Softwarebasierte Segmentierung

Ein Inside-out-Ansatz für sorgenfreie Sicherheit

INHALTSVERZEICHNIS

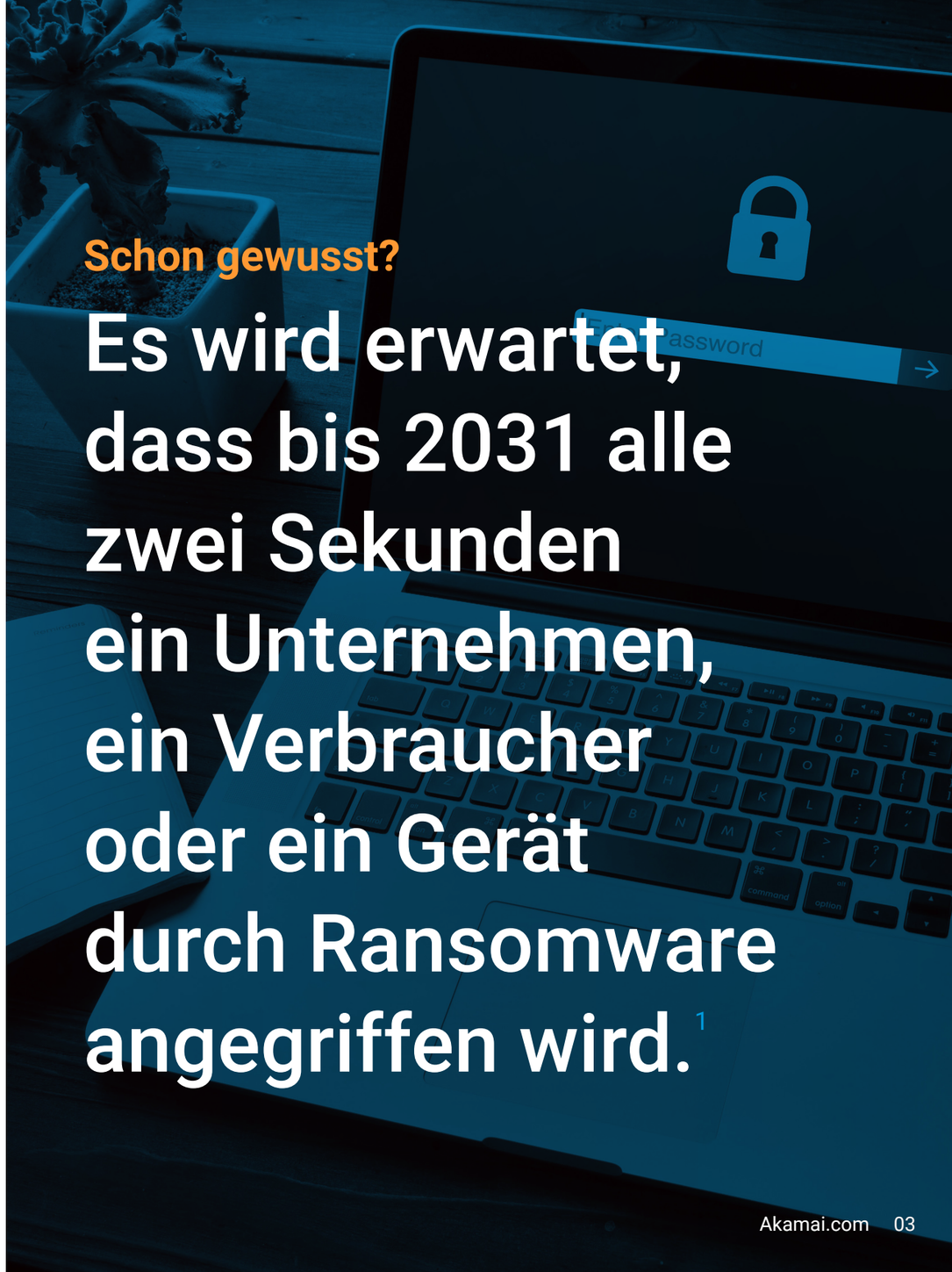
Lassen Sie die herkömmlichen Firewalls hinter sich

Wir verstehen Sie. Sie haben Ihre alten lokalen Firewalls satt. IT-Umgebungen und Sicherheitsvorgaben haben mit ihrem ursprünglichen Zweck nicht mehr viel zu tun. Gleichzeitig hat sich die Welt der Cybersicherheit weiterentwickelt. Die Angriffsmethoden sind raffinierter geworden, und es gibt mehr Cyberkriminelle denn je. Eine viele Jahrzehnte alte Anwendungsarchitektur kann den neuesten Malwares, Botnet-Angriffen, Phishing-Methoden, dem Social Engineering und der Datenerpressung einfach nicht mehr standhalten.

Aber trotz der vielen Probleme, die sie verursachen – sie sind unter anderem teuer, unflexibel und intransparent –, ist es so, dass herkömmliche Firewalls nicht so bald verschwinden werden. Sie erfüllen eine wichtige Funktion am Netzwerkrand mit der Handhabung des North-South-Traffic und bilden einen Schutzwall um das Unternehmen.

Aber Firewalls können keinen East-West-Traffic in unseren Rechenzentren und in der Cloud steuern.

Hier kommt die softwarebasierte Segmentierung ins Spiel.



Gelöst!

Drei Probleme mit herkömmlichen Firewalls

1. Das Problem: **Mangelnde Transparenz**

   Die mangelnde Transparenz der Datenbewegungen erschwert die Implementierung und Aufrechterhaltung von Regeln. Deswegen haben Firewalls oft sehr lange Regelsätze und viele Regeln, die zu tolerant oder nicht einmal nötig sind.

Die Lösung

Suchen Sie nach Lösungen, die visuelles Mapping, Ressourcenklassifizierung und Mapping der Anwendungsabhängigkeiten mit dem Aufstellen und Management von Regeln kombinieren.

Gelöst!

Drei Probleme mit herkömmlichen Firewalls

2. Das Problem: Firewalls sind schwer zu warten

Application Owner und Firewall-Admins kennen oft die geeigneten IP-Ports und Protokolle nicht, die kommunizieren müssen. Das Verwalten von Firewalls wird so zu einem iterativen Fehlerbehebungsverfahren.

Die Lösung

Statt auf Richtlinien, die sich auf feste Netzwerk-„Leitungen“ wie IPs und Ports beziehen, sollten sie auf aussagekräftigen Attributen wie dem von einer Anwendung verwendeten Prozess, voll qualifizierten Domainnamen (FQDN) und der Nutzeridentität basieren. Auf diese Weise bleiben die Attribute erhalten und Ihre Richtlinien funktionieren weiterhin, auch wenn Sie eine Änderung an Ihrem Rechenzentrum vornehmen oder Ihren Workload in die Cloud migrieren.

Gelöst!

Drei Probleme mit herkömmlichen Firewalls

3. Das Problem: Firewalls sind nicht agil genug

Jegliche Änderung, die an einer Firewall vorgenommen wird, erfordert normalerweise eine geplante Ausfallzeit. Dies bedeutet: Wenn ein Application Owner eine Änderung vornehmen muss, muss er eine Woche oder länger darauf warten, dass die Änderung während eines Wartungsfensters geprüft und implementiert wird.

Die Lösung

Moderne IT-Unternehmen haben von den Änderungsfenstern auf DevOps-Modelle umgestellt, bei denen Anwendungen ständig aktualisiert werden. Finden Sie eine Technologielösung, die automatisiert werden kann, indem Sie dieselben DevOps-Tools verwenden, die Sie für die Anwendungen selbst benutzen. Auf diese Weise entwickelt sich das Sicherheitskonzept analog zu den Anwendungen kontinuierlich weiter.

Kombinieren Sie das Alte mit dem Neuen

Sehen wir uns die herkömmliche Methode einmal genauer an. Sie ist kompliziert. Und sie ist nicht anpassungsfähig. Bei der bisherigen Herangehensweise in Bezug auf die Verwaltung herkömmlicher Firewalls basiert die Segmentierung auf dem Standort. Und dieser kann nicht ohne Weiteres geändert werden. Er basiert normalerweise auf einer fest codierten IP-Adresse oder wird an ein Rechenzentrum weitergeleitet. Dies bedeutet, dass die Daten, die Sie schützen wollen, physisch hinter die Firewall bewegt werden müssen. Dieser Vorgang ist ressourcenintensiv, risikoreich und langsam. Cloudmigration? Transparenz? Adäquate Sicherheit? Vergessen Sie's.

Lassen Sie Ihre herkömmlichen Firewalls an Ort und Stelle. Atmen Sie tief durch und machen Sie sich bereit für etwas Neues. Softwarebasierte Segmentierung kann einfach zusätzlich zu Ihren vorhandenen Firewalls implementiert werden, und sie ist anpassbar. Mit softwarebasierter Segmentierung können Sie Ihre Umgebung, Ihr Rechenzentrum und Ihr Netzwerk tatsächlich verändern und Richtlinien festlegen, die auf dem basieren, was Sie sehen. Und der Workload und die Richtlinien können überall sichtbar sein, zum Beispiel in der Cloud oder im Rechenzentrum – wo auch immer. Außerdem können Sie Ihre Sicherheitsrichtlinien anwenden und anpassen, ohne Änderungen an dem Netzwerk vorzunehmen und ohne eine Ausfallzeit des Systems in Kauf zu nehmen.

Transparenz für interne Segmente

Würden Sie auf etwas vertrauen, das Sie nicht sehen können? Bestimmt nicht. Aber genau das tun Sie, wenn Sie Sicherheitsrichtlinien hinter einer Firewall festlegen. Sie können nicht wirklich sehen, was sich im Inneren befindet. Es ist so, als würden Sie auf ein Gebäude blicken, aber nicht sehen, wer sich darin aufhält.

Bei einer softwarebasierten Segmentierung wird nichts dem Zufall überlassen. Sie zerlegt die einzelnen Elemente, sodass Sie sich vollkommen im Klaren über alle Aktivitäten sind, in die Ihre Workloads involviert sind. Sobald Sie wissen, was sich im Inneren Ihrer Umgebung befindet, können Sie einen Plan erstellen und die Segmente basierend auf Ihren spezifischen Anwendungsfällen in sinnvolle und effiziente Einheiten zerlegen.

Sicherheit jenseits des Netzwerkrands

Herkömmliche Firewalls sind ganz einfach nicht auf Veränderung ausgelegt. Sie erfüllen zwar am Netzwerkrand wichtige Aufgaben, beispielsweise DDoS-Schutz und das Filtern und Prüfen von Traffic. Sicherheit innerhalb eines Netzwerks ist mit ihnen allerdings nicht ohne Weiteres zu gewährleisten. Warum? Sie wurden als natürliche Choke Points entwickelt. Das bedeutet, dass jede Segmentierungsmaßnahme betriebliche Hindernisse mit sich bringt, wie zum Beispiel, dass Netzwerke und Anwendungen geändert und entfernt werden müssen. Dies ist mühsam und ressourcenintensiv.

Softwarebasierte Segmentierung kann diese betrieblichen Herausforderungen überwinden und es Ihnen ermöglichen, Ihre Sicherheitspraktiken über Endpunkte und den Netzwerkrand hinaus fortzuführen. Erstens bietet sie einen verteilten Firewall-Ansatz (im Gegensatz zu einem Choke Point). Zweitens ist sie Workload-zentriert. Das bedeutet, dass Sie Daten vom Hostsystem sammeln und sie dann für Ressourcenklassifizierung und einen detaillierteren Ansatz für Regeln verwenden können, wie Content und Richtlinien auf Prozessebene. Insgesamt ist die softwarebasierte Segmentierung eine anpassungsfähigere, detailliertere Möglichkeit zum Schutz von kritischen Ressourcen in Ihrem Netzwerk und erfordert weniger Mühe und Ressourcen als Firewalls.

Vier Grundlagen der Segmentierung

Segmentierung ist heute wichtiger denn je. Die Angriffsfläche nimmt zu. Komplexe Angriffe wie Ransomware bewegen sich nach dem Eindringen lateral fort. Daher müssen Sie über die Anwendungsabhängigkeiten jenseits des Netzwerkrands nachdenken. Segmentierung ist aber kein Verfahren, das mit einem Eingriff erledigt ist.

Im Folgenden stellen wir Ihnen die vier gängigen Segmentierungsarten vor und erklären Ihnen, wie sie sich unterscheiden und warum sie nützlich sind.

1. Umgebungssegmentierung

teilt Systeme in verschiedene Entwicklungsumgebungen auf wie Entwicklung, QS, Staging und Produktion. Dies ist eine weit gefasste Version der Segmentierung, bei der das Endziel die Trennung in verschiedene Umgebungen ist. So kann gewährleistet werden, dass der Zugriff ausschließlich auf die relevanten Nutzer und Anwendungen beschränkt ist. Viele Compliance-Initiativen erfordern die Sicherheit, dass nicht zur Produktion gehörende Systeme nicht auf Produktionssysteme zugreifen können.

2. Netzwerksegmentierung

ist eine Architekturpraxis, bei der ein Netzwerk in verschiedene Unternetzwerke aufgeteilt wird, von denen jedes ein eigenes kleineres Netzwerksegment ist. Netzwerksegmentierung gibt IT-Bedienern ein Tool an die Hand, um den Netzwerk-Traffic besser zu kontrollieren, die Performance zu verbessern und die Sicherheit zu erhöhen.

3. Mikrosegmentierung

ist eine detailliertere Form der Segmentierung, die verwendet wird, um Workloads voneinander zu trennen und sie einzeln zu sichern. Dies umfasst die Fähigkeit, Segmentierungsregeln für Elemente wie Prozesse, Container, Nutzer, Domainnamen und Geräte festzulegen. Dieser Ansatz ist bei der Kontrolle von East-West-Traffic und beim Schutz vor lateraler Netzwerkbewegung unübertroffen.

4. Identitätsbasierte Segmentierung

ist weitreichender als die Fähigkeit der Mikrosegmentierung, einzelne Endpunkte, Geräte, Workloads oder Container zu schützen, indem sie dynamische Regeln ermöglicht, die Identitäten bewertet. Das kann der Nutzer, das Gerät oder der Kontext sein. Darauf basierend wird festgelegt, ob eine Kommunikation erlaubt wird oder nicht. Richtlinien für identitätsbasierte Segmentierung können – statt nur auf der IP-Adresse oder dem Port – auf detaillierten Einstellungen basieren wie Tags, OS-Typ oder Anwendungsmerkmalen.

Mythos versus Realität: Fünf Mythen über Segmentierung und ihre Widerlegung

Mythos 1

Segmentierungsprojekte sind zu komplex und dauern zu lange.

Fakt: Da sie auf Transparenz und einem klaren Verständnis der Vorgänge in Ihrer Umgebung aufbaut, dauert die Segmentierung nicht mehr Monate, sondern nur noch Wochen oder sogar Tage. Moderne Segmentierungstechnologien können auch KI verwenden, um die Prozesse noch weiter zu beschleunigen.

Mythos 2

Segmentierungsprojekte erfordern Änderungen der Netzwerkinfrastruktur und Ausfallzeiten.

Fakt: Softwarebasierte Segmentierung entkoppelt die Sicherheit von der Infrastruktur, sodass Segmentierung unabhängig von der zugrunde liegenden Infrastruktur durchgeführt werden kann, ohne dass Änderungen oder Ausfallzeiten erforderlich sind.

Mythos 3

Segmentierungsblocks legitimieren Traffic in meinem Netzwerk.

Fakt: Durch das Visualisieren Ihrer Umgebung und die Verwendung von softwarebasierten Segmentierungsrichtlinien können Sie den Effekt sehen, den diese Richtlinien auf Ihre geschäftlichen Aktivitäten haben, bevor die Echtzeitdurchsetzung aktiviert wird.

Mythos 4

Segmentierung verhindert den Zugriff durch Nutzer und führt zu unnötiger Latenz.

Fakt: Es werden verteilte, softwarebasierte Segmentierungsrichtlinien verwendet, anstatt den gesamten Traffic durch bestimmte Choke Points einer Firewall zu leiten. Dadurch werden Engpässe im Netzwerk vermieden. Präzisere Richtlinien, die anwendungs- und identitätsorientiert sind, reduzieren das Risiko unbeabsichtigter Zugangsprobleme.

Mythos 5

Ich kann in der Cloud nicht mehr die gleichen Segmentierungstools verwenden wie in meiner lokalen Umgebung.

Fakt: Wenn Sie die Segmentierungsrichtlinien von der Infrastruktur abkoppeln, können in der Cloud dieselben Richtlinien verwendet werden wie im Rechenzentrum.

Akamai

Geringeres Risiko im Inneren

Es wird zu Angriffen kommen. Und sie können Ihr Unternehmen lahmlegen, Ihre Daten kompromittieren, Ihre Marke beschädigen und Sie Millionen kosten.

Glauben Sie immer noch, dass Firewalls alles schaffen können? Da liegen Sie möglicherweise falsch. Sobald ein Angreifer in ein Netzwerk, eine Umgebung oder ein Rechenzentrum eingedrungen ist, wird er sich lateral durch das Netzwerk bewegen, um Daten zu stehlen und Schaden anzurichten, indem er zum Beispiel die Kontrolle über Anwendungsserver übernimmt oder sich Zugriff auf Datenbankserver verschafft.

Tatsächlich unternehmen heutzutage 70 % aller Angreifer Versuche lateraler Netzwerkbewegungen.[2]

Während Firewalls laterale Netzwerkbewegungen als legitimen Traffic innerhalb des Netzwerks wahrnehmen, werden sie durch die softwarebasierte Segmentierung frühzeitig unterbunden. Als kritische Komponente für Ihr Sicherheitsprogramm erlaubt Ihnen die softwarebasierte Segmentierung, laterale Netzwerkbewegung zu verhindern. Im Falle eines Angriffs erschwert sie dem Angreifer außerdem die Navigation in der Umgebung. Sie haben die Möglichkeit, Daten und kritische Anwendungen zu schützen, die Verweilzeit zu reduzieren und den Angreifer aufzuspüren. Dieser Ansatz ist besser skalierbar sowie leicht zu verwenden und ermöglicht Ihnen die schnelle Implementierung einer Segmentierung, ohne Änderungen an Ihrem Netzwerk oder Ihren Systemen vornehmen zu müssen.

Zero Trust muss nicht kompliziert sein.

Bei Zero Trust geht es darum, wer in Bezug auf wen was tut und wie. In anderen Worten: Es geht um explizite Kontrolle darüber, wer innerhalb Ihres Netzwerks was tut.

Wenn Sie einem Nutzer Zugriff auf sämtliche Inhalte des Netzwerks gewähren, schenken Sie ihm automatisch zu viel Vertrauen und setzen damit Ihr gesamtes Unternehmen einem Risiko aus. Zunächst einmal machen Mitarbeiter oft Fehler, was die Sicherheit ernsthaft gefährden könnte. Manche haben sogar die Absicht, dem Unternehmen zu schaden.

Außerdem sind abgesehen von VPN-Netzwerken und Geräten viele Einstiegspunkte in das Rechenzentrum vorhanden, die Sie in Erwägung ziehen sollten. Angreifer können beispielsweise durch den Produktionsserver (wie beim Angriff auf SolarWinds), eine vulnerable internetseitige Anwendung oder ein vulnerables VPN in das Netzwerk gelangen. In diesem Fall vertrauen Sie nur deswegen auf einen Server, weil er sich innerhalb des Netzwerks befindet. In der Praxis kann der Angreifer allerdings auf alles zugreifen und sich ohne Einschränkungen lateral bewegen.

Um Zero Trust in Ihrem Produktionsnetzwerk zu erreichen, müssen Sie alle Aktivitäten blockieren, die nicht explizit genehmigt sind.

Dazu sind herkömmliche Firewalls auf einem detaillierten Niveau schlicht und einfach nicht in der Lage, weil dies das Identifizieren von Attributen auf einem tiefergehenden Level als IP-Adressen und Ports erforderlich macht.

Im Gegensatz dazu können Sie mithilfe der softwarebasierten Segmentierung wirklich sehen, was im Detail geschieht, und präzise, für Menschen verständliche Richtlinien aufstellen, die die Identität miteinbeziehen.

Ihre Zero-Trust-Checkliste: Sechs Möglichkeiten, um explizite Kontrolle zu erhalten

Halten wir es einfach. Vertrauen sollte auf der Größe des Segments basieren. Beim Schutz von kritischen Daten, Ressourcen und Anwendungen lautet die Devise: Je kleiner das Segment, desto besser. Im Folgenden finden Sie sechs Schritte, wie Sie Zero Trust auch ohne operative Komplexität erreichen.

1 Identifizieren Ihrer sensiblen Daten durch die Verwendung von Visualisierungslabels.

2 Visualisieren der Bewegungen Ihrer sensiblen Daten mithilfe der automatisierten Abbildung von Abläufen und Abhängigkeiten.

3 Entwerfen Ihrer Zero-Trust-Mikroperimeter mithilfe der richtigen Tools für die schnelle Definition aller Segmentierungs- oder Mikrosegmentierungsrichtlinien.

4 Kontinuierliche Überwachung Ihres Zero-Trust-Ökosystems durch Echtzeitüberwachung und -analysen.

5 Automatisierung und Orchestrierung der Sicherheit mit APIs und Technologieintegrationen.

6 Maßnahmen treffen, um jemanden oder etwas als nicht vertrauenswürdig kategorisieren zu können, sodass Sie bei einem Angriff ein Gerät durch voreingestellte Attribute ganz einfach als nicht vertrauenswürdig einstufen können, unabhängig von Nutzer oder Segment.

Zusammenfassung

Jetzt fragen Sie sich wahrscheinlich, wie Sie sich von Ihren alten Lösungen trennen können, um Ihre Sicherheitsstrategie innerhalb Ihres Netzwerks zu verbessern.

Gar kein Problem.

Lassen Sie Ihre herkömmlichen Firewalls an Ort und Stelle. Sie eignen sich gut für den Schutz am Netzwerkrand. Aber da hört es auch schon auf.

Das Wichtigste befindet sich im Kern Ihres Unternehmens: die digitalen Ressourcen, Daten und Anwendungen jenseits des Netzwerkrandes. Diese stellen sozusagen das Herzstück der Infrastruktur Ihres Unternehmens dar. Wenn Sie Ihren Fokus von außen nach innen verlegen und softwarebasierte Segmentierung und ein Zero-Trust-Netzwerk implementieren, erhalten Sie die Transparenz und Kontrolle, die Sie benötigen, um laterale Netzwerkbewegungen zu erkennen, detaillierte und anwendbare Richtlinien zu etablieren und Cyberangriffe wie Ransomware davon abzuhalten, sich in Ihrem Netzwerk zu verbreiten.

Fordern Sie eine Demo an oder **erfahren Sie mehr** darüber, wie die Segmentierung Ihnen unter anderem bei Ransomware, Zero Trust und Cloudsicherheit hilft.

1 Cybersecurity Ventures. 2022 Who's Who in Ransomware Report. Conceal, 2022.

2 Kellerman, Tom und Greg Foss. Global Incident Response Threat Report. VMware Carbon Black, Okt. 2020.

3 „Cyber Security Statistics Trends & Data 2023." PurpleSec, 22. Feb. 2023.