Akamai

WHITE PAPER

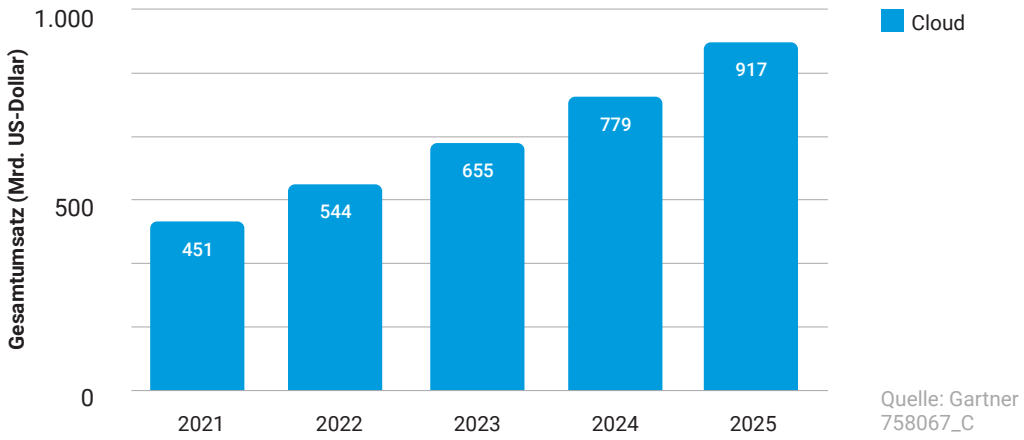
Der Weg führt zur Mikrosegmentierung

Ein Strategieleitfaden für Mikrosegmentierung in Hybrid Clouds

Mehr Clouds in Aussicht

Die Migration riesiger Datenmengen und Datenverarbeitungskapazitäten in die Cloud – oder genauer gesagt in mehrere Clouds – ist wohl die größte Veränderung im Computing-Verhalten von Unternehmen der letzten zehn Jahre. Immer mehr Unternehmen wechseln zu Public Clouds und in der Regel zu Public-Private-Hybrid-Rechenzentrumsarchitekturen. Gleichzeitig nutzen sie IaaS (Infrastructure as a Service) für mehr Agilität. Der Technologieanalyst Gartner rechnet damit, dass bis 2025 etwas mehr als die Hälfte aller IT-Ausgaben der Zielgruppen von traditionellen Lösungen auf die Public Cloud verlagert werden, im Vergleich zu 41 % im Jahr 2022. Während die Gesamtausgaben für die Public Cloud bis 2025 voraussichtlich 900 Milliarden US-Dollar übersteigen werden.[1]

Die Unterscheidung zwischen „der Cloud“ und „mehreren Clouds“ ist nicht trivial. Unternehmen setzen zunehmend auf Multi-Cloud-Plattformen und -Serviceanbieter. Eines ist jedoch klar: Die Idee eines Unternehmens-Rechenzentrums als ein einzelner, sicherer physischer Raum wird nicht überleben. Moderne Rechenzentren bestehen zunehmend aus einer heterogenen Mischung von Umgebungen und Technologien, die physische Server, virtuelle Maschinen und Container in lokalen Einrichtungen, Private Clouds und IaaS-Anbieter für Public Clouds kombinieren. Und diese heterogenen Installationen sind nicht statisch. Unternehmen verlagern ständig Daten und Workloads zwischen ihren unterschiedlichen lokalen und Cloudumgebungen, je nach Traffic- und Verarbeitungsanforderungen.



Umsatzprognose für Public-Cloud-Services weltweit (in Milliarden)

Die zunehmende Komplexität löst neue Schwachstellen aus und vergrößert die Angriffsfläche

Cloudkunden profitieren sicherlich von der zusätzlichen Agilität, Elastizität und Skalierbarkeit, die ihnen IaaS bietet. Diese Vorteile sind ein wesentlicher Grund für die Attraktivität der Cloud. Die Nachteile sind jedoch eine erheblich höhere Verwaltungskomplexität, ein Verlust der umgebungsübergreifenden Workload-Transparenz und eine unbekannte Cybersicherheitslandschaft. Die Zusammenarbeit mit mehreren Cloudanbietern bedeutet, dass Sicherheitsteams mit sehr unterschiedlichen Sicherheitsstandards und -funktionen umgehen müssen. Herkömmliche Sicherheitstools, die für lokale Server und Endpunkte entwickelt wurden, können die Skalierbarkeit und Komplexität der Cloud einfach nicht bewältigen. Neuere Tools, die von IaaS-Anbietern bereitgestellt werden, können in der Umgebung des Anbieters zwar effektiv sein, sind aber in einer Infrastruktur mit mehreren Anbietern von geringem Wert.

Darüber hinaus beruht die Sicherheitsmentalität (und damit auch der Großteil der Investitionen) selbst in diesem Zeitalter von Virtualisierung und „Software-defined everything“ immer noch auf der Notwendigkeit, Angriffe speziell am Eintrittspunkt zu blockieren. Dies ist kein Angriff auf den Netzwerkschutz – er ist immer noch sehr relevant für die IT-Sicherheit, aber er ist nicht so leistungsfähig, wenn sich das Netzwerk ständig verschiebt. Daten und Workloads werden zwischen Public und Private Clouds und lokalen Rechenzentren hin und her verschoben, und die Nutzer, die auf sie zugreifen, arbeiten zunehmend von Remote-Standorten aus, die über die entsprechenden Sicherheitskontrollen verfügen oder auch nicht.

Die schiere Anzahl der jährlich gemeldeten Datenschutzverletzungen reicht aus, um uns zu sagen, dass schlaue Angreifer den Netzwerkschutz praktisch nach Belieben überwinden. Und sobald sie drin sind, finden sie ein relativ flaches Netzwerk vor, in dem die Assets innerhalb des Netzwerks praktisch ungeschützt sind. Trotz all der Flexibilität, die Unternehmen gewonnen haben, hat die zusätzliche Komplexität der Verwaltung und Sicherung von Multicloud-Infrastrukturen die Angriffsfläche exponentiell vervielfacht. Da nur wenige oder gar keine Kommunikationskontrollen vorhanden sind, wird jeder einzelne Server zu einer Angriffsfläche für sich. Infolgedessen haben Angreifer mehr Zeit, sich lateral – und unerkannt – zwischen den Workloads des East-West-Traffics zu bewegen und Ihre wichtigsten Ressourcen aufzuspüren.

Die Netzwerksegmentierung gehört zu den erprobten und etablierten Sicherheitspraktiken, aber heutzutage kann es schwierig sein, sie in dynamischen IT-Infrastrukturen und in der Cloud durchzuführen. Grund dafür ist die Kommunikation von Workloads, die häufig segmentübergreifendend migrieren. Enterprise-Cloud-Kunden haben erkannt, dass sie ihre Anwendungen und Workloads weiter segmentieren müssen, um Kommunikationsflüsse in Echtzeit streng zu kontrollieren und Bedrohungen im Rechenzentrum zu erkennen und zu verhindern, bevor diese Schäden anrichten können. Es wird eine Lösung benötigt, die die Komplexität der IT-Sicherheit verringert, indem sie über Infrastrukturgrenzen hinweg konsistent arbeitet, um die Angriffsfläche insgesamt zu verkleinern, sodass Sicherheitsteams mehr Bedrohungen schneller erkennen und ihre Ausbreitung begrenzen können.

Und genau hier kommt die Mikrosegmentierung ins Spiel.

Definition der Mikrosegmentierung

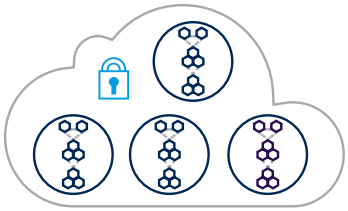
Gartner definiert Mikrosegmentierung als den „Prozess der Implementierung von Isolierung und Segmentierung zu Sicherheitszwecken innerhalb des virtuellen Rechenzentrums“. Darüber hinaus verringert die Mikrosegmentierung „das Risiko einer lateralen Ausbreitung von hoch entwickelten Angriffen in Rechenzentren von Unternehmen und ermöglicht Unternehmen, konsistente Segmentierungsrichtlinien für On-Premise- und Cloud-basierte Workloads durchzusetzen.“[2]

Bei der Mikrosegmentierung werden in der Regel Sicherheitsrichtlinien für einzelne oder Gruppen von Anwendungen festgelegt, unabhängig davon, wo sie sich im hybriden Rechenzentrum befinden. Diese Richtlinien bestimmen, welche Anwendungen und Komponenten miteinander kommunizieren können und welche nicht. Jeder Versuch einer nicht autorisierten Kommunikation ist daher ein sofortiger Hinweis auf das Vorhandensein einer Bedrohung. Mikrosegmentierungstechnologien sind bestenfalls infrastrukturunabhängig, sodass Sicherheitsrichtlinien auch weiterhin ihre jeweiligen Anwendungen schützen können, wenn sie zwischen Cloudumgebungen wechseln.

Lösungsbereiche für die Segmentierung

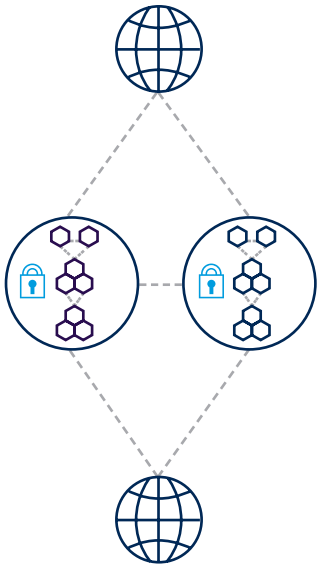
Infrastruktursegmentierung

Sicherer Anwendungs-Traffic innerhalb einer bestimmten Infrastruktur.



Anwendungssegmentierung

Sicherer Traffic zwischen Anwendungen und externen Netzwerken.



Mikrosegmentierung

Regeln zur Sicherung des Traffics in Anwendungen mit zusätzlichem Kontext, z. B. Zuordnung auf Prozessebene.

2 Gartner, „Technology Insight for Microsegmentation“, März 2017; „Hype Cycle for Cloud Security 2017“, Juli 2017

Der Fall der Mikrosegmentierung

Angesichts der dynamischen Rechenzentren von heute ist es erforderlich, dass Unternehmen ihre Aufmerksamkeit von Intrusion Prevention und Zugriffsmanagement auf die Workloads und Anwendungen selbst richten. Und das scheint sich in zunehmendem Tempo zu vollziehen. Bereits 2017 bemerkte Gartner einen Trend zu einem „verstärkten Fokus auf den Schutz von Serverworkloads vor hoch entwickelten, gezielten Bedrohungen, die den herkömmlichen Netzwerk- und signaturbasierten Schutz umgehen. In der Regel handelt es sich dabei um finanziell motivierte Angriffe, die auf Server- und Anwendungs-Workloads abzielen, um an sensible Daten oder Transaktionen zu gelangen“.[3]

Ein wichtiger Faktor für die Mikrosegmentierung ist der Schutz unternehmenskritischer Anwendungen und Workloads. Dies mag einfach nur zum Schutz eigener Interessen oder des geschäftlichen Erfolgs dienen, aber in vielen Fällen ist dies auch durch Sicherheitsrichtlinien und gesetzliche Auflagen vorgeschrieben.

Sicherheitsteams müssen Wege finden, um die wachsende Angriffsfläche in Rechenzentren zu reduzieren, d. h. die Anfälligkeit von Servern zu verringern, auf denen Anwendungen ausgeführt werden. Herkömmliche Authentifizierungstechniken wie das Blockieren von Signaturen oder das Zulassen von Anwendungen werden zu leicht von ausgeklügelten Angreifern umgangen. Die Mikrosegmentierung ermöglicht es Teams, genaue granulare Zugriffs- und Kommunikationsrichtlinien festzulegen und durchzusetzen. Sie sollte zudem die Transparenz der Anwendungsabläufe verbessern und Teams in die Lage versetzen, ihren Sicherheitsstatus besser zu beurteilen.

Benötigen Sie eine Mikrosegmentierung?

Die Beantwortung einiger einfacher Fragen wird Ihnen helfen, Ihren Bedarf an Mikrosegmentierung zu ermitteln.

- Sind Sie in einer regulierten Branche tätig oder müssen Sie Vorschriften zur Datensicherheit und Transaktionssicherheit einhalten?
- Verfügen Sie über eine hybride Infrastruktur mit Workloads, die sich über mehrere Clouds erstrecken?
- Führen Sie Anwendungen auf virtuellen Maschinen oder Containern aus?
- Haben Sie das Gefühl, dass Sie den Überblick und die Kontrolle über Ihre Workloads verlieren?
- Können Sie jederzeit feststellen, ob in Ihrem Rechenzentrum eine Bedrohung vorliegt oder ein Angriff im Gange ist?
- Können Sie die Sicherheit in Ihrer gesamten Infrastruktur über eine einzige Schnittstelle kontrollieren?

Die vier Haupthindernisse auf dem Weg

Wenn sich doch Sicherheitsexperten im Allgemeinen über die Notwendigkeit einer Mikrosegmentierung in den dynamischen Rechenzentren von heute einig sind, warum wird eine effiziente und erfolgreiche Implementierung als so schwierig angesehen? Unternehmen, die versuchen, die Mikrosegmentierung mithilfe herkömmlicher Tools zu implementieren, stoßen in der Regel auf vier große Hindernisse:

1. **Mangelnde Transparenz auf Prozessebene**
   Dies ist wahrscheinlich das erste Hindernis, auf das Sie stoßen werden: Sie können nicht schützen, was Sie nicht sehen. Bei der Mikrosegmentierung geht es um die Sicherung einzelner oder mehrerer Anwendungen und Workflow-Prozesse. Sicherheitsteams benötigen Einblicke in die tatsächlichen East-West-Trafficströme, um diese im Kontext zu verstehen. Die meisten Tools ermöglichen diese Tiefe nicht.

2. **Fehlende Hybrid-Multicloud-Unterstützung**
   Sicherheitsrichtlinien für die Mikrosegmentierung müssen sich problemlos über On-Premise- und Public-Cloud-Umgebungen hinweg skalieren lassen und Workloads auch dann abdecken, wenn sie hin und her verschoben werden. Tools, die für die Arbeit in einer spezifischen Umgebung entwickelt wurden, sind in hybriden Umgebungen ineffektiv.

3. **Unflexible Richtlinien-Engines**
   Wie bereits erwähnt, sind moderne Rechenzentren nicht statisch. Sicherheitsmaßnahmen dürfen es auch nicht sein – eine einmalige Einrichtung ohne weiteres Zutun reicht nicht mehr aus. Leider bieten die vorhandenen Tools von Cloudanbietern nicht die nötige Flexibilität, um Regeln regelmäßig zu prüfen, zu testen und zu verfeinern. Diese Herausforderung wird durch hybride Infrastrukturen noch verschärft, die mehrere Richtlinien-Tools erfordern.

4. **Fehlende Integration in ergänzende Kontrollen**
   Bei richtiger Anwendung schützt die Mikrosegmentierung nicht nur Prozesse, sondern fängt auch Angriffe ab. Die Tools, die nur Mikrosegmentierung bieten, verfügen jedoch in der Regel nicht über Funktionen zur Erkennung von Sicherheitsverletzungen, sodass es dem Nutzer überlassen bleibt, Tools zu integrieren und sie effektiv miteinander zu verbinden. Dieser Patchwork-Ansatz birgt ein hohes Fehlerrisiko.

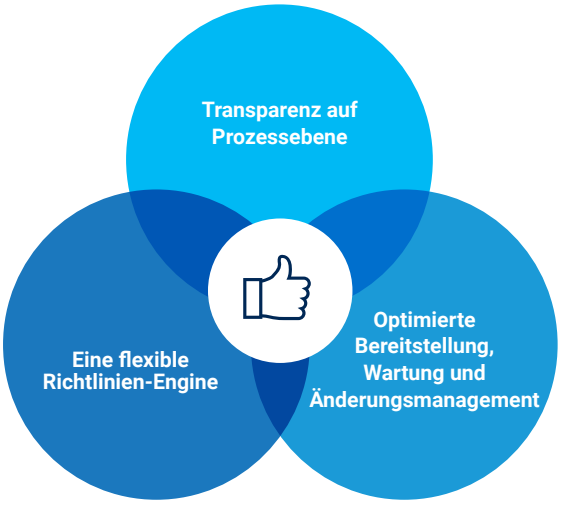
Erfolglose Projekte sind die Norm, nicht die Ausnahme

Angesichts all dieser Hindernisse überrascht es nicht, dass die meisten Mikrosegmentierungsprojekte tendenziell unter extrem langsamen Umsetzungszyklen leiden. Dies führt im Endeffekt dazu, dass die Kosten immer weiter steigen, Ressourcen vorgelagert werden und letztendlich die Ziele nicht erreicht werden. Unternehmen stolpern häufig darüber, was segmentiert werden muss (aufgrund mangelnder Transparenz) und zu entscheiden, wie viel Segmentierung erforderlich ist. Sie können Monate damit verbringen, Tabellen mit komplizierten Regeln für die Kommunikation auf Prozessebene zu erstellen und sind nicht in der Lage, Möglichkeiten zur Gruppierung von Anwendungen und zur Optimierung von Richtlinien zu erkennen. Allzu oft neigen sie zu einer „Übersegmentierung", d. h. es werden zu viele einzelne Richtlinien festgelegt, was zu einer zu hohen Komplexität der Sicherheit führt, was genau das ist, was Sie vermeiden wollen. Nach einer Einschätzung von Gartner „werden mehr als 70 % der Segmentierungsprojekte aufgrund der Übersegmentierung zu einer Neugestaltung der gesamten Netzwerkarchitektur führen".[4]

Eine übermäßige Segmentierung birgt das Risiko, Anwendungen und letztendlich auch den geschäftlichen Erfolg auszubremsen. Das Pendel kann jedoch auch zu weit in die andere Richtung ausschwingen, in Richtung einer nicht ausreichenden Segmentierung, die am Ende Ihre Sicherheitsstrategie gefährdet.

Strategie für eine erfolgreiche Mikrosegmentierung

Der Weg zur Implementierung der Mikrosegmentierung verläuft nicht geradlinig – es gibt viele Drehungen und Windungen, wenn Sie die Kommunikationsflüsse in Ihrer Umgebung entdecken, verstehen und steuern. Daher ist bei der Entwicklung von Sicherheitsrichtlinien Flexibilität erforderlich, um immer wieder neue Änderungen oder Erweiterungen zu integrieren, ohne Anwendungen zu unterbrechen. Viele Lösungen bieten unflexible Engines für die Richtlinienerstellung, sodass Sicherheitsteams unvollständige oder ineffektive Regeln implementieren müssen.



Eine erfolgreiche Implementierung besteht ganz einfach darin, die vier Haupthindernisse zu überwinden oder zu umgehen, unnötige Komplexität zu vermeiden und das Risiko einer Unter- oder Übersegmentierung durch einen stufenweisen Ansatz zu verringern. Das bedeutet, dass eine Lösung vorhanden sein muss, die die folgenden Anforderungen erfüllt:

- **Transparenz auf Prozessebene:** Teams müssen in der Lage sein, alle East-West- und North-South-Datenflüsse aufzudecken, zu erfassen und zu normalisieren; Tools, die eine automatische Erkennung von Anwendungen und ein Verständnis ihrer Kommunikationsanforderungen ermöglichen; die Möglichkeit, nach mehreren Anwendungsattributen zu filtern, um die Kennzeichnung und Gruppierung von Assets zu vereinfachen, die Richtlinien gemeinsam nutzen können.

- **Eine flexible Richtlinien-Engine:** Sie sollten in der Lage sein, gleichzeitig allgemeinere Best Practice- und Compliance-Regeln für große Segmente und detailliertere Regeln für Mikrosegmente zu entwerfen. Die Lösung sollte es Ihnen ermöglichen, schrittweise von der Warnmeldung zur Durchsetzung überzugehen. Außerdem sollten Sie Richtlinien erstellen können, die über alle Plattformen, Geräte und Clouds hinweg funktionieren.

- **Optimierte Implementierung, Wartung und Änderungsmanagement:** Mit dem System sollte es einfach sein, Regeln zu implementieren, zu pflegen und bei Bedarf zu ändern. Die Lösung sollte integrierte Funktionen zur Erkennung von Sicherheitsverletzungen und zur Reaktion auf Vorfälle umfassen. Letztendlich sollten Ihre Richtlinien ausreichend definiert sein, damit Sie sie in automatisierte Bereitstellungs-Tools (CI/CD) für jede neu gestartete Anwendung integrieren können.

Funktionen einer idealen Lösung

Natürlich gibt es viele Mikrosegmentierungstools auf dem Markt, und nicht alle von ihnen machen es einfach, diesem Weg zu folgen. Um eine reibungslose und möglichst erfolgreiche Implementierung zu gewährleisten, sollten Sie sich für eine Lösung mit den folgenden Funktionen entscheiden:

- **Automatische Anwendungserkennung** mit vollständiger Transparenz auf Prozessebene für Bare-Metal-Server, virtuelle Maschinen und Container

- Die Fähigkeit, **zuverlässige und umfassende Abfragen** zu definieren, um kontextbezogene Labels und Objektgruppen zu erstellen

- Eine **flexible Richtlinien-Engine** mit intelligentem Regeldesign, mit der Sie Richtlinien verfeinern, verstärken und verwalten können

- Eine integrierte **Funktion zur Erkennung von Sicherheitsverletzungen** mit mehreren Methoden, mit der Sie mehr Bedrohungen schneller finden und deren Ausbreitung begrenzen können

- **Unterstützung einer hybriden Infrastruktur** – eine Plattform, die mit jeder Infrastruktur kompatibel ist – Rechenzentren, Public und Private Clouds und mehr

Eine Lösung mit diesen Kernfunktionen bietet Ihnen den erfolgreichsten Weg zur Implementierung der Mikrosegmentierung, ermöglicht Ihnen die Überwindung bekannter Hindernisse und Komplexitäten und bereitet Sie darauf vor, alle Geschäftsvorteile einer flexiblen Hybrid-Cloud-Infrastruktur zu nutzen, ohne Abstriche bei der Sicherheit machen zu müssen.

Hybride Rechenzentren, Multicloud-Plattformen und IaaS bieten Unternehmen mehr Flexibilität, Skalierbarkeit und Agilität als in einem „geschlossenen" On-Premise-Rechenzentrum möglich wären. Aber sie machen Anwendungen und Workloads, die eigentlichen Assets, auf die Cyberangreifer abzielen, auch anfälliger und verwundbarer. Obwohl die Mikrosegmentierung weithin als Best Practice für den Schutz von Workloads in der Cloud gilt, fällt es Unternehmen schwer, sie richtig umzusetzen. Die gute Nachricht ist, dass man nicht alles auf einmal machen muss. Die modernen Lösungen in Verbindung mit einem schrittweisen Ansatz erleichtern den Weg zur Implementierung der Mikrosegmentierung erheblich. Und das bedeutet mehr Sicherheit für die wichtigsten Assets Ihres Unternehmens.

Weitere Informationen zur erfolgreichen Implementierung der Mikrosegmentierung finden Sie unter akamai.com/guardicore

1 Laut Gartner werden bis 2025 mehr als die Hälfte der IT-Ausgaben von Unternehmen in Schlüsselmarktsegmenten in die Cloud verlagert werden. Gartner, 9. Februar 2022.

2 Heiser, Jay. „Hype Cycle for Cloud Security, 2017." Gartner, 17. Juli 2017.

3 MacDonald, Neil. „Market Guide for Cloud Workload Protection Platforms." Gartner, 22. März 2017.

4 Young, Greg. „Best Practices in Network Segmentation for Security." Gartner, 28. Juli 2016.

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 Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 05/23.