Akamai | TechnologyAdvice

Mikrosegmentierung bringt Zero Trust im Handelssektor voran

Handelsunternehmen in den Bereichen Einzelhandel, Reise und Gastgewerbe sind attraktive Ziele für Cyberkriminelle, Ransomware-Banden und Betrüger, die sensible Unternehmens- oder Finanzdaten zu Geld machen wollen. Laut dem RH-ISAC Industry Insights Report sind Kreditkarten- und Zahlungsinformationen, personenbezogene Daten (PII) aus Prämien- oder Treueprogrammen sowie geistiges Eigentum die Arten von Informationen, auf die es Datendiebe besonders häufig abgesehen haben.

Die im Visier möglicher Angreifer stehenden Unternehmen und ihre Sicherheitsteams müssen sich mit viele potenziellen Eindringpunkten befassen, über die Cyberkriminelle in das Netzwerk gelangen und Ransomware oder andere Arten von Malware einschleusen können. Alle Unternehmen sind mit den Auswirkungen von Phishing-E-Mails, gestohlenen VPN-Anmeldedaten und Zero-Day-Exploits konfrontiert. Viele Handelsunternehmen müssen aber noch mit zusätzlichen Risiken umgehen, die durch Kiosks, IoT-Geräte, In-Store-Tablets, POS-Terminals, Gast-WLAN und vieles mehr entstehen. Was die Sache noch komplexer macht: Mit jedem Einzelhandelsstandort, der zur Abwicklung von Geschäften öffentlich zugänglich ist, bietet ein Unternehmen Angriffsfläche für physische Attacken und eine ganz Reihe weiterer Bedrohungen.

Je wertvoller die Daten und je größer die Zahl der Angriffsvektoren, desto wichtiger ist es auch, dass Sicherheitsverantwortliche in Unternehmen menschliche Fehler als die Hauptursache für Sicherheitsprobleme kompensieren: Menschliches Versagen ist für 82 % der Sicherheitsvorfälle verantwortlich. Die zunehmende regulatorische Kontrolle durch die Payment Card Industry (PCI) oder gesetzliche Vorschriften (DSGVO, SEC usw.) erhöht den Druck und zehrt an den ohnehin schon angespannten IT-Sicherheitsbudgets und -Ressourcen.

Es ist unmöglich, alle Risiken zu eliminieren. Handelsunternehmen müssen heutzutage davon ausgehen, dass es zu Angriffen kommt, um die Ausbreitung einer unvermeidlichen Infektion oder eine Umgehung des Netzwerkschutzes schnell zu erkennen und zu stoppen. Mit Zero-Trust-Segmentierungslösungen von Akamai können Handelsunternehmen ihre Anwendungen, Server und Netzwerkumgebungen einfacher und schneller schützen und sowohl die schädliche Verschlüsselung als auch die Extraktion vertraulicher Daten verhindern.

Mikrosegmentierung funktioniert am besten auf Basis eines softwaredefinierten Ansatzes und erfüllt als ein Eckpfeiler für Zero-Trust-Sicherheitsframeworks drei wichtige Anforderungen von Handelsunternehmen. Erstens begrenzt Mikrosegmentierung auf natürliche Weise die möglichen Auswirkungen einer Ransomware-Infektion, indem sie die laterale Bewegung blockiert. Zweitens kann sie dazu beitragen, die Kosten für die Erfüllung und Aufrechterhaltung der PCI-Compliance zu senken. Drittens ermöglicht Mikrosegmentierung die erforderlichen detaillierten Einblicke und die benötigte Abdeckung, um moderne und dabei komplexere Ökosysteme in Hybrid-, Multicloud- und Microservices-Umgebungen sowie in Legacy-Infrastrukturen zu schützen.

Begrenzen Sie potenzielle Auswirkungen von Ransomware

Ein Klick auf einen Phishing-Link in einer E-Mail, fehlerhafte Sicherheitskonfigurationen, offene RDP-Ports oder kompromittierte Anmeldeinformationen: All das sind immer wieder Einfallstore für Angreifer, die auf der Suche nach den Kronjuwelen Ihres Unternehmens das Netzwerk erkunden, um die Ausführung eines Ransomware-Angriffs vorzubereiten. Unternehmen, die Opfer eines erfolgreichen Massenverschlüsselungsereignisses sind und im Falle von Datenextraktion möglicherweise doppelt erpresst werden, erleiden finanzielle Verluste und Geschäftsschaden auf mehreren Ebenen.

Direkte Geschäftsverluste können sofort auftreten, wenn Online-Bestellungen und Filialgeschäfte stocken oder zum Stillstand kommen, wenn Kunden keine Artikel kaufen oder keine Hotels oder Flüge buchen können. E-Commerce-Unternehmen können bestehende Bestellungen möglicherweise nicht verarbeiten, erfüllen oder versenden, da kritische Systeme und Server nicht mehr zugänglich sind oder zur Begrenzung eines Angriffs offline geschaltet werden.

Wenn sensible Unternehmens- oder Kundendaten kompromittiert werden, entstehen durch die unangenehme Publicity und Rufschädigung bereits **indirekte Geschäftsverluste**. Es ist eine bei Ransomware-Banden beliebte Taktik, Angriffe und Datenlecks auf „Pranger"-Websites publik zu machen, um den erpresserischen Druck auf die Opfer zu erhöhen und Lösegeldzahlungen zu erzwingen. Neue SEC-Auflagen verlangen von Unternehmen außerdem, die SEC innerhalb von vier Tagen über wesentliche Auswirkungen auf das Unternehmen zu informieren, was für zusätzliche Schlagzeilen sorgt und den Reputationsschaden verstärkt.

Der nach einem erfolgreichen Ransomware-Angriff durch Rechtskosten, Vorfallsreaktion, Datenforensik und Behebungsmaßnahmen entstehende **finanzielle Folgeaufwand** ist hoch, und Consultants und IT-Teams müssen sich um die Wiederherstellung von Daten und Backups kümmern und die Systeme wieder online verfügbar machen. Diese Kosten sind schon hoch genug, doch sie könnten durch Prozesskosten oder regulatorische Strafen und Geldbußen, die aufgrund des Verlusts sensibler Daten fällig werden, noch übertroffen werden. Die Prämien für Cyberversicherungen können drastisch steigen, Versicherungen können Zahlungen im Ransomware-Schadensfall verweigern, oder der Versicherungsschutz erlischt ganz.

Es steht viel auf dem Spiel, und es überrascht nicht, dass Ransomware-Angriffe von CISOs als das größte Risiko für Einzelhandel und Gastgewerbe im Jahr 2024 genannt wurden. Sicherheitsverantwortliche sind bereit, in Kontrollen zu investieren, die das Risiko für den Fall, dass Angreifer Zugriff auf Systeme erlangen, verringern. Damit Ransomware sich verbreiten kann, müssen Angreifer jedoch in der Lage sein, die Richtung zu ändern und sich lateral zu bewegen, nachdem sie den ersten Zugriff erhalten haben. Erst dann können die Angriffe maximale Wirkung zu entfalten. Laut dem Microsoft Digital Defense Report 2022 sind 93 % der Ransomware-Vorfälle auf unzureichende Kontrollen der lateralen Netzwerkbewegungen zurückzuführen. Sie ermöglichen es Cyberkriminellen, kritische Anwendungen und Infrastrukturen zu sperren. Die Zeit, in der ein Angreifer dann von einem Endpoint innerhalb des Unternehmensnetzwerks aus eine laterale Bewegung beginnt, beträgt im Mittel nur eine Stunde und 42 Minuten.

Aus jüngst von Akamai veröffentlichten Daten zum Zustand der Segmentierung geht hervor, dass E-Commerce-Organisationen in den letzten 12 Monaten im Vergleich zu anderen Branchen die höchste Anzahl an Ransomware-Angriffen gemeldet haben. Aus diesem Grund wenden sich CISOs und Sicherheitsexperten auf Zero Trust basierenden Sicherheitstools wie Mikrosegmentierung zu. Damit wollen sie das Risiko einer erfolgreichen Ransomware-Infektion reduzieren, Angriffsflächen minimieren und die Ransomware-Kill-Chain „durchbrechen“.

Werden die über laterale Bewegung erfolgenden Erkundungsaktivitäten erkannt und blockiert, wird es für die Angreifer schwer, auf die IT-Ressourcen zuzugreifen, die für die Eskalation von Berechtigungen, das Auffinden vertraulicher Daten und die Ausbreitung großangelegter Ransomware-Angriffe erforderlich sind. Durch die Anwendung des Prinzips der geringstmöglichen Zugriffsrechte auf kritische Workloads in der gesamten Handelsinfrastruktur ermöglicht die von Analysten als führend anerkannte Mikrosegmentierungslösung von Akamai umfassende Einblicke in Ost-West-Datenflüsse von Anwendungen und Workloads. Die Lösung bietet darüber hinaus fein abgestuften Schutz durch softwaredefinierte Richtlinien, um die laterale Bewegung einzuschränken und Cyberkriminellen Einhalt zu gebieten.

Auch führende Cyberversicherungen erkennen den Wert der Mikrosegmentierung. Da Ransomware die Zahl der Versicherungsabschlüsse wie auch der Schadensfälle ansteigen lässt, sahen sich viele Versicherer gezwungen, die Anforderungen an Sicherheitskontrollen und Überprüfungen zu erhöhen, die Prämien anzuheben – um bis zu 96 % innerhalb eines Jahres – und die Deckungsgrenzen für Lösegeldzahlungen zum Ausgleich von Verlusten abzusenken. Manche Unternehmen finden auf dem Markt schon keinen bezahlbaren Cyberversicherer mehr, oder ihnen wird der Versicherungsschutz gänzlich verweigert. Cyberversicherungen allein können einen schädlichen Einbruch und die daraus resultierenden finanziellen Auswirkungen nicht verhindern. Doch es gibt Sicherheitskontrollen wie Mikrosegmentierung, die es Unternehmen ermöglichen, die neuesten versicherungstechnischen Anforderungen leichter zu erfüllen.

„Mit nur einem einzigen Agent pro Gerät haben wir das Problem eines Endpoint-Angriffs jetzt für immer gelöst.“

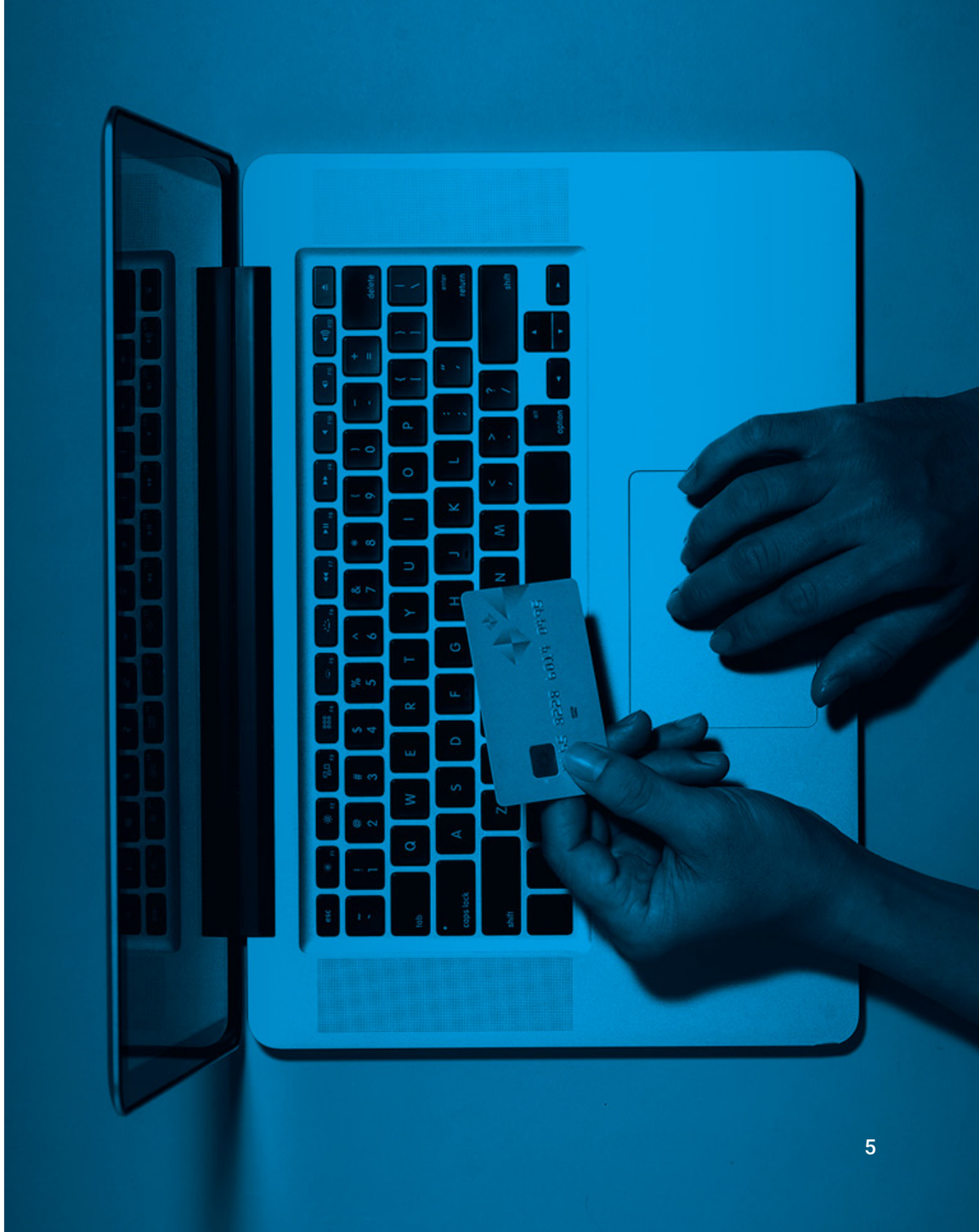
Infrastrukturarchitekt,
Globaler Hersteller von Einzelhandels- und Konsumgütern

Reduzierter Umfang von Audits für PCI-Compliance

E-Commerce-Unternehmen wissen nur zu gut, dass die Erfüllung und Aufrechterhaltung der PCI-Compliance einen beträchtlichen Teil der jährlichen Budgets für Governance, Risiko und Compliance ausmacht und eine erhebliche Belastung für Personal und Ressourcen im Bereich Sicherheit bedeuten kann. Der PCI Data Security Standard (PCI DSS) erfordert fortlaufende Audits von Sicherheitsrichtlinien und -kontrollen zum Schutz der Karteninhaberdatenumgebung (Customer Data Environment, CDE). Auch eine PCI-Umfangsbestimmung – sie dient der Identifizierung von Personen, Prozessen und Technologien, die mit Karteninhaberdaten interagieren oder die Sicherheit in anderer Weise beeinträchtigen könnten – kann die mit der Durchführung eines PCI-Audits verbundenen Kosten deutlich erhöhen.

Obwohl die Netzwerksegmentierung keine offizielle Anforderung von PCI DSS ist, verwenden Handelsunternehmen seit Jahren traditionelle Methoden der Netzwerksegmentierung wie VLANs, ACLs und interne Firewalls. Damit wollen sie Umfang, Kosten, Risiken und Komplexität von Maßnahmen zur Aufrechterhaltung der Compliance reduzieren. Da jedoch die IT-Umgebungen moderner Einzelhandelsunternehmen über Hybrid-, Multicloud- und Microservices-Architekturen hinweg dynamischer geworden sind, können ältere Segmentierungstechnologien und -techniken nicht mehr Schritt halten. Das erhöht den betrieblichen Aufwand, die Komplexität, die Häufigkeit von Anwendungsausfällen und auch die Zahl der Sicherheitslücken.

Grund dafür ist, dass die Verwaltung und Pflege älterer Segmentierungsmethoden umständlich ist. Sie verbrauchen Ressourcen, da sichergestellt sein muss, dass Systeme, Netzwerke und Anwendungen innerhalb der Grenzen der CDE ordnungsgemäß gesichert und kontrolliert werden. Unternehmen operieren in verschiedenen Umgebungen, vom Rechenzentrum über die Cloud bis hin zu containerbasierten Assets. Daher fehlt vielen von ihnen eine umfassende Transparenz der Kommunikationsabläufe von Anwendungen und Systemen. Folglich haben sie Schwierigkeiten, die von der PCI geforderten Firewall-Konfigurationsstandards einzuhalten.



Dies führt zu unzulänglichen Segmentierungspraktiken, die Sicherheitslücken verursachen und ein Nichtbestehen von PCI-Audits zur Folge haben können. Aus diesem Grund setzen Handelsorganisationen verstärkt auf softwaredefinierte Segmentierung. So können sie die Trennung zwischen CDE und außerhalb des CDE-Umfangs liegenden Systemen über Infrastrukturen hinweg einfacher durchsetzen, den Umfang von PCI-Audits reduzieren und die Compliance beschleunigen, weil Segmentierung und Durchsetzung bis hin zu Layer 7 ermöglicht werden. Dieses Niveau wäre mit älteren Tools nicht annähernd erreichbar. Der schlanke Agent von Akamai erfordert keine Firewall, keine Netzwerkänderungen oder Serverneustarts. Zudem arbeitet er unabhängig von der zugrunde liegenden Infrastruktur. Das bedeutet: Es gibt keine Ausfallzeiten von Anwendungen und man hat die Möglichkeit, für Änderungskontrolle oder Wartung erforderliche Zeitfenster zu meiden.

Da bei der softwaredefinierten Segmentierung die Sicherheit von der zugrunde liegenden Infrastruktur und den Betriebssystemen abgekoppelt ist, kann die Segmentierung unabhängig durchgeführt werden, ohne das Netzwerk oder die Anwendung zu berühren. Mit diesem Ansatz können Unternehmen im Handel eine detaillierte Transparenz von Netzwerken und Assets in den unterschiedlichen Umgebungen erreichen. Die dazu verwendete Lösung fungiert als verteilte Firewall mit statusgesteuerten Inspektionsfunktionen und ermöglicht einen vollständigen Schutz. Da außerdem weniger Aufwand und Ressourcen für die Bereitstellung und Verwaltung erforderlich sind und die Produktivität von SecOps um ca. 95 % steigt, können Unternehmen ihre Sicherheitslage verbessern und sich gleichzeitig vieler Probleme rund um die PCI-Compliance entledigen. Als zusätzlichen Bonus ermöglicht unsere Lösung Handelsunternehmen, Echtzeit- und Verlaufsansichten des Netzwerks zu nutzen, um im Rahmen von Audits die Compliance zu überprüfen.

> „Dank der softwaredefinierten Segmentierung konnten wir Segmentierungsrichtlinien auf Prozessebene erstellen und durchsetzen. Das hatte sowohl für unsere Sicherheit als auch für die Fähigkeit zur Erfüllung der technischen PCI-DSS-Anforderungen erhebliche Verbesserungen zur Folge.“
>
> Senior Infrastructure Engineer, The Honey Baked Ham Company

Sorgen Sie für Transparenz und Schutz – vom IoT bis hin zur Legacy-Infrastruktur

Von der Ransomware-Eindämmung bis hin zur Verwaltung von Sicherheitskontrollen für die PCI-Compliance: Handelsunternehmen sind mit zusätzlicher Komplexität konfrontiert, wenn sie physische Standorte wie stationäre Geschäfte, Produktionsstätten und Distributionslager sichern wollen. Bei Fluggesellschaften können IoT-Sensoren und -Geräte die Echtzeitüberwachung und vorausschauende Wartung von Flugzeugsystemen ermöglichen, um Performance und Sicherheit zu verbessern. Und Unternehmen im Gastgewerbe setzen IoT-basierte Geräte ein, um intelligente Hotelzimmer zu ermöglichen, die das Kundenerlebnis und die betriebliche Effizienz steigern.

Es liegt auf der Hand, dass viele dieser Standorte und Umgebungen eine Vielzahl von IoT- oder OT-Assets (OT = Operational Technology) enthalten, die keine hostbasierten Sicherheitsagenten ausführen können, wodurch sie noch anfälliger für Hardware- und Softwareschwachstellen sind. In der 2023 veröffentlichten Forrester-Studie „The State of IoT Security“ nannten 33 % der Sicherheitsverantwortlichen weltweit IoT-Geräte als das häufigste Ziel externer Cyberangriffe. Unternehmen müssen daher eine Segmentierungslösung mit agentenloser Funktionalität implementieren, die IoT- und OT-Umgebungen schützt. Die Lösung muss außerdem das Risiko minimieren können, dass ein Angreifer eine Geräteschwachstelle ausnutzt, um Zugriff auf die gesamte IT-Infrastruktur zu erhalten.

Diese Art von Lösung muss in der Lage sein, im Zuge der durchgängigen Überwachung neu verbundene Geräte zu erfassen und die Kommunikation nicht genehmigter Geräte mit dem Netzwerk automatisch zu blockieren. Durch integriertes Geräte-Fingerprinting erkennt die Lösung von Akamai verbundene Geräte automatisch und klassifiziert sie nach logischen Gruppen, die die Grundlage für skalierbare, abstrakte Sicherheitsrichtlinien bilden. Segmentierungsrichtlinien können für IoT- und OT-Geräte über eine einheitliche Schnittstelle erstellt werden. Wie andere Richtlinien folgen sie dem durch Fingerprinting erkannten Gerät. Das geschieht unabhängig davon, wo sich die Geräte befinden (und auch wenn Geräte zu neuen Netzwerkstandorten wechseln) oder wie viele Geräte in der Umgebung vorhanden sind.

Zero-Trust-basierte Richtlinien werden über Netzwerk-Switch-ACLs durchgesetzt, ohne dass dafür ein Agent erforderlich ist. Dadurch werden Lücken bei der Durchsetzung beseitigt, die bei IoT- und OT-Bereitstellungen zu Risiken führen können. Auch wenn man solche sicheren Grenzen festlegt, bleiben die erforderlichen Verbindungen zu IT-Managementsystemen, dedizierten Update-Servern und Protokollierungsservern verfügbar, sodass sicherheitsbedingte Reibungsverluste reduziert werden. Mit unserer Lösung können Sie alle IoT- und OT-Systeme neben Ihrer IT-Infrastruktur erkennen, visualisieren und zuordnen, um eine zentrale Ansicht Ihrer Unternehmensressourcen zu erhalten.

Neben der Sicherung von IoT/OT-Assets und anderen Endpunkten mit Air-Gap-Funktionen verlassen sich viele Einzelhandelsunternehmen bekanntermaßen auf Systeme, Server und Anwendungen, die auf älteren oder End-of-Support-Betriebssystemen und -Infrastrukturen ausgeführt werden, die nicht gepatcht werden können. Das damit verbundene Risiko ist erheblich. Viele dieser älteren Server können nicht ausgemustert werden, da sie immer noch Umsatz generieren oder das Rückgrat des Unternehmens bilden. Das gilt insbesondere für E-Commerce-Unternehmen, die nicht von Anfang an auf Cloudnativität ausgelegt waren. Die Agenten von Akamai bieten branchenführende Abdeckung und Kompatibilität. Sie können sowohl auf modernen als auch auf älteren Betriebssystemen ausgeführt werden und bieten umfassende Einblicke in den Netzwerkfluss bis hin zu individuellen Prozess- und Serviceebenen, sowohl für Windows als auch für Linux. Auch die Abdeckung von MacOS-Endpunkten ist enthalten.

Andere Lösungen bieten nur teilweise Transparenz für ältere Betriebssysteme und keine Einsicht in Microsoft Windows-Systeme vor Windows Server 2008 R2. Dies liegt daran, dass der Agent herkömmlicher Mikrosegmentierungslösungen eine Windows-Firewall zur Durchsetzung einer Richtlinie verwendet, die erst für Systeme ab 2002 verfügbar war. Agenten für Linux-Systeme unterstützen nur die Transparenz auf Layer 4, bieten keine Regeln auf Layer-7-Prozessebene für Linux-Umgebungen und sind bei der Durchsetzung von Richtlinien abhängig von iptables. Die Funktionen von Akamai Guardicore Segmentation werden auf fast allen neuen und älteren Windows- und Linux-Betriebssystemen unterstützt, da der Einsatz unserer Lösung nicht von der zugrunde liegenden Infrastruktur abhängig ist.

Einfach, schnell, intuitiv – und sicherer

Von der Unternehmenszentrale bis zum Einzelhandelsgeschäft, vom Rechenzentrum bis zur Cloud und darüber hinaus: Mikrosegmentierung ist entscheidend, wenn es darum geht, Zero Trust zum Schutz kritischer IT-Assets einzuführen.

Die Einfachheit von Akamai Guardicore Segmentation reduziert im Vergleich zu langsameren, herkömmlichen Methoden der Netzwerksegmentierung den Zeit- und Arbeitsaufwand für Bereitstellung, Durchsetzung, Überwachung und Vorfallsreaktion erheblich. Änderungen der Richtlinien lassen sich schnell umsetzen und erfordern keine komplexen Netzwerkänderungen. Das kann während der Hauptsaison, bei Werbeaktionen, Produkteinführungen oder in anderen geschäftlich bedeutsamen Phasen von entscheidender Bedeutung sein.

Das Ergebnis: So wie Sie Ihre Kunden, Gäste oder Passagiere nicht bitten würden, sich zwischen Qualität und Sicherheit zu entscheiden, verlangt eine gute Lösung zur Mikrosegmentierung nicht von Ihnen, eine Wahl zwischen Sicherheit und Agilität zu treffen. Es ist an der Zeit, Segmentierung einfacher zu machen.

Möchten Sie mehr erfahren?

Erfahren Sie, wie Sie mit Akamai Guardicore Segmentation, das zum Akamai Zero Trust-Portfolio gehört, Ihre Angriffsfläche reduzieren, kritische Anwendungen schützen, und die Compliance optimieren können.

Weitere Informationen

TechnologyAdvice | Akamai

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.