Segmentierungen durchgeführt wurden, ist in EMEA-Ländern höher: Die Befragten in der EMEA-Region geben eher an, dass keine geschäftskritischen Assets segmentiert wurden (7 %) – in allen anderen Regionen war jeweils zumindest ein gewisser Segmentierungsgrad vorhanden.

Am ehesten haben Unternehmen aus LATAM bei der Segmentierung die größten Fortschritte gemacht: Der Anteil der Finanzdienstleister, die mehr als zwei geschäftskritische Assets segmentiert haben, ist in LATAM (60 %) höher als in APAC (41 %), EMEA (31 %) und den USA (31 %).

Unternehmen in allen Regionen stehen vor Herausforderungen: 98 % der befragten Unternehmen in APAC gaben an, dass sie Probleme bei der Segmentierung ihres Netzwerks haben. Ähnlich hoch war der Wert für die USA (97 %). In EMEA (89 %) und LATAM (87 %) war der Anteil etwas geringer.

Finanzdienstleister in LATAM weisen bei der Implementierung des Zero-Trust-Sicherheitsframeworks einen deutlich höheren Reifegrad auf: In LATAM erklärt ein größerer Anteil der Unternehmen, die Zero-Trust-Implementierung vollständig abgeschlossen und definiert zu haben (57 %), als in EMEA (48 %), den USA (47 %) und APAC (41 %).

Die Umfrageteilnehmer

Für die vollständige Studie haben wird 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.

Die Umfrage berücksichtigte Unternehmen aus den USA, Indien, Mexiko, Brasilien, Großbritannien, Frankreich, Deutschland, China, Japan und Australien. Die befragten Personen arbeiteten für Unternehmen mit mehr als 1.000 Mitarbeitern und repräsentierten unterschiedliche Branchen und Sektoren.

Für die Zwecke dieses Berichts haben wir die Antworten von 173 (2023) bzw. 140 (2021) befragten Unternehmen aus dem Finanzdienstleistungssektor ausgewertet.

Weitere Informationen zu Akamai Guardicore Segmentation

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. 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 Lösungen von Akamai für die Finanzdienstleistungsbranche erfahren? Dann besuchen Sie uns unter akamai.com/finserv und akamai.com/blog, oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn. Veröffentlicht: 05/24.

VansonBourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Das Unternehmen 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.