Akamai

E-BOOK

Der Zustand der Segmentierung

Das Überwinden von Bereitstellungshindernissen erweist sich als Vorteil

E-Commerce-Branche

Inhaltsverzeichnis

Einführung

IT-Sicherheitsteams – insbesondere diejenigen, die für die Sicherheit von E-Commerce-Unternehmen zuständig sind – hatten es noch nie leicht. Traditionell haben engere Budgets und begrenzte Sicherheitsressourcen dazu geführt, dass diejenigen, die für den Unternehmensschutz zuständig sind, mit weniger mehr erreichen müssen. Heute jedoch setzen hoch motivierte und hoch entwickelte Angreifer die Sicherheitsteams, die auch noch mit der Verwaltung einer immer komplexeren Infrastruktur zu kämpfen haben, stärker unter Druck, die Risiken zu minimieren, als je zuvor. E-Commerce-Unternehmen sind abhängig von einer leistungsfähigen Online-Präsenz, sodass ein erfolgreicher „Einbruch“ – wie ein Ransomware-Angriff – erhebliche, wenn nicht gar irreparable Schäden an Markenimage und Umsatz verursachen kann. Stellen Sie sich die schädlichen Auswirkungen vor, wenn der Online-Betrieb, die Auftragsabwicklung oder die Produktionslinien zum Stillstand kämen, da kritische Server und Systeme aufgrund einer Massenverschlüsselung – und möglicherweise doppelter Erpressung durch Datenextraktion – nicht mehr verfügbar wären.

Wie die Ergebnisse in diesem Bericht „Zustand der Segmentierung im E-Commerce“ zeigen, haben diese Angriffe inzwischen auch größere Auswirkungen. Führungskräfte müssen die richtigen Tools und Lösungen auswählen, die dazu beitragen, wichtige Daten sicher aufzubewahren, ohne die Performance zu beeinträchtigen oder den betrieblichen Aufwand zu erhöhen. Dem Bericht zufolge ist der E-Commerce der am häufigsten betroffene Industriezweig unter allen Befragten. Dies unterstreicht die Dringlichkeit, Ransomware-Angriffe zu verhindern, zu erkennen und so schnell wie möglich darauf zu reagieren, um die Auswirkungen einzudämmen.

Die Befragten in E-Commerce-Unternehmen (aus allen Regionen, einschließlich USA, LATAM, EMEA und APAC) sind sich mit überwältigender Mehrheit einig, dass Segmentierung Assets effektiv schützt. Der Fortschritt bei ihrer Umsetzung für kritische Geschäftsanwendungen und Assets ist unter den Teilnehmern jedoch geringer als erwartet. Die größten Hindernisse für E-Commerce-Unternehmen waren der Mangel an Fachwissen bei der effektiven Implementierung von Segmentierung in Verbindung mit aufwendigen Compliance-Anforderungen. Dies zeigt, dass Teams nicht nur Schwierigkeiten haben, die erforderlichen Talente für ihre Branche zu rekrutieren oder zu binden, sondern auch wertvolle Zeit damit verbringen, die Einhaltung von Rechtsvorschriften sicherzustellen, und damit bereits strapazierte Ressourcen weiter belasten.

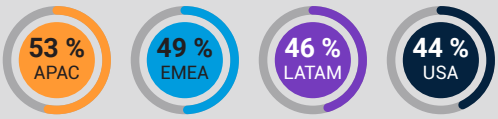
Die gute Nachricht: Durchhaltevermögen – und die Wahl der richtigen Lösung – zahlt sich aus. Für diejenigen, die die meisten ihrer kritischen Assets erfolgreich über sechs Schlüsselbereiche hinweg segmentiert hatten, erwies sich die Segmentierung als überaus effektive Abwehrlösung. So konnten die Verantwortlichen 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 nicht nur für Ihr Krisenteam, sondern auch für Ihre Kunden und den Ruf Ihrer Marke machen können.

Die Segmentierung hat sich insgesamt langsam entwickelt, aber diejenigen mit Durchhaltevermögen haben ihr Risiko enorm reduziert

Segmentierung ist gut. Mikrosegmentierung ist besser.

Segmentierung ist ein architektonischer Ansatz, bei dem ein Netzwerk in kleinere Segmente unterteilt wird, um die Sicherheit zu verbessern und die Risiken im Zusammenhang mit flachen Netzwerken zu verringern. Sie wird zudem eingesetzt, um den Umfang, die Kosten und die Schwierigkeiten bei der Erreichung und Aufrechterhaltung der PCI-Compliance für E-Commerce-Unternehmen zu reduzieren.

Mikrosegmentierung ist eine softwaredefinierte Sicherheitstechnik, bei der ein Netzwerk logisch in verschiedene Sicherheitssegmente unterteilt wird, bis hin zur individuellen Workload- oder Prozessebene (Layer 7). Im Vergleich zu herkömmlichen Segmentierungsmethoden wie VLANs, ACLs und internen Firewalls, die nur Layer-4-Kontrolle bieten, können dann Sicherheitskontrollen und Servicebereitstellung für jedes einzelne Segment auf einer detaillierteren Ebene definiert werden. Aus diesem Grund bevorzugen 94 % der Befragten im E-Commerce softwarebasierte Segmentierungslösungen gegenüber herkömmlichen Methoden.



Sicherheitsentscheider in den APAC-Ländern gaben eher an, dass die Netzwerksegmentierung äußerst wichtig ist, um die Sicherheit ihres Unternehmens zu gewährleisten, als in EMEA, LATAM oder den USA. Die Befragten der LATAM-Regionen waren eher der Meinung, dass die Mikrosegmentierung oberste Priorität hat (42 %), als die in APAC (35 %), den USA (34 %) und EMEA (26 %).

E-Commerce ist die am häufigsten betroffene Branche, und Ransomware-Angriffe nehmen weiter zu

Die Anzahl der Ransomware-Angriffe in E-Commerce-Organisationen (mit und ohne Erfolg) lag in den letzten 12 Monaten durchschnittlich bei 167. Damit steht der E-Commerce nicht nur bei der Anzahl der durchschnittlichen Ransomware-Angriffe ganz oben auf der Liste, sondern weist auch etwa doppelt so viele Angriffe auf wie der nächstfolgende Sektor (89 Angriffe im Durchschnitt).

In den USA ist die Wahrscheinlichkeit von Cyberangriffen auf E-Commerce-Unternehmen höher: Die Zahl der Ransomware-Angriffe in den USA ist mit durchschnittlich 312 Angriffen in den letzten 12 Monaten die höchste in allen Regionen, verglichen mit 119 in APAC, 91 in EMEA und 68 in LATAM (Abbildung 1).

Durchschnittliche Anzahl der Ransomware-Angriffe in E-Commerce-Organisationen in den letzten 12 Monaten nach Regionen

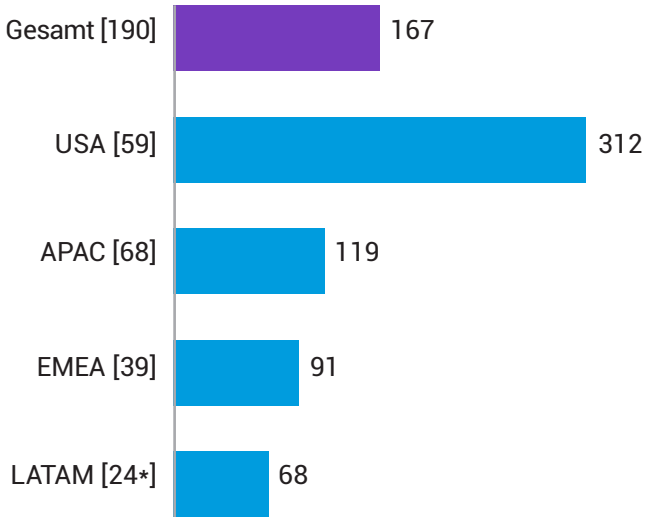


Abb. 1: Wie viele Ransomware-Angriffe gab es in den letzten 12 Monaten auf Ihr Unternehmen (unabhängig davon, ob die Angriffe erfolgreich waren oder nicht)? Das Diagramm zeigt die durchschnittliche Anzahl von Angriffen in den letzten 12 Monaten, aufgeschlüsselt nach Region; nur Daten aus E-Commerce-Branche.

* Vorsicht – niedrige Basisgröße unter 30

Obwohl die Durchschnittswerte in den Regionen außerhalb der USA nicht als niedrig bezeichnet werden können, werden sie doch von der Zahl der Angriffe, die sich auf die USA konzentrieren, in den Schatten gestellt. Als größte Volkswirtschaft der Welt sind die USA das Hauptzielland von Ransomware-Banden, und die Angreifer haben es häufig auch auf andere englischsprachige und westliche Länder abgesehen. Geopolitische Motive spielen ebenfalls eine Rolle dabei, welche Länder und Sektoren am stärksten betroffen sind. E-Commerce-Unternehmen werden häufig ins Fadenkreuz genommen, da sie im Vergleich zu anderen Branchen wie Finanzdienstleistungen traditionell über weniger ausgereifte Sicherheitsstrategien verfügen, was sie zu einem leichten Ziel macht. Erschwerend kommt hinzu, dass ein erfolgreicher Ransomware-Angriff ein hohes Maß an Öffentlichkeit erzeugen kann, vor allem, wenn Unternehmen in Zeiten getroffen werden, in denen wichtige Einnahmen generiert werden, wie z. B. an Feiertagen, Festivals, Sportveranstaltungen, zum Schulanfang oder während anderer großer Shopping-Events: eine Unterbrechung des Betriebs erhöht die Wahrscheinlichkeit einer Auszahlung – aus Sicht des Angreifers.

Trotz der hohen Anzahl von Ransomware-Angriffen, die auf E-Commerce-Unternehmen abzielen, ist der Umfang der durchgeführten Segmentierung enttäuschend. Nur 11 % dieser Unternehmen haben mehr als zwei Bereiche segmentiert, eine Zahl, die für alle Regionen weitgehend gleich ist. Dies deutet darauf hin, dass viele dieser Unternehmen nicht über die Ressourcen verfügen, die für die Bewältigung von Problemen und Angriffen erforderlich wären.

Ransomware-Angriffe im E-Commerce-Sektor können enorme und unmittelbare Auswirkungen auf das Unternehmen haben (Abbildung 2). Unsere Umfrageteilnehmer gaben finanzielle Verluste und Reputationsschäden an. Beides erhöht den Handlungsdruck für Sicherheitsteams in E-Commerce-Unternehmen erheblich.
Auch der Anteil der Befragten, der höhere Versicherungsprämien meldete, ist gestiegen. Dies zeigt, wie hoch das Risiko ist, das E-Commerce-Unternehmen eingehen können, da sie häufig personenbezogene Daten über Einzelpersonen und ihre Einkaufsgewohnheiten speichern, zusätzlich zu den Risiken im Zusammenhang mit logistischen Problemen mit Beständen oder Lagerhaltung.

Die Auswirkungen können je nach Region variieren: Die Befragten aus der APAC-Region geben besonders häufig finanzielle Verluste an (51 %), verglichen mit dem Gesamtdurchschnitt von 42 %. Von den Befragten in den USA melden fast die Hälfte (49 %) Netzwerkausfälle, im Vergleich zu einem Gesamtdurchschnitt von 39 %. Die Befragten in der EU geben eher eine geringere Arbeitsmoral der Arbeitnehmer an (41 % gegenüber insgesamt 36 %).

Die Auswirkungen dieses Drucks sehen wir auch bei der Strategie: Die Zahl der E-Commerce-Unternehmen, die Strategien oder Richtlinien zur Cybersicherheit kontinuierlich aktualisieren, ist von 3 % im Jahr 2021 auf 13 % im Jahr 2023 gestiegen. Dies geschah nicht nur als Antwort auf Ransomware, sondern generell als Reaktion auf die ständige Veränderung der Angriffsfläche. Die zunehmende Komplexität der Infrastruktur bei der Migration von Workloads in die Cloud ist nur einer der Risikofaktoren, die sich täglich auf Sicherheitsstrategien und Sicherheitsteams auswirken.

Auswirkungen von Ransomware/ Cyberangriffen auf E-Commerce-Unternehmen

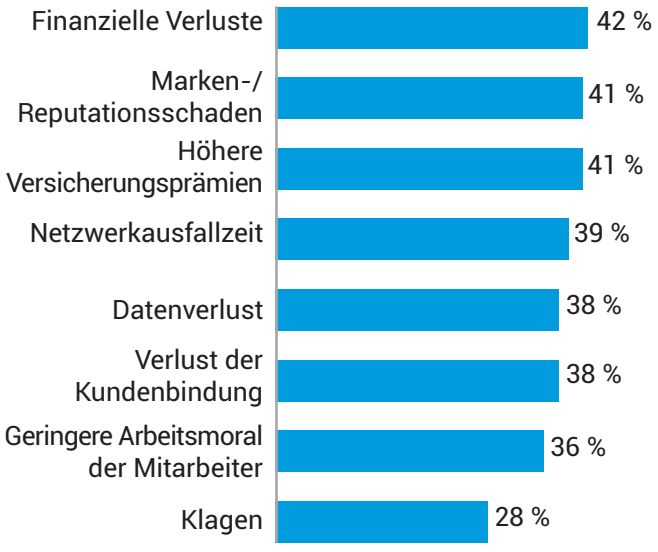


Abb. 2: Welche der folgenden Auswirkungen hatte es für Ihr Unternehmen, wenn es in der Vergangenheit Ransomware oder einen anderen Cyberangriff erkannt hat? Das Diagramm zeigt nicht alle Antwortoptionen, sondern nur Daten des E-Commerce-Sektors.

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.

Fast die Hälfte (48 %) gibt an, dass Segmentierung äußerst wichtig ist, und 89 % glauben, dass sie ein entscheidender Faktor für die Abwehr schädlicher Angriffe ist.

Die Segmentierung gilt auch als Eckpfeiler eines Zero-Trust-Sicherheitsframeworks, und die gute Nachricht für E-Commerce-Organisationen ist, dass in diesem Bereich bereits Fortschritte erzielt wurden. Alle sind dabei, ein Zero-Trust-Sicherheitsframework zu implementieren, oder haben bereits ein Zero-Trust-Framework (100 %) implementiert. Allerdings haben nur zwei von fünf (42 %) der befragten Unternehmen das Zero-Trust-Framework vollständig definiert und abgeschlossen. Dies ist daher ein Bereich, in dem Segmentierung E-Commerce-Unternehmen auf ihrem Weg zu Zero Trust unterstützen kann. Den Daten zufolge sind Unternehmen in den USA weitaus besser aufgestellt, wenn es um die Bereitstellung ihres Zero-Trust-Frameworks geht: Sie sagen mit weitaus größerer Wahrscheinlichkeit, dass die Zero-Trust-Implementierung vollständig abgeschlossen und definiert ist (63 %), im Vergleich zu LATAM (46 %), APAC (32 %) und EMEA (23 %).

Die Gründe für den Start von Projekten zur Netzwerksegmentierung waren von Region zu Region unterschiedlich, wobei von staatlichen Stellen geförderte Umsetzungen einer Cybersicherheitsstrategie mit 41 % an erster Stelle steht. Sowohl LATAM- als auch die EU-Länder nannten öffentlichkeitswirksame Zero-Day-Schwachstellen als Hauptgrund für die Durchführung einer Segmentierungsinitiative (44 % bzw. 42 %). Die Befragten in der EU geben an, dass Projekte gestartet wurden, weil es sich um Best Practices handelt (41 %, verglichen mit dem Gesamtdurchschnitt von 22 %). Die Befragten in den USA und den APJ-Ländern sagen jedoch eher, dass sie aufgrund der Konzentration ihrer Regierung auf Cybersicherheit begonnen haben (41 % bzw. 39 %, verglichen mit dem Gesamtdurchschnitt von 35 %). Befragte aus dem APJ-Raum geben zudem eher an, dass die Verlagerung kritischer Anwendungen in die Cloud dazu geführt hat, dass sie ein Projekt gestartet haben (39 %, verglichen mit dem Gesamtdurchschnitt von 32 %).

Die Mehrheit der befragten E-Commerce-Unternehmen strebt an, weiterzugehen und Mikrosegmentierung zu implementieren, um Anwendungs-Workloads auf einer granularen Ebene zu schützen: 92 % geben an, Mikrosegmentierung habe mindestens eine hohe Priorität, und 34 % nennen sie als ihre oberste Priorität. Darüber hinaus berichten alle (100 %) Entscheidungsträger in den Bereichen IT und Sicherheit in diesem Sektor, dass sie von mindestens einer Minderheit ihrer Branche angenommen wurde, und betonen, dass es sich um eine Lösung handelt, die zumindest in Grundzügen allen bekannt ist, auch wenn die Fortschritte bisher begrenzt sind.

Die Befragten weisen auch darauf hin, dass eine größere Transparenz der IT-Umgebung des Unternehmens erforderlich ist. Laut LATAM sei „viel mehr“ Transparenz (63 %) erforderlich – gefolgt von APAC (56 %), den USA (46 %) und EMEA (44 %) – in Bezug auf Netzwerkkommunikation, Asset-Standorte usw., um Risiken zu reduzieren.

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 durch den Schutz von IT-Ressourcen ist. Die ernüchternde Realität ist jedoch, dass die Implementierung von Segmentierungen nur langsam vorankommt – langsamer als vielleicht erwartet.

Nur 11 % der E-Commerce-Unternehmen haben mehr als zwei kritische Geschäftsbereiche segmentiert, und 48 % haben vor zwei oder mehr Jahren ein Netzwerksegmentierungsprojekt gestartet, was darauf hindeutet, dass die Bemühungen zum Stillstand gekommen sind.

Die unternehmenskritischen Bereiche

- Kritische Anwendungen
- Öffentlich zugängliche Anwendungen
- Domaincontroller
- Endpunkte
- Server
- Geschäftskritische Assets/Daten

Langsame Implementierungen lassen sich am überzeugendsten durch die wesentlichen Hindernisse erklären, mit denen die Befragten konfrontiert sind: Mangel an Kompetenzen/Fachwissen für die Segmentierung (40 %), Compliance-Anforderungen (40 %) und zunehmende Performance-Engpässe (38 %) – allesamt verbunden mit traditionellen Segmentierungsmethoden. Erwähnenswert ist, dass fehlende Kompetenzen/Fachwissen häufigste Ursachen für Verzögerungen bei Segmentierungsprojekten sind, 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.

E-Commerce-Unternehmen in allen Regionen stehen vor Herausforderungen: 100 % der Befragten in den USA und der LATAM-Region geben an, dass sie Probleme bei der Segmentierung ihres Netzwerks haben. Fast genauso viele äußern das Gleiche in APAC (99 %) und in EMEA (97 %).

Bei einer Aufschlüsselung nach Regionen (Abbildung 3) gibt es jedoch Unterschiede in Bezug auf die Hindernisse, die am wahrscheinlichsten auftreten. Dies zeigt, dass bestimmte Probleme (z. B. Mangel an Fachkenntnissen, Compliance) genauso stark oder stärker von lokalen Problemen als von globalen Problemen verursacht werden können.

Die EMEA- und LATAM-Länder nennen fehlende Kompetenzen/Fachkenntnisse (jeweils 54 %) als größte Herausforderung für die Segmentierung. Die größte Herausforderung in den USA stellen erhöhte Performance-Engpässe dar (44 %), und in der APAC-Region sind die Compliance-Anforderungen (43 %) das häufigste Problem.

	Häufigstes Problem	Zweit- und dritthäufigstes Problem	
USA [59]	Zunehmende Performance-Engpässe (44 %)	Compliance-Anforderungen / Begrenzte Verfügbarkeit geeigneter Tools (beide 41 %)	
LATAM [24*]	Fehlende Kompetenzen/Fachkenntnisse für die Segmentierung (54 %)	Hohe Komplexität (46 %)	Einige/alle verwendeten Geräte sind proprietär / Einige/alle verwendeten Geräte sind veraltet (beide 38 %)
EMEA [39]	Fehlende Kompetenzen/Fachkenntnisse für die Segmentierung (54 %)	Begrenzte Verfügbarkeit geeigneter Tools (41 %)	Compliance-Anforderungen / Einige/alle verwendeten Geräte sind veraltet / Es ist sehr teuer (alle 36 %)
APAC [67]	Compliance-Anforderungen (43 %)	Begrenzte Verfügbarkeit geeigneter Tools / Einige/alle verwendeten Geräte sind proprietär / Zunehmende Performance-Engpässe (alle 37 %)	

Abb. 3: Mit welchen Problemen war Ihr Unternehmen bei der Segmentierung des Netzwerks konfrontiert, bzw. mit welchen Problemen rechnen Sie? Das Diagramm zeigt die Teilnehmer, die ihr Netzwerk zu einem bestimmten Zeitpunkt segmentiert haben, die drei wichtigsten Antworten nach Region und nur Daten der E-Commerce-Branche.

* Vorsicht – niedrige Basisgröße unter 30

Wichtige Erkenntnisse: Unternehmen, die sechs kritische Geschäftsbereiche segmentiert haben, haben Risiken erheblich verringert

Der Schutz und die Segmentierung von mehr Assets in der gesamten E-Commerce-Umgebung machen das Unternehmen sofort sicherer. Mit der richtigen Lösung sind Sicherheitsteams in der Lage, Angriffe schneller zu erkennen und so die mittlere Erkennungszeit (Mean Time to Detect, MTTD) und die mittlere Reaktionszeit (Mean Time to Respond, MTTR) auf einen Vorfall zu verbessern. Allerdings kann eine unzureichende Segmentierung von Assets – in der Regel als Folge der Verwendung älterer Segmentierungstechnologien – zu Sicherheitslücken und Schwachstellen führen und das Unternehmen in eine anfälligere oder reaktivere Position bringen. Doch wenn sie richtig durchgeführt wird, kann die Segmentierung über einen softwaredefinierten Ansatz Unternehmen dabei unterstützen, Angriffsflächen besser zu kontrollieren, um kritische Assets effizienter und kostengünstiger zu schützen.

Unsere Ergebnisse zeigen, dass mit Segmentierung die Wiederherstellung nach einem Angriff 11 Stunden schneller erfolgt. Eine einfache Rechnung: Bei E-Commerce-Unternehmen, 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 14 Stunden.

Mit Segmentierung beschleunigt sich auch die Eindämmung lateraler Netzwerkbewegungen um 11 Stunden. Für diejenigen, die Segmentierungen über alle sechs unternehmenskritischen 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.

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

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: **14 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 deren 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 für die Durchsetzung von Richtlinien nicht auf das zugrunde liegende Betriebssystem angewiesen ist, 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 und Windows XP bis hin zu den neuesten POS-Systemen, 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

Akamai Guardicore Segmentation 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, sondern vielmehr durch Personalengpässe. Der Zeit- und Arbeitsaufwand, der für die manuelle Segmentierung von Geschäftsbereichen und die manuelle Fehlerbehebung in diesen Bereichen aufgewendet werden muss, kann enorm sein. 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 Kennzeichnungs- und 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 Segmentierung zur Optimierung der Compliance beiträgt

Viele unserer Kunden verwenden unsere Lösung, um die Einhaltung verschiedener länderspezifischer und internationaler Compliance-Auflagen wie PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, DSGVO zu gewährleisten und nachzuweisen. Diese Compliance-Anforderungen erfordern in der Regel, dass Daten, die Gegenstand des Geltungsbereichs sind – wie die Karteninhaberdatenumgebung (Customer Data Environment, CDE) für PCI-DSS – von anderen Systemen in Ihrer Umgebung getrennt und geschützt 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, Systeme 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 und ermöglicht Krisenteams, bei einem akuten Angriff schneller zu reagieren. Außerdem sind nach einem Angriff die Wiederherstellungsmaßnahmen gesichert und benötigen weniger Zeit.

Wenn Sie sich für eine softwaredefinierte Lösung entscheiden, die darauf ausgelegt ist, die mit einer herkömmlichen Segmentierungsimplementierung verbundenen Herausforderungen zu überwinden, 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.

Die Umfrageteilnehmer

Für die Zwecke dieses Berichts haben wir 190 Befragte in der E-Commerce-Branche analysiert (59 in den USA, 39 in EMEA, 68 in APAC und 24 in LATAM).

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 IT-Sicherheitsansätzen, zu 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 Befragten stammen aus der ganzen Welt, darunter aus den USA, Indien, Mexiko, Brasilien, Großbritannien, Frankreich, Deutschland, China, 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. Beispielgrößen: 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 Mitarbeiter, 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, 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 Cloud-Computing-, Sicherheits- 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: 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.