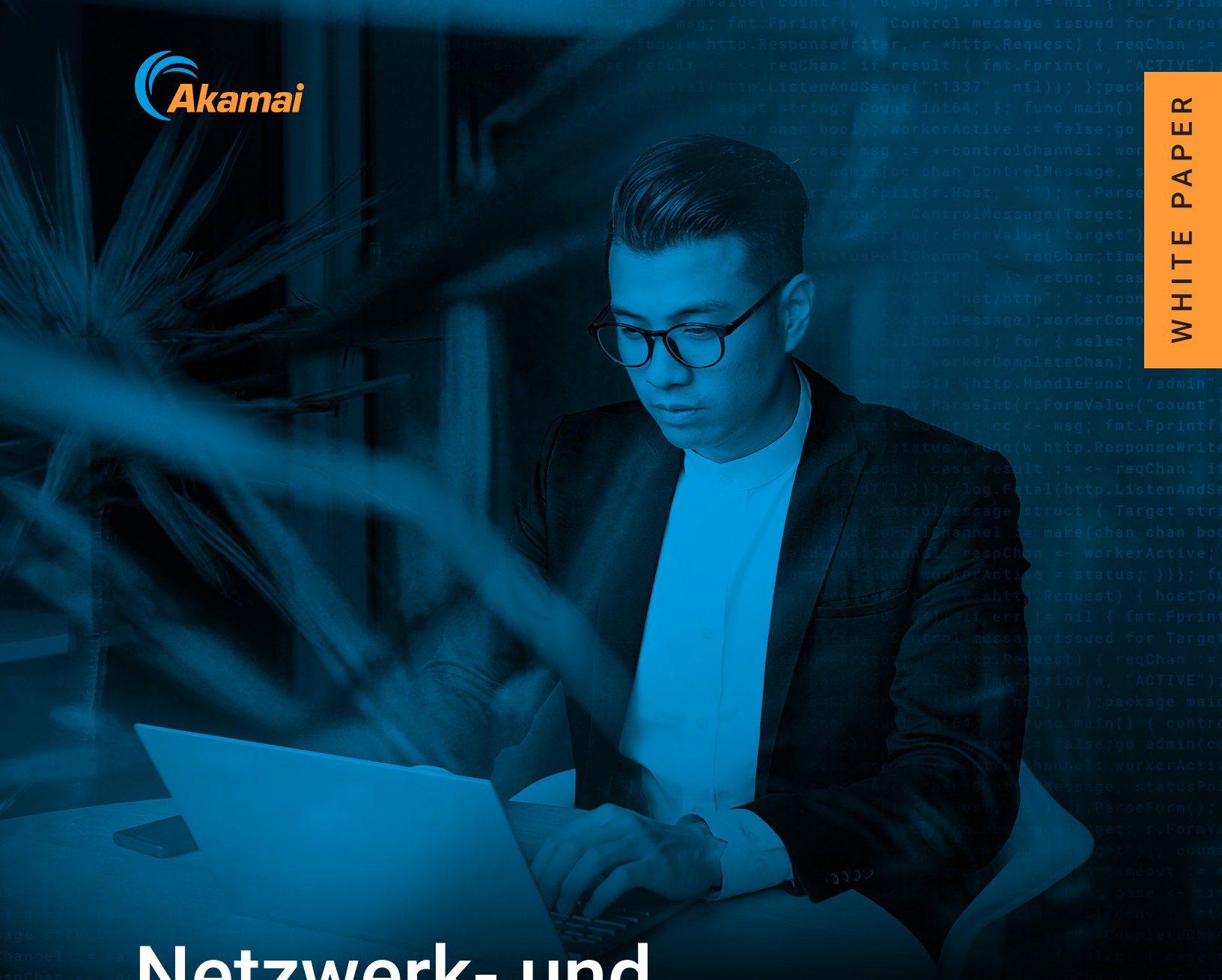
Akamai

WHITE PAPER



Netzwerk- und Mikrosegmentierung in modernen Unternehmensumgebungen

Übersicht

Die Idee, Sicherheit durch Segmentierung zu erreichen, ist nichts Neues. Die meisten Unternehmen nutzen bisher Netzwerk-Firewalls, VLANs und ACLs, um ihre IT-Infrastruktur zu segmentieren und zu schützen. Die Zeiten ändern sich jedoch. Die zunehmende Containerisierung, softwaredefinierte Netzwerke, die Nutzung öffentlicher und Multi-Cloud-Infrastrukturen und die Ausweitung von internetfähigen Geräten haben neue Sicherheitsprobleme geschaffen, die angegangen werden müssen. Sie benötigen eine Lösung, die für eine heterogene IT-Umgebung mit unterschiedlichen Sicherheitsanforderungen entwickelt wurde. Zudem stellen Ransomware und Bedrohungsakteure mit staatlicher Unterstützung mittlerweile ein Risiko für jedes Unternehmen dar, und Angreifer gehen immer raffinierter vor, während die Transparenz Ihrer IT-Umgebung immer schwieriger zu fassen wird. Herkömmliche Netzwerksicherheitsmaßnahmen sowie Firewalls der nächsten Generation, die auf Deep Packet Inspection oder signaturbasierter Erkennung basieren, sind dabei nicht mehr in der Lage, mit der Menge an Traffic Schritt zu halten, die ein Rechenzentrum heutzutage erlebt. Sehen wir uns an, warum die richtigen Mikrosegmentierungstechniken die beste Technologie sind, um die Unzulänglichkeiten anderer alternativer Ansätze zur Netzwerksegmentierung zu beheben.

> Da Hybrid-Cloud-Umgebungen zur Norm geworden sind, verlangen sie bestimmte Voraussetzungen, die über die herkömmliche Netzwerksicherheit hinausgehen

Ältere Firewalls sind für den East-West-Traffic nicht geeignet

Wenn ein Unternehmen seine IT-Umgebungen segmentieren möchten, wird es vielleicht zunächst auf ältere Netzwerksicherheitssysteme zurückgreifen. Leider wurden diese Systeme dafür entwickelt, den North-South-Traffic, von Client zu Server, zu überwachen. Dazu gehört auch der Traffic, der von einer beliebigen externen Quelle in das Rechenzentrum gelangt. In jüngster Zeit ist jedoch der Traffic im Rechenzentrum, der sich von Server zu Server bewegt, in der Regel als East-West-Traffic bezeichnet, exponentiell angestiegen. Dies ist zum großen Teil auf die zunehmende Virtualisierung und konvergierte Infrastruktur wie Hypervisor, VPC und Container-basiertes Computing zurückzuführen.

Sicherheitsmaßnahmen am Netzwerkrand wie herkömmliche Firewalls schützen Ihr Unternehmen weder vor infizierten Geräten noch verhindern sie, dass Angreifer über den East-West-Traffic Fuß fassen können. Mit dem Aufkommen der TLS-Verschlüsselung und dem einfachen Verbergen von bösartigem Traffic, der über offene, legitime Anwendungsports läuft, können viele Angriffe selbst durch die Firewalls hindurch gelangen. Dadurch können Sie bestehende Sicherheitsverstöße nicht erkennen und beheben oder umleiten. Das bedeutet auch, dass es schwierig ist, die Verweildauer von Angreifern in Ihrem Netzwerk zu begrenzen. Je länger die Verweilzeit, desto katastrophaler ist der Angriff. Laut dem Active Adversary Playbook 2022 von Sophos betrug die durchschnittliche Verweildauer 15 Tage, während sie jedoch in kleinen Unternehmen und bestimmten Branchen mit bis zu 34 Tagen deutlich länger war.[1] Je länger ein Angreifer in Ihrem Netzwerk unentdeckt bleibt, desto mehr Schaden kann er anrichten.

Es ist einfach nicht möglich, so viele virtualisierte Firewalls einzusetzen, dass Tausende von Anwendungen oder Workloads geschützt werden können. Selbst wenn eine virtualisierte Lösung erstellt werden könnte, wäre es angesichts der sich ständig ändernden dynamischen Umgebungen, in denen wir heute arbeiten, unmöglich, diese zu verwalten oder zu steuern. Bei Hybrid Clouds beispielsweise ist der Einsatz herkömmlicher Firewalls noch schwieriger, da sie in verschiedenen Umgebungen arbeiten, Workloads über verschiedene Clouds hinweg verfolgen und von einem zentralen Punkt aus gesteuert werden müssen. Um diese Probleme zu lösen, wurden verschiedene Ansätze zur Netzwerksegmentierung entwickelt.

Drei zu berücksichtigende Segmentierungsansätze

Da sich Unternehmen bewusst sind, dass selbst virtuelle Firewalls nicht für den Schutz von Hybrid-Cloud-Rechenzentren geeignet sind, versuchen sie, die Segmentierung innerhalb der East-West-Infrastruktur auf drei grundlegende Arten anzuwenden. Wie bereits erwähnt, kann jeder Port oder Server mit jedem anderen kommunizieren, wenn strenge Segmentierungsrichtlinien und Sicherheitsmaßnahmen fehlen. Das bedeutet, dass ein Angreifer, der die Firewall eines Servers durchbricht, leicht auf eine beliebige Anzahl von anderen Servern im Netzwerk zugreifen kann. Die effektivste Möglichkeit, die Konnektivität zwischen Servern einzuschränken, ist die Segmentierung des Netzwerks. Es gibt drei grundlegende Arten der Netzwerksegmentierung, wobei die Mikrosegmentierung die Technologie ist, mit der Unternehmen zunehmend feiner abgestufte Richtlinien und Kontrollen durchsetzen können. Nutzer können die drei im Folgenden aufgeführten Arten von Segmentierungsrichtlinien kombinieren, um feiner abgestimmte Richtlinien für kritische oder riskante Anwendungen zu erstellen.

Umgebungssegmentierung

Mit diesem Ansatz werden verschiedene Umgebungen voneinander getrennt. Dadurch könnten Unternehmen beispielsweise den Entwicklungsbereich ihres Unternehmens von der Produktionsumgebung abgrenzen. Dies ist die erste entscheidende Phase in jeder Segmentierungsstrategie, auf die dann eine detailliertere Richtlinienerstellung folgen kann.

Anwendungssegmentierung

Im weiteren Verlauf der Segmentierung wird durch das „Ringfencing“ hochwertiger Anwendungen jede einzelne kritische Anwendung vom Rest des Netzwerks getrennt. Die besten Mikrosegmentierungslösungen ermöglichen sogar eine Steuerung auf Prozessebene.

Segmentierung nach Ebenen

Die engste Form der Segmentierung findet innerhalb der Anwendung selbst statt. Hier können Sie Richtlinien für die Verwaltung der Kommunikation zwischen Ebenen innerhalb desselben Anwendungsclusters erstellen, um beispielsweise den Traffic zwischen Webservern, Anwendungsservern und Datenbankservern zu kontrollieren. Auch eine Durchsetzung und Steuerung auf Prozessebene ist möglich, wenn Sie dies wünschen.

Netzwerksegmentierungsmethode – Netzwerksegmentierung über VLANs (Virtual Local Area Networks)

Die meisten Unternehmen setzen zunächst VLANs ein. Mit diesen virtuellen lokalen Netzwerken können Unternehmen jedem Segment einen eigenen Kommunikationspfad zuweisen, entweder über eine Firewall oder über ACLs (Access Control Lists) auf dem Router selbst. Obwohl VLANs eine gängige Wahl für die Netzwerksegmentierung sind, lauern unter der Oberfläche einige Probleme. Lassen Sie uns dem auf den Grund gehen und überlegen, warum VLANs für heutige Sicherheitsanforderungen eine suboptimale Wahl sind.

Es liegt auf der Hand, warum viele Unternehmen VLANs als Segmentierungsmethode wählen. Sie kann mit der vorhandenen Architektur durchgeführt werden, wodurch sie kostengünstig und einfach zu implementieren erscheint. Es handelt sich jedoch um einen sehr starren und komplexen Segmentierungsansatz, der teuer in der Wartung sein kann und mit Ausfallzeiten bei der Implementierung einhergeht.

Bevor Sie VLANs nutzen können, müssen Sie sich mit den Servern und Abhängigkeiten in jedem Segment vertraut machen und dann die gewünschte Konfiguration für die Netzwerk-Switches erstellen, die Sie segmentieren. Da diese Arbeiten von Netztechnikern durchgeführt werden und oft mehrere Standorte betreffen, kann das mehrere Tage dauern und einen unverhältnismäßig hohen Zeit- und Kostenaufwand verursachen. Der Traffic kann während der Konfiguration unterbrochen werden oder langsam sein.

In einer Zeit, in der Agilität ein wichtiger Wettbewerbsvorteil und vielleicht sogar ein Muss ist, können hohe Kosten und ein langsames Tempo bei der Umsetzung von Veränderungen katastrophale Folgen für Ihren geschäftlichen Erfolg haben. Laut Forbes ist Anpassungsfähigkeit der Schlüssel zum Überleben: „Umbrüche sind nicht neu, aber die Geschwindigkeit, die Komplexität und die globale Dimension der Umbrüche haben ein Ausmaß erreicht, das wir noch nie zuvor gesehen haben. ... Nicht die größten oder finanziell stabilsten Unternehmen werden überleben, sondern diejenigen, denen es gelingt, sich an das exponentiell beschleunigte Tempo des Wandels anzupassen.“[2]

Sie müssen erkennen, dass VLANs nicht für die Segmentierung entwickelt wurden. Sie wurden ursprünglich zur Verringerung von Engpässen konzipiert und die Nutzung dieser Technologien zur Steuerung der Kommunikation ist keine intelligente Art, die vorhandene Technologie zu nutzen – sie ist in vielerlei Hinsicht eine Zweckentfremdung. Angesichts dessen überrascht es nicht, dass bei der Segmentierung mithilfe von VLANs einige Einschränkungen zu beachten sind.

- **Cloud-Technologie** – VLANs und andere herkömmliche Richtlinien zur Netzwerksegmentierung können nicht auf die Cloud ausgedehnt werden. Wenn Sie ISFWs (Internal Segmentation Firewalls) oder ACLs verwenden, um zu steuern, welche Nutzer auf Netzwerksegmente zugreifen können, müssen Sie sich wahrscheinlich auf SDN (Software-Defined-Networking) für die Cloud verlassen. Dies geschieht in der Regel durch Drittanbieter von Software, die virtuelle Firewalls oder Subnetze verwenden.
- **Container** – Die Sicherheit ist nach wie vor ein großes Problem, da Container in IT-Umgebungen weit verbreitet sind. Da jeder Container auf demselben Kernel ausgeführt wird, kann ein Exploit alle Container gefährden. Die Isolation ist ein ständiger Kampf und kann nicht mit den üblichen Netzwerksegmentierungsmethoden gelöst werden.
- **Protokolleinschränkungen** – Der Grenzwert für VLANs liegt bei 4.096 Segmenten, was die Möglichkeit einer angemessenen Segmentierung in großen Rechenzentren einschränkt. Bei granularen Segmentierungsansätzen gibt es diese Einschränkung nicht.

Netzwerksegmentierung zur Anwendungssegmentierung – Einführung von Layer 4-Kontrollen

Viele dieser Probleme wurden durch die Segmentierung von Anwendungen mithilfe von Sicherheitsgruppen in Cloudumgebungen und Hypervisor-basierten Firewalls für virtualisierte On-Premise-Umgebungen verringert. Die herkömmliche Anwendungssegmentierung implementiert Layer 4-Kontrollen, mit denen Sie Service-Tiers voneinander isolieren können, sodass eine Anwendung über eine sichere Grenze verfügt. Jede Ebene ist auf die Zugriffsstufe beschränkt, die sie für volle Funktionalität benötigt, mehr nicht. Es besteht eine klare Trennung zwischen den Ebenen einer einzelnen Anwendung, und die Gefahr einer potenziellen Gefährdung wird auf ein Minimum beschränkt.

Denken Sie an die Ebenen, die Sie in einem Standardunternehmen finden können, von Load Balancer und Datenbanken bis hin zu Anwendungsservern innerhalb/außerhalb Ihrer eigenen DMZ. Wenn diese Ebenen separat verwaltet werden, kann jede ihre eigenen Sicherheitsregeln und -funktionen haben. Die Anwendungssegmentierung kann Unternehmen dabei unterstützen, die richtigen Kontrollen für jede Ebene zuzulassen, ihre vertraulichen Informationen und Kommunikationen einzuschränken und gleichzeitig einen breiten Nutzerzugang zu ermöglichen, wo dies erforderlich ist. So kann ein Unternehmen beispielsweise bestimmte Datenbanken an der Kommunikation mit dem Internet hindern oder sicherstellen, dass ein Angreifer, wenn er einen einfachen Load Balancer außer Gefecht setzt, nicht auf sensible Informationen auf der Datenbankebene zugreifen kann.

Wenn eine Lösung granularer wird, ermöglicht die Anwendungssegmentierung einem Unternehmen, ein ganzes Anwendungscluster von anderen Bereichen des Unternehmens zu trennen. Wie bereits erwähnt, verringert sich dadurch die Angriffsfläche und die Fähigkeit der Angreifer, laterale Bewegungen von einer Ebene zur anderen durchzuführen.

Die Grenzen von Layer 4-Kontrollen

Der herkömmlichen Anwendungssegmentierung kann es an Tiefe mangeln, was sich direkt auf Ihre Sichtbarkeit auswirkt. Auf der Netzwerkebene, wo das Routing stattfindet, werden Daten zwischen Systemen verschoben, indem IP-Adressen und Protokolle zugewiesen werden, die den Weg der Datensegmente zu ihrem Ziel genau beschreiben. Bei der Anwendungssegmentierung werden häufig Layer 4-Netzwerkkontrollen verwendet, wobei der Schwerpunkt auf der Art und Weise liegt, wie die Daten selbst bereitgestellt werden. Größere Datensegmente werden in kleinere Segmente oder Blöcke unterteilt, die dann am Zielort wieder zusammengesetzt werden können. Durch die Datenflusssteuerung kann dieser Prozess dynamisch beschleunigt oder verlangsamt werden, wenn die Geräte, die die Informationen senden oder empfangen, dies erforderlich machen.

In der heutigen Bedrohungslandschaft sind Kontrollen auf diesen Ebenen unerlässlich, aber in bestimmten Fällen möchten Sie vielleicht die Möglichkeit haben, Richtlinien auf einer noch detaillierteren Ebene festzulegen. Angreifer haben bewiesen, dass sie IP-Adressen fälschen und „Huckepack“ unter Ausnutzung zulässiger Ports in das Netzwerk eindringen können. Darüber hinaus beschränkt der Layer 4-Schutz nicht die lateralen Bewegungen innerhalb einer Anwendung oder einer Ebene, wodurch die Angriffsfläche noch immer größer sein kann, als Sie möchten.

Eines der besten Beispiele für die Notwendigkeit von Kontrollen, die mehr Details als Layer 4 bieten, sind Compliance-Initiativen. Herkömmliche Methoden der Anwendungssegmentierung haben es Unternehmen bis zu einem gewissen Grad ermöglicht, bestimmte Compliance-Vorschriften zu erfüllen, wie z. B. die Trennung von CDE für PCI-DSS oder den Schutz von PHI für HIPAA. Obwohl Layer 4-Techniken in der Vergangenheit als wirksame Mittel zum Compliance-Nachweis akzeptiert wurden, hat die Realität gezeigt, dass dies möglicherweise nicht ausreicht. Laut dem „2022 Payment Security Report“ von Verizon erfüllen nur 43 % der Unternehmen „alle Compliance-Anforderungen“.[3] Schlimmer noch: Selbst 100 % Compliance bedeutet nicht 100 % Sicherheit. Layer 4-Kontrollen decken zwar Ihre Compliance-Umgebungen ab, reduzieren die Angriffsfläche jedoch nicht genug, um die Sicherheit entscheidend zu verbessern. Punkt. Angreifer können einen offenen Layer 4-Port zwischen zwei Ebenen mit einem separaten Prozess (Layer 7) nutzen und sich nehmen, was sie wollen.

Segmentierung im Dunkeln – mangelnde Transparenz bei der Netzwerk- und Anwendungssegmentierung

Unternehmen stellen fest, dass die Anwendungssegmentierung zwar zweifellos ein Schritt in die richtige Richtung ist, aber nicht weit genug geht, um alle Probleme zu lösen, die sich bei einem groben Segmentierungsansatz ergeben. Eine weitere Herausforderung, die noch angegangen werden muss, ist die Sichtbarkeit. Eine präzise Echtzeitübersicht Ihres Netzwerk ist in jeder Phase des Segmentierungsprozesses von entscheidender Bedeutung, was bei vielen Segmentierungsansätzen jedoch nicht berücksichtigt wird.

Bevor Sie beginnen, sollten Sie die Anwendungsabhängigkeiten visualisieren, damit Sie genaue Richtlinienregeln erstellen können. Nach der Segmentierung benötigen Sie den Nachweis, dass Ihre Segmentierung wie vorgesehen funktioniert, nicht nur um zu bestätigen, dass Ihre Sicherheit immer gewährleistet ist, sondern auch um bei Bedarf die Einhaltung gesetzlicher Vorschriften nachzuweisen.

Ohne Echtzeit- und Verlaufstransparenz gibt es keinen Nachweis für Sie selbst oder für Dritte und Aufsichtsbehörden. Die manuelle Nachweiserfassung ist zeitaufwändig und kostspielig in der Verwaltung, und es besteht immer die Möglichkeit von Konfigurations- und anderen Fehlern. Eine Segmentierungslösung, die diese Art von Transparenz nicht bieten kann, ist einfach nicht ausreichend.

Mikrosegmentierung bis zu Layer 7 – die Anwendungsebene

Im Gegensatz dazu ist die Segmentierung auf Anwendungsebene (Layer 7) sehr effektiv bei der Begrenzung lateraler Bewegungen, selbst innerhalb eines Anwendungsclusters. Auf Layer 7 werden Netzwerkdienste in das Betriebssystem integriert. Protokolle wie HTTP, FTP, TFTP und SMTP sind alle Layer 7-Protokolle. Die neuesten Fortschritte in der Mikrosegmentierungstechnologie ermöglichen eine weitaus tiefere Segmentierung auf dieser Ebene als andere Lösungen, so dass Ihr Unternehmen die Aktivitäten auf Layer 7 ebenso wie auf dem herkömmlichen Layer 4 visualisieren und steuern kann. Das bedeutet, dass Unternehmen sich bei der Konfiguration ihrer Richtlinien nicht auf IP-Adressen und Ports verlassen müssen, sondern spezifische Prozesse und Datenflüsse verwenden. Auf diese Weise können die Vorteile der Segmentierung nicht nur für eine bestimmte Ebene oder ein Anwendungscluster genutzt werden. Sie können auch potenzielle Bedrohungen erkennen, und sei es nur ein falscher Hash, selbst wenn der Angreifer einen autorisierten Prozess oder Pfad spiegelt.

Bei der Erstellung von Richtlinien ermöglicht die Segmentierung auf Layer 7 sehr spezifische Zulassungsregeln oder Ausnahmen, bei denen nur exakte Prozesse oder Datenflüsse zulässig sind, während die gesamte andere Kommunikation standardmäßig blockiert wird. Hierzu kann die Isolierung von Daten zwischen Systemen erforderlich sein, wobei aber dennoch die Kommunikation für notwendige oder geschäftskritische Datenflüsse zugelassen wird.

Die besten Mikrosegmentierungslösungen bieten die Transparenz, die Unternehmen für mehr Agilität benötigen

Mit Agents für jeden Workload – Hypervisor- oder VPC-basierte Container, Bare-Metal-Server oder sogar IoT/OT-Systeme – kann eine ganzheitliche Mikrosegmentierungslösung Ihrem Unternehmen eine vollständige visuelle Übersicht der gesamten IT-Infrastruktur bereitstellen. Bei wirklich intelligenten Lösungen umfasst dies Rechenzentren, Cloud-, Multicloud- und Hybrid-Cloud-Umgebungen sowie Remote-Geräte. Herkömmliche Lösungen zur Anwendungssegmentierung haben Schwierigkeiten, diese Komplettübersicht zu bieten, da sie in der Regel eine Kombination aus netzwerkzentrierten Technologien verwenden.

Eine umfassende visuelle Übersicht Ihrer Umgebung sollte Ihnen außerdem zeigen, welche Sicherheitsrichtlinien in Echtzeit implementiert und durchgesetzt werden. Ihre Techniker und Sicherheitsexperten sollten in der Lage sein, mögliche Sicherheitslücken in Ihrer Richtlinienabdeckung auf einen Blick zu erkennen oder zu sehen, welche zusätzlichen Richtlinien sie implementieren oder von Grund auf neu erstellen müssen.

Diese Transparenz ermöglicht es Ihrem Unternehmen auch, sich im Voraus auf neue Software oder Updates für vorhandene Systeme vorzubereiten, indem Regeln für die Segmentierung aktualisierter oder neuer Anwendungen erstellt werden, bevor diese für die Bereitstellung bereit sind. Sobald die Updates aktiv sind, erhalten Ihre Sicherheitsteams die Echtzeitinformationen, die sie benötigen, um Anwendungsaktivitäten zu erkennen und zu beheben, die außerhalb der Norm liegen. So wird sichergestellt, dass Sicherheitsrisiken nicht unbemerkt bleiben oder zu aktiven Exploits werden. Im Anschluss daran stehen Ihrem Unternehmen kontextbezogene Tools zur Verfügung, um einen Vorfall mit historischen Daten zu vergleichen und die Umgebung, in der die Anomalie auftrat, genau zu verstehen. Richtlinien können verschärft werden, die Segmentierung kann angepasst werden, und Sie können den Vorfall zur Einhaltung von Compliance-Vorschriften oder für weitere Untersuchungen detailliert erfassen.

Setzen Sie auf Zero Trust

Ein weiterer Vorteil der Mikrosegmentierung ist die Fähigkeit, das Zero-Trust-Sicherheitsmodell zu nutzen. Obwohl die Idee von Zero Trust bereits 2010 von Forrester geprägt wurde, tragen Technologien wie die Mikrosegmentierung dazu bei, das Konzept in die Realität umzusetzen, und Forscher und Sicherheitsexperten betonen weiterhin seine Vorteile.[4]

Die Idee ist einfach: Kein Traffic oder Nutzer ist vertrauenswürdig, bis dies nachgewiesen und genehmigt ist, unabhängig davon, ob es sich um eine externe oder eine interne Quelle handelt, und zwar bei jedem Verbindungsversuch. Die drei von Forrester geprägten Zero-Trust-Grundprinzipien[5] werden alle durch starke, fein abgestufte Richtlinien für die Mikrosegmentierung unterstützt:

- Alle Nutzer gelten standardmäßig als nicht vertrauenswürdig
- Eine umfassende Sicherheitsüberwachung ist implementiert
- Der Zugriff mit geringstmöglichen Berechtigungen wird durchgesetzt

Zero Trust steht praktisch am anderen Ende des Spektrums der reinen Netzwerksicherheit, bei der Sie die Eingänge Ihres Schlosses mit einem tiefen Graben schützen und davon ausgehen, dass alles, was sich im Inneren befindet, für den Zutritt freigegeben ist. Da die meisten Unternehmen nicht mehr über ein geschlossenes Netzwerk oder Rechenzentrum verfügen, ist die Idee eines solchen „Schlosses“ jedoch überholt, und eine Strategie der geringstmöglichen Berechtigungen wie Zero Trust ist der einzige Weg, um sicherzustellen, dass Sie jederzeit wissen und kontrollieren können, wem Sie Zugang gewährt haben.

Zukunftssicherheit für Ihr Unternehmen durch Mikrosegmentierung

Die Netzwerksegmentierung kann sicherlich über einen Ansatz hinausgehen, der sich nur auf die Netzwerkgrenzen beschränkt, und die Segmentierung von Umgebungen und Anwendungen bis zu Layer 4 sind wichtige Schritte beim Aufbau Ihrer Segmentierungsstrategie. Da IT-Umgebungen jedoch immer komplexer werden, benötigen Sie möglicherweise eine Segmentierungslösung, die eine noch feiner abgestufte Segmentierung nach Ebenen und die Durchsetzung auf Prozessebene bis Layer 7 in den Anwendungs- und Tier-Phasen bietet.

Moderne Unternehmen haben eine in sich abgeschlossene Infrastruktur hinter sich gelassen. Sie verlassen sich meist auf Technologien wie SDN in der Cloud, Container oder Bare-Metal-Hypervisoren. Sie arbeiten in verschiedenen Regionen und physischen Rechenzentren.

Der einzige Weg, sich vor externen und internen Bedrohungen zu schützen, ist eine Lösung, die den gesamten Traffic überprüft und kontrolliert, sowohl East-West als auch North-South, und Ihnen – bei kritischen oder riskanten Anwendungen – mehr Transparenz bietet, als Sie nur mit Layer 4 erzielen können. Durch die Mikrosegmentierung bis zu Layer 7 auf Anwendungs- oder Tier-Ebene erhalten Sie einen genauen Überblick über Ihre gesamte IT-Umgebung und können problemlos detaillierte Sicherheitsrichtlinien nach dem Zero-Trust-Modell erstellen und durchsetzen. Eine gute Mikrosegmentierungslösung wird Sie nicht vor die Wahl zwischen Sicherheit und Agilität stellen. Entscheiden Sie sich für die Lösung, die Ihnen die beste Gesamtsicherheit für Ihr Unternehmen bietet.

Weitere Informationen finden Sie unter akamai.com/guardicore.

1 Shier, John. 2022. „The Active Adversary Playbook 2022.“ Sophos. 7. Juni.

2 Gonda, Rob. 2018. „Adaptability Is Key To Survival In The Age Of Digital Darwinism.“ Forbes. 24. Mai.

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. Juni 2022. „Best Practices For Zero Trust Microsegmentation.“ Forrester. April.

5 Holmes, David und Jess Burn. Jan. 2022. „The Definition Of Modern Zero Trust.“ Forrester. April.