
WHITEPAPER

# Untersuchung der wichtigsten Anwendungsfälle für die Mikrosegmentierung

Von John Grady, Senior Analyst der Enterprise Strategy Group

Januar 2023

Dieses Whitepaper der Enterprise Strategy Group wurde von Akamai in Auftrag gegeben und wird unter Lizenz von TechTarget, Inc., vertrieben.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

## Inhalt



© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

## Zusammenfassung

Zero Trust ist in der Cybersicherheitsbranche mittlerweile allgegenwärtig. Dennoch haben die Breite der Initiative und die konkurrierenden Ansichten dazu, was für die Strategie am wichtigsten ist, zu Verwirrung darüber geführt, wo Unternehmen ansetzen sollten und welche Tools das Framework am besten unterstützen. Zwar gibt es nicht nur einen richtigen Weg zu Zero Trust, aber die Strategie ist letztlich davon abhängig, dass sichergestellt wird, dass Ressourcen und Entitäten nur dann miteinander kommunizieren können, wenn dies laut Richtlinien ausdrücklich erlaubt ist. Das deutet auf die Bedeutung der Mikrosegmentierung hin.

Der Einsatz von Mikrosegmentierungstools ist heute noch nicht sehr verbreitet, wird jedoch angesichts der Bedeutung der Mikrosegmentierung für Zero Trust und ihre Anwendbarkeit auf eine Vielzahl von Anwendungsfällen voraussichtlich deutlich ansteigen. Egal, ob Unternehmen Zero Trust in Betracht ziehen, um Bedrohungen zu verhindern, die Effizienz im gesamten Unternehmen zu fördern oder ihren allgemeinen Sicherheitsansatz zu modernisieren – Mikrosegmentierung kann dabei helfen. Insbesondere der softwaregestützte Ansatz von Akamai für die Mikrosegmentierung mit künstlicher Intelligenz bietet granulare Transparenz und ermöglicht es Unternehmen, laterale Bewegung zu verhindern, Ransomware-Angriffe zu stoppen und Zero-Trust-Prinzipien in der gesamten Umgebung einheitlich durchzusetzen.

**Egal, ob Unternehmen Zero Trust in Betracht ziehen, um Bedrohungen zu verhindern, die Effizienz im gesamten Unternehmen zu fördern oder ihren allgemeinen Sicherheitsansatz zu modernisieren – Mikrosegmentierung kann dabei helfen.**

## Zero Trust gewinnt an Fahrt, aber die Festlegung klarer Prioritäten ist entscheidend

Unternehmensumgebungen werden immer komplexer, da Ressourcen in die Cloud verlagert werden, digitale Geschäftsmodelle greifen und Nutzer zunehmend verteilt sind. Diese Änderungen machen die Arbeit von Cybersicherheitsteams von Natur aus schwieriger, da Angreifer versuchen, Lücken in den Abwehrmechanismen zu durchdringen, um Ransomware-Angriffe zu starten, Kundendaten zu stehlen oder sensibles geistiges Eigentum zu extrahieren. Leider können herkömmliche Sicherheitsansätze, die auf stark freizügigen, perimeterbasierten Kontrollen basieren, diese Gegebenheiten nicht mehr bewältigen und zwingen Sicherheitsteams, ihre Strategien neu zu bewerten. Darüber hinaus nimmt die Anzahl und die Raffinesse der Angriffe zu, sodass Sicherheitsteams nicht mehr mit jeder potenziellen Bedrohung Schritt halten, sie abwehren und Patches dagegen einspielen können.

Diese Probleme haben bei vielen dazu geführt, sich mit dem Konzept von Zero Trust zu beschäftigen. Zero-Trust-Strategien sind zwar nicht neu, werden jedoch für Unternehmen zunehmend interessant, da sie einen Weg zu einem dynamischeren und risikobasierteren Ansatz für Cybersicherheit bieten, der auf einem Zugriff mit geringstmöglichen Berechtigungen beruht. Ein Zero-Trust-Ansatz eliminiert das implizite Vertrauen in der Umgebung und validiert kontinuierlich jede digitale Interaktion. Daher sollte ein Zero-Trust-Ansatz Sicherheitsteams mehr Sicherheit bieten, dass ihre Ressourcen, Nutzer und Geräte sicher und verfügbar bleiben. Die weite Verbreitung von Zero Trust in Verbindung mit manchmal widersprüchlichen Ansichten und Definitionen darüber, was Zero Trust ist, hat jedoch zu Verwirrung geführt, sodass Unternehmen mitunter nicht mehr wissen, wo sie ansetzen sollen.

Die Bewertung der Unternehmensprioritäten und der gewünschten Ergebnisse kann helfen, den Schwerpunkt einzugrenzen und zu bestimmen, wo mit einer Zero-Trust-Initiative begonnen werden sollte. Es gibt eine Vielzahl von Geschäftsfaktoren, die Unternehmen zu Zero Trust bewegen (siehe Abbildung 1).[1] Das häufigste Ziel ist die Modernisierung der Cybersicherheit, die von 51 % der Befragten angegeben wird. Diese Einstellung wurde von der US-Bundesregierung

**Zero Trust ist davon abhängig, sicherzustellen, dass Ressourcen und Entitäten nur miteinander kommunizieren können, wenn dies durch Richtlinien ausdrücklich zugelassen wird.**

[1] Quelle: Ergebnisse der Umfrage der Enterprise Strategy Group, *The State of Zero Trust Security Strategies*, Mai 2021.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

durch die von der Biden-Regierung erlassenen Exekutivaufträge zur Cybersicherheit unterstrichen, die die Zero-Trust-Architektur in ihren Modernisierungsanforderungen genannt hat. Diese Aufträge sind zwar nicht direkt auf den Privatsektor ausgerichtet, können aber dazu beitragen, Sicherheitsteams außerhalb der Bundesregierung eine Richtung vorzugeben. Weitere strategische Ziele für Zero Trust sind die Unterstützung der digitalen Transformation (35 %) und die Beschleunigung der Cloudeinführung (34 %). Diese Faktoren verdeutlichen die Erwartungen, die viele Unternehmen an ihre Sicherheitsteams stellen, nämlich das Unternehmen zu unterstützen, anstatt nur Ressourcen zu schützen. Taktische Ziele wie die Reduzierung der Anzahl von Sicherheitsvorfällen (43 %), die Ermöglichung eines sicheren Remotezugangs (41 %), die Vereinfachung der Compliance (31 %) und die Verhinderung von Datenextraktion (30 %) werden ebenfalls häufig genannt.

**Abbildung 1. Treibende Faktoren für Zero Trust**


*Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.*

Die Eingrenzung des anfänglichen Schwerpunkts eines Zero-Trust-Projekts kann dem Sicherheitsteam in einigen Fällen helfen, die Tools zu identifizieren, die zur Unterstützung der Strategie erforderlich sind. Wenn das Ziel beispielsweise darin besteht, den sicheren Remotezugriff für Mitarbeiter und Dritte zu verbessern, werden sich viele für einen Zero-Trust-Netzwerkzugang (ZTNA) entscheiden. In diesem Szenario können auch Identitätstools wie die Multi-Faktor-Authentifizierung (MFA) zum Einsatz kommen. Bei einigen Faktoren lassen die Anforderungen an die Technologie möglicherweise jedoch Raum für Interpretationen, und viele Unternehmen konzentrieren sich selbst nach dem Eingrenzen auf mehrere Ziele. In einer solchen Situation ist es für Unternehmen wichtig, Tools und Verfahren zu identifizieren, die eine Vielzahl von Anwendungsfällen und Ergebnissen unterstützen können.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

## Die Mikrosegmentierung wird derzeit bei der Unterstützung eines Zero-Trust-Modells nicht ausreichend genutzt

Zwar gibt es nicht nur einen richtigen Weg zu Zero Trust, aber die Strategie ist letztlich davon abhängig, dass sichergestellt wird, dass Ressourcen und Entitäten nur dann miteinander kommunizieren können, wenn dies laut Richtlinien ausdrücklich erlaubt ist. Das bedeutet, dass ein Schlüsselelement der Zero-Trust-Philosophie jedes Unternehmens darin bestehen sollte, die richtige Segmentierung ihrer Ressourcen sicherzustellen, um die Auswirkungen erfolgreicher Angriffe zu begrenzen. Dies kann für ein übergeordnetes Ziel, wie z. B. die Modernisierung der Cybersicherheit, genauso gelten wie für einen fokussierteren Zweck, etwa die Verhinderung von Datenextraktion.

In der heutigen Umgebung reicht die grobkörnige Segmentierung jedoch in der Regel nicht aus. Vielmehr ist eine granulare Mikrosegmentierung erforderlich, um die Unternehmensressourcen angemessen zu schützen. Moderne Anwendungsarchitekturen basieren häufig auf Workloads, die über mehrere Serverinstanzen und in einigen Fällen auch über mehrere Cloudumgebungen hinweg verteilt sind. Die Segmentierung von Ressourcen nach Standort ist veraltet und geht nicht mehr auf die Herausforderungen ein, mit denen sich Sicherheitsteams heute konfrontiert sehen.

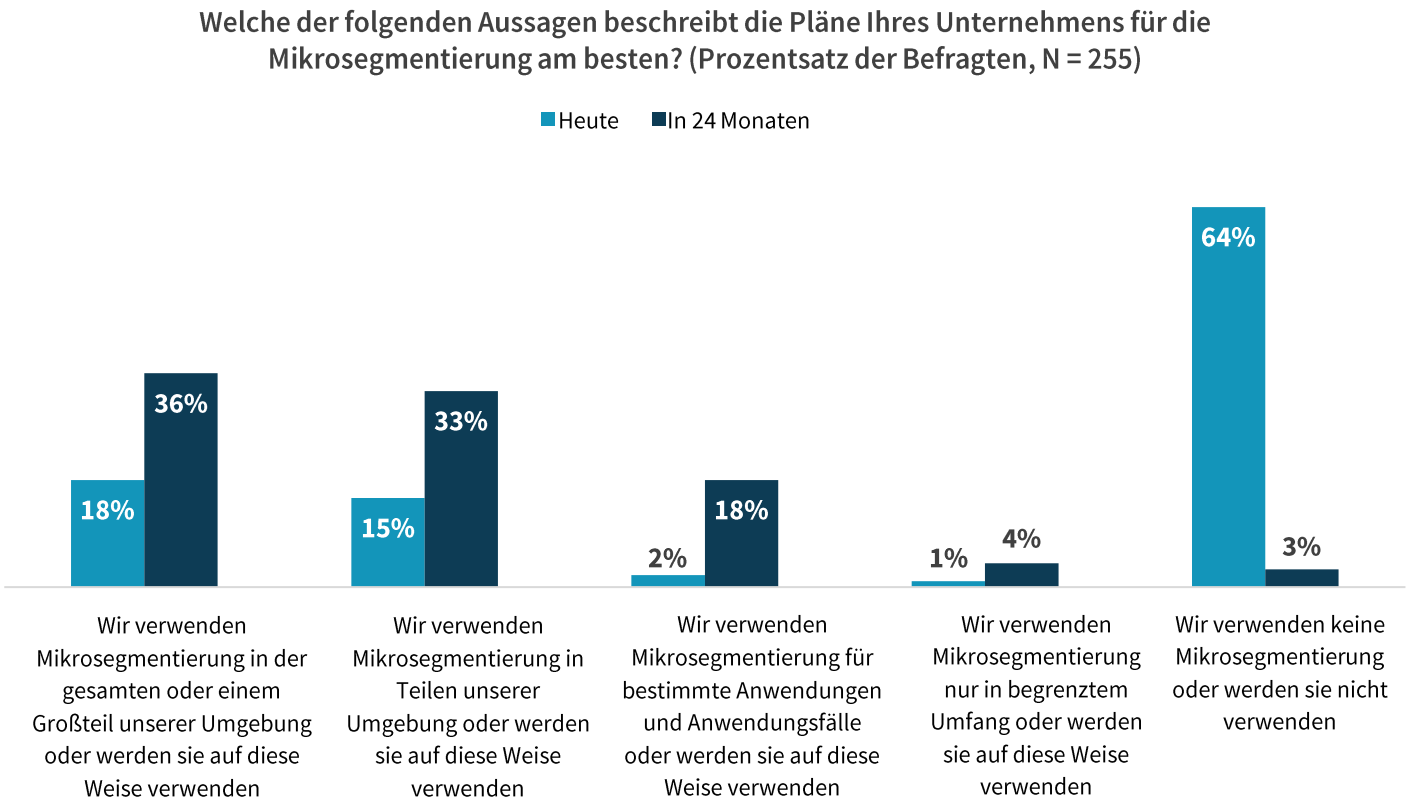
In der Vergangenheit waren Unternehmen eher zögerlich, Mikrosegmentierungstools einzuführen. Untersuchungen der Enterprise Strategy Group (ESG) von TechTarget haben ergeben, dass 28 % der Unternehmen die Mikrosegmentierung für zu komplex halten. Dies ist jedoch wahrscheinlich zum großen Teil darauf zurückzuführen, dass Sicherheitsteams die falschen Tools für die Mikrosegmentierung verwenden. Insbesondere haben ESG-Studien ergeben, dass 55 % der Unternehmen Infrastrukturtools für die Mikrosegmentierung verwenden, wie z. B. Firewalls, während nur 8 % hostbasierte Tools verwenden.[2] Firewalls können die granularen Richtlinien, die für eine erfolgreiche Mikrosegmentierung erforderlich sind, nicht durchsetzen. Darüber hinaus bieten diese Tools nur eine eingeschränkte Transparenz über alle Anwendungs-Workloads hinweg und können nur schwer die Anforderungen für alle Aspekte der Umgebung sowohl an lokalen als auch an Cloudstandorten konsequent erfüllen.

Dies hat dazu geführt, dass die Mikrosegmentierung nicht ausreichend genutzt wird. Trotz der Bedeutung von Zero Trust verwenden laut einer ESG-Studie nur 36 % der Unternehmen heute Mikrosegmentierung (siehe Abbildung 2). Die gute Nachricht ist, dass viele Unternehmen erkennen, dass dies eine erhebliche Lücke in ihrer Verteidigungsstrategie ist. Daher gehen 91 % davon aus, dass sie in den nächsten 24 Monaten die Mikrosegmentierung verwenden werden.[3] Letztendlich verfestigt und unterstützt die Mikrosegmentierung die wichtigsten Vorteile von Zero Trust, indem physische, virtuelle und Cloudnetzwerke vor externen und internen Bedrohungen geschützt werden. Daher sollte die Mikrosegmentierung eine Kernkomponente jeder Zero-Trust-Strategie sein.

[2] Quelle: Ergebnisse der Umfrage der Enterprise Strategy Group, *Network Security Trends in Hybrid Cloud Environments*, Dezember 2021.
[3] Ibid.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

**Abbildung 2. Einführung der Mikrosegmentierung**




*Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.*

## Wichtige Anwendungsfälle für die Mikrosegmentierung

Die Mikrosegmentierung ist für eine Vielzahl von Zero-Trust-Anwendungsfällen allgemein anwendbar – ein wichtiger Grund dafür, dass sie mehr denn je betont wird. Zunächst einmal ist die Mikrosegmentierung ein guter Ausgangspunkt für den Weg eines Unternehmens hin zu Zero Trust, da sie die wichtigsten Unternehmensressourcen sichern kann, insbesondere wenn die verwendete Lösung eine hochgradig granulare Transparenz über Workload- und Entitätsbeziehungen hinweg bietet. Die Entwicklung von Normwerten für Datenverkehrsflüsse und Abhängigkeiten ist für alle Zero-Trust-Bemühungen von grundlegender Bedeutung. Dies ist ein erster Schritt, um implizites Vertrauen zu beseitigen, ohne den Geschäftsablauf zu stören. Eine aktive Zero-Trust-Implementierung ermöglicht es Sicherheitsteams, die wichtigsten Ressourcen schnell zu schützen, um die Auswirkungen im Falle eines Sicherheitsverstoßes zu begrenzen. Sobald diese Sicherheitsstufe implementiert ist, können Sicherheitsteams dann ihre Aufmerksamkeit auf einige der anderen Anwendungsfälle lenken, die die Mikrosegmentierung unterstützt.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

## Verhinderung von Bedrohungen

Zero Trust ist ein Sicherheitsframework, und das Ziel der Sicherheit ist es, das Unternehmen vor Cyberbedrohungen zu schützen. Es folgt also, dass einige der wichtigsten Anwendungsfälle der Mikrosegmentierung darauf ausgerichtet sind, Bedrohungen zu verhindern und deren Auswirkungen auf Unternehmensressourcen zu begrenzen, insbesondere:

- Isolierung kritischer Ressourcen. Sicherheitsteams müssen Risiken abwägen, wenn sie Entscheidungen zur Priorisierung von Schutzmaßnahmen treffen. Hochwertige Anwendungen, die regulierte Kundeninformationen, geistiges Eigentum oder andere sensible Informationen enthalten, sollten aufgrund der potenziellen Auswirkungen einer Kompromittierung dieser Systeme mehr Aufmerksamkeit und erhöhte Sicherheitskontrollen erhalten. Mithilfe der Mikrosegmentierung können Sicherheitsteams sicherstellen, dass diese Anwendungen und die zugehörigen Workloads vollständig vom Rest der Infrastruktur getrennt werden.

- Begrenzung der lateralen Bewegung. Ein unterschätzter Grundsatz von Zero Trust besteht darin, dass immer ein Verstoß unterstellt und davon ausgegangen wird, dass Angreifer Zugang zum Unternehmensnetzwerk haben. Die unkontrollierte Ausbreitung herkömmlicher Endgeräte, Server, Cloudressourcen und sogar intelligenter Geräte macht Eindringversuche unvermeidlich. Wenn der Auswirkungsradius eines potenziellen Angriffs durch Mikrosegmentierung begrenzt wird, kann dies verhindern, dass Angreifer sich lateral durch das Netzwerk bewegen.

### Schutz vor Ransomware

Aufgrund der anhaltenden Verbreitung von Ransomware und der Auswirkungen dieser Angriffe ist das Problem mittlerweile zu einem Problem für die Führungsebene geworden, wenn nicht gar für die Vorstandsebene. Während die Ransomware-Bereitschaft nicht nur eine hohe Sicherheit, sondern auch einen guten Datenschutz und eine gute Vorfallsreaktion erfordert, kann die Mikrosegmentierung Unternehmen eine verlässliche Grundlage dafür bieten, dass sie Angriffe bekämpfen können. Angreifer nehmen im Verlauf eines Angriffs vertrauliche Informationen und Systeme erst ins Visier, nachdem sie in die Umgebung eingedrungen sind und sich Zeit genommen haben, sie zu erkunden. Wenn die Mikrosegmentierung verwendet wird, um kritische Ressourcen einzuzäunen und laterale Bewegung zu begrenzen, können sich Angreifer weniger frei durch die Umgebung bewegen. Wenn ein Ransomware-Angriff entdeckt wird, kann ein Unternehmen, das Mikrosegmentierung verwendet, die von den Angreifern genutzten Kommunikationswege schnell herunterfahren und infizierte Server isolieren, um eine weitere Ausbreitung des Angriffs zu verhindern.

- Bedrohungserkennung und -reaktion. Im Falle eines Angriffs ist Zeit entscheidend. Mithilfe von Mikrosegmentierungstools können Sicherheitsteams schnell und effektiv reagieren, indem sie anhand von Anwendungsbeziehungen potenzielle Angriffswege rasch erkennen, die von den Angreifern während eines Angriffs genutzten Ports blockieren und betroffene Systeme schnell vom restlichen Netzwerk trennen und unter Quarantäne stellen. Dies gilt auch für den Angriff auf den ersten Einstiegspunkt.

## Steigerung der Effizienz im gesamten Unternehmen

Während das erste Ziel des Sicherheitsteams darin besteht, die Umgebung zu schützen, ist es heute auch ungeschriebenes Gesetz, dass dabei die Effizienz des Geschäftsablaufs nicht beeinträchtigt werden soll. Wenn Sicherheitsteams ihre Kollegen tatsächlich unterstützen und befähigen können, hilft dies dem gesamten Unternehmen. Die Unterstützung kann eine Vielzahl von Formen annehmen, wobei die folgenden die häufigsten sind:

- Unterstützung der Cloudeinführung. Die Umstellung auf die Cloud ist nichts Neues, aber Sicherheitsbedenken sind für viele Unternehmen weiterhin ein Thema. Einige Bedenken sind auf die mangelnde Vertrautheit mit den nativen Sicherheitskontrollen auf Infrastructure-as-a-Service-Plattformen zurückzuführen, andere auf die Sicherheitsinkonsistenz, die in Hybrid-Cloud-Umgebungen auftreten kann. Die Mikrosegmentierung gibt Unternehmen mehr Sicherheit, da Kontrollen in allen Teilen der Umgebung eingesetzt werden können und eine bessere Sicherheitskonsistenz in Hybrid-Cloud-Szenarien bieten.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

- Ermöglichung der Anwendungsmodernisierung. Neben der Umstellung auf die Cloud schreitet auch die Einführung moderner Anwendungsarchitekturen wie Container immer schneller voran. Mit diesen Modellen können Anwendungsteams Anwendungen schneller als je zuvor entwickeln, erstellen und bereitstellen. Tools, die sicherstellen können, dass diese Ressourcen geschützt sind, ohne die Geschwindigkeit der Entwickler einzuschränken, wirken sich positiv auf das Unternehmen aus. Mithilfe von Tools zur Mikrosegmentierung, die einen Einblick in den Datenverkehrsfluss in Container-Umgebungen bieten und automatisch Segmentierungsrichtlinien anwenden, wenn Container online gebracht oder verschoben werden, können die Entwicklungsteams sicherstellen, dass ihre Anwendungen sicher sind.

- Optimierung der Compliance. Regulatorische Angelegenheiten nehmen immer mehr Zeit, Budget und Aufmerksamkeit in einem Unternehmen in Anspruch. Wenn Sie sicherstellen, dass Sicherheitsrisiken so weit wie möglich isoliert sind, um potenzielle Probleme wie Datenschutzverletzungen oder den Verlust von personenbezogenen Daten zu begrenzen, kann dies den Prozess wesentlich weniger belastend gestalten. Durch die Mikrosegmentierung kann sichergestellt werden, dass Systeme, die Compliance-Anforderungen unterliegen, von der übrigen Umgebung isoliert sind, wodurch die Belastung für Sicherheitsteams verringert werden kann.

### Zero-Trust-Segmentierung

Einer der attraktivsten Aspekte der Mikrosegmentierung besteht darin, dass sie den Unternehmen unmittelbaren Nutzen bringen kann, wenn sie sich auf sehr zielgerichtete Anwendungsfälle konzentriert. Die Möglichkeit, mit Blacklisten zu beginnen, kritische Anwendungen zu umzäunen, sowie die Umgebungssegmentierung und andere weniger komplizierte Richtlinien zu erstellen, die relativ einfach und schnell einen Wert bieten, kann für viele von Vorteil sein. Nur wenige Unternehmen, wenn überhaupt, setzen eine vollständige Mikrosegmentierungsstrategie im gesamten Unternehmen auf einmal um. Wenn jedoch die Mikrosegmentierung im Rahmen einer Zero-Trust-Initiative in der gesamten Umgebung umfassender implementiert wird, werden viele Unternehmen damit beginnen, die Zero-Trust-Segmentierung anzugehen. Diese kombiniert die zuvor besprochenen Anwendungsfälle und positiven Ergebnisse, da Unternehmen in der Lage sind, umfassende und granulare Einblicke in die Datenverkehrsflüsse zu erhalten, ihre sensibelsten Ressourcen zu schützen, laterale Bewegung zu verhindern und schnell auf Bedrohungen zu reagieren und dabei gleichzeitig das Unternehmen besser zu unterstützen. Dies ist zwar nicht der Ausgangspunkt für viele Mikrosegmentierungsprojekte, sollte aber als Ziel betrachtet werden, das mit der Zeit angestrebt werden soll.

## Der Mikrosegmentierungsansatz von Akamai

**Die Lösung Akamai Guardicore Segmentation ist ein softwarebasierter Mikrosegmentierungsansatz, der Bedrohungen daran hindern soll, eine laterale Bewegung in der digitalen Umgebung zu erreichen.**

Unternehmen müssen bedenken, dass die Mikrosegmentierung zwar ein wichtiger Aspekt von Zero Trust ist, dass es jedoch auch andere wichtige Komponenten gibt, die andere Technologien zur Bedrohungserkennung und -reaktion, zum Schutz von Identitäten, zur Datensicherheit und vielem mehr erfordern. Die Bewertung, Auswahl und Zusammenarbeit mit Technologieanbietern ist ein detailorientierter, methodischer Prozess, der entweder so gestaltet werden kann, dass die Cybersicherheitsziele des Unternehmens erfüllt werden, oder der einfach nur Geld, Zeit und Personalkapazitäten verschlingt. Wenn Unternehmen die Verwendung von Mikrosegmentierungstools, die eine breite Palette von Integrations- und Signalfreigabefunktionen bieten, in Erwägung ziehen, kann dies dazu beitragen, eine Zero-Trust-Strategie über die Mikrosegmentierung hinaus voranzutreiben und die betriebliche Komplexität zu reduzieren.

Akamai, ein etablierter Anbieter von Netzwerkinfrastrukturen, hat Mikrosegmentierung und Zero-Trust-Kernelemente in sein Lösungsportfolio aufgenommen. Das Wissen des Unternehmens über die Anforderungen an die Unternehmensinfrastruktur sowohl für lokale als auch für Cloudumgebungen berücksichtigt die Erfahrung bei der Erkennung und Bearbeitung potenzieller Cybersicherheitsherausforderungen.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

Die Akamai Guardicore Segmentation ist ein softwarebasierter Mikrosegmentierungsansatz, der Bedrohungen daran hindern soll, eine laterale Bewegung in der digitalen Umgebung zu erreichen. Die Sichtbarkeit ist granular, damit Unternehmen Zero-Trust-Prinzipien auf Netzwerkebene durchsetzen und Aktivitäten und Bewegungen innerhalb der physischen und virtuellen Umgebung visualisieren können. Das auf künstlicher Intelligenz basierende Segmentierungsframework nutzt integrierte Vorlagen, um Vorfälle wie Ransomware, Angriffe auf Endgeräte und Angriffe auf Remotemitarbeiter zu erkennen und zu stoppen. Es kann auf einer Vielzahl von Plattformen verwendet werden, darunter Bare-Metal-Server, virtuelle Maschinen, Container, IoT-Geräte und Cloudinstanzen.

Akamai Guardicore Segmentation sammelt auf verschiedene Weise umfangreiche Daten über die zugrunde liegende Infrastruktur. Dazu gehören agentenbasierte Sensoren, netzwerkbasierte Datenerfassung, Virtual Private Cloud Flow Logs sowie Integrationen, die agentenlose Funktionalitäten ermöglichen. Dynamisches Mapping bietet Administratoren eine End-to-End-Ansicht der Aktivitäten mit grober Granularität. Aufgrund der Erfahrung von Akamai in Unternehmensnetzwerkumgebungen ist Akamai Guardicore Segmentation auf Skalierbarkeit auf Unternehmensniveau und konsistente Performance ausgelegt, die Quellen von Datenverkehrsengpässen identifiziert und entsprechende Problemumgehungen bietet.

## Fazit

Die Mikrosegmentierung ist keine neue Technologie. Tatsächlich war sie vielleicht sogar ihrer Zeit voraus. Die Bedeutung der Mikrosegmentierung bei der Sicherung moderner hybrider Multi-Cloud-Umgebungen und insbesondere bei der Umsetzung von Zero-Trust-Strategien kann jedoch nicht hoch genug angesetzt werden. Die Mikrosegmentierung bietet die Flexibilität, Agilität und Effizienz, die notwendig ist, um Zero Trust in einer Reihe von unternehmens- und geschäftskritischen Anwendungsfällen zu ermöglichen und alles von kritischer Infrastruktur und geistigem Eigentum bis hin zu Identitäten und Anmeldedaten zu schützen. Die Erfahrung von Akamai in den Bereichen Netzwerkinfrastruktur, Segmentierung und Mikrosegmentierung macht das Unternehmen zu einem geeigneten Partner für die Planung, den Aufbau, die Bereitstellung und sogar die Verwaltung einer sicheren Infrastruktur, die auf Mikrosegmentierungstools und -denkweisen basiert.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.

Alle Produktnamen, Logos, Marken und Handelsmarken sind Eigentum ihrer jeweiligen Inhaber. Die in dieser Veröffentlichung enthaltenen Informationen wurden von Quellen bezogen, die TechTarget, Inc., als zuverlässig erachtet, die jedoch von TechTarget, Inc., nicht garantiert werden. Diese Veröffentlichung kann Meinungen von TechTarget, Inc., enthalten, die sich ändern können. Diese Veröffentlichung kann Prognosen, Projektionen und andere vorausschauende Aussagen enthalten, die angesichts der derzeit verfügbaren Informationen die Annahmen und Erwartungen von TechTarget, Inc., darstellen. Diese Prognosen basieren auf Branchentrends und beinhalten Variablen und Unsicherheiten. Folglich übernimmt TechTarget, Inc., keine Garantie für die Richtigkeit der hierin enthaltenen spezifischen Prognosen, Projektionen oder vorausschauenden Aussagen.

Diese Veröffentlichung ist urheberrechtlich geschützt durch TechTarget, Inc. Jede Reproduktion oder Weitergabe dieser Veröffentlichung, ganz oder teilweise, sei es in Papierform, elektronisch oder anderweitig, an Personen, die nicht dazu berechtigt sind, sie zu erhalten, ohne die ausdrückliche Zustimmung von TechTarget, Inc., verstößt gegen das US-amerikanische Urheberrechtsgesetz und wird zivil- und gegebenenfalls strafrechtlich verfolgt. Bei Fragen wenden Sie sich bitte an Client Relations unter cr@esg-global.com.

Enterprise Strategy Group by TechTarget

**Enterprise Strategy Group** ist ein integriertes Unternehmen für Technologieanalyse, Forschung und Strategie, das der globalen IT-Community Marktinformationen, umsetzbare Erkenntnisse und marktdienliche Inhaltsservices bietet.

www.esg-global.com

contact@esg-global.com

508.482.0188

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.