FORTINET

Dynamische Sicherheit in AWS

Schaffen eines nahtlosen Schutzes für Cloud- und On-Premises-Netzwerke

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Mit einem Umsatz von 15,5 Milliarden US-Dollar im Jahr 2018 ist Amazon Web Services (AWS) der unangefochtene Marktführer im 32 Milliarden US-Dollar starkem IaaS-Cloud-Services-Markt (Infrastructure-as-a-Service).[1] Diese Popularität führt jedoch dazu, dass Cyber-Kriminelle ihr gesamtes Arsenal an hochentwickelter Malware auf die Infrastruktur, Anwendungen und Daten von AWS ausrichten. Security-Architekten sollten deshalb beim Entwerfen, Implementieren und Aufrechterhalten der Sicherheit für AWS-Umgebungen umfassende Lösungen einsetzen, die einen mehrstufigen Schutz bieten und native AWS-Tools erweitern. Eine nahtlose cloudnative Integration und Workflow-Automatisierung sind entscheidend, damit personell begrenzte Security-Teams die zunehmende Nutzung von AWS erfolgreich managen können. Da sich Anwendungen und Workloads (und Bedrohungen) in der Regel zwischen AWS und lokalen Umgebungen bewegen, müssen Sicherheitslösungen zudem das gesamte hybride Netzwerk abdecken. Nur so lässt sich ein konsequenter, zentral verwalteter Schutz bieten, der sowohl den Betriebsaufwand als auch das Sicherheitsrisiko verringert.

Chancen und Risiken in AWS

AWS bietet ein beispielloses Angebot an Rechen-, Speicher-, Datenbank- und anderen Diensten mit einem extrem einfachen Zugriff und einer benutzerfreundlichen Verwendung. Wegen der hohen Leistung und Verfügbarkeit von AWS stellen immer mehr Unternehmen Anwendungen jeder Art auf dieser Cloud-Plattform bereit – darunter auch geschäftskritische Anwendungen. Mittlerweile nutzen Hunderttausende von Unternehmen in 190 Ländern diesen Cloud-Anbieter.[2]

Die zunehmende Beliebtheit und Verbreitung von AWS eröffnet aber auch neue Spielräume für Cyber-Kriminelle, die auf Profit, Zerstörung und politischen Gewinn aus sind. Es handelt sich dabei um hochkomplexe Bedrohungen, die von gut finanzierten Entwickeln und Handlangern verbreitet werden. Entsprechend stark investiert AWS in die Security seiner Infrastruktur. Für den Schutz in AWS – also von allem, was in der Cloud bereitgestellt wird – sind jedoch die Kunden zuständig. Für Amazon Elastic Compute Cloud-Instanzen (Amazon EC2) umfasst dies das Gast-Betriebssystem sowie sämtliche Anwendungssoftware und Dienstprogramme, die auf den Instanzen installiert werden. Auch sind die Kunden für die Daten in ihrem Amazon S3-Speicher und in Amazon DynamoDB-Datenbanken verantwortlich.[3] Kurzum: Die Sicherheit von fast allem, was ein Kunde in der Cloud nutzt, liegt in seiner Verantwortung.

Die Definition und Implementierung der Security für cloudbasierte Anwendungen und Workloads übernimmt meistens der Security-Architekt. Bei genauerem Blick auf die Optionen der AWS-Plattform müssen Security-Architekten jedoch feststellen, dass AWS-Sicherheitsgruppen lediglich grundlegende Firewall-Funktionen bieten. Eine gründliche anwendungsbezogene Überprüfung oder Inspektion des verschlüsselten Datenverkehrs fehlt bei AWS. Da aber 60 % der Malware verschlüsselt ist, um einer Erkennung zu entgehen,[4] besteht die Gefahr, dass große Mengen Malware zwischen AWS und On-Premises-Netzwerken übertragen werden. Auch bei der seitlichen (Ost-West-) Ausbreitung von Bedrohungen im Netzwerk zwischen Virtual Private Clouds (VPCs), Availability Zones (AZs) und Regionen ist die native AWS-Security nur wenig effektiv.

Da 60 % der Malware verschlüsselt ist, um der Erkennung zu entgehen,[5] besteht die Gefahr, dass große Mengen Malware zwischen AWS und On-Premises-Netzwerken übertragen werden.

Während AWS für die Sicherheit *seiner Cloud-Ressourcen* zuständig ist, liegt der Schutz von allem, was sich *in AWS* abspielt – einschließlich Netzwerk, Anwendungen und Konfigurationen – in der Verantwortung des Kunden.

AWS erfordert drei Sicherheitsstufen

Die Art der wachsenden Angriffsfläche und der hochkomplexen Bedrohungen erfordert einen umfassenderen Schutz. Insbesondere muss in AWS die Security auf drei Ebenen gegeben sein: Netzwerk, Anwendungen und Transparenz/Kontrolle über die Plattform.

Netzwerk-Security

Als erste Verteidigungslinie spielt die Netzwerk-Security eine Schlüsselrolle beim Schutz von cloudbasierten Ressourcen. Virtuelle Next-Generation-Firewalls (NGFWs), die direkt in AWS bereitgestellt werden, schützen den Netzwerk-Rand (Edge) in mehrerlei Hinsicht:

- NGFWs blockieren bekannte Angriffsvarianten sowie Datenverkehr aus unautorisierten Quellen.
- NGFWs dienen als Terminierungspunkte für sichere VPN-Tunnel über VPCs und Standorte hinweg und verschlüsseln den autorisierten Datenverkehr, um die Vertraulichkeit und Integrität zu gewährleisten.

Um Bedrohungen für Anwendungen in einer VPC zu schützen oder die Verbreitung von Infektionen zu verhindern, können Security-Architekten mit virtuellen NGFWs eine logische (absichtsbasierte) Segmentierung implementieren. Damit lassen sich Zugriffsrechte und Segmente basierend auf Rollen und Geschäftslogik anlegen.[6] Auch sollten NGFWs Zero-Trust-Access-Strategien unterstützen und Zugriffsberechtigungen dynamisch an Infrastruktur-Änderungen anpassen können.

Für DevOps-Teams, die in AWS arbeiten, gewährleisten Schutzmaßnahmen auf Netzwerk-Ebene eine konsequente Sicherheit für alle Phasen der Implementierung und Einführung von Containern. Dies umfasst cloudbasierte NGFWs, die anhand der definierten Sicherheitsrichtlinien Container-Labels erkennen können, um Container-Workloads über alle Phasen des Anwendungs-Lebenszyklus hinweg zu verfolgen.

Anwendungssicherheit

Die meisten Anwendungen, die in AWS ausgeführt werden, sind Web Apps. Für Web Services zum Verbinden von Daten und anderen Anwendungen müssen in AWS ausgeführte Anwendungen vor Bedrohungen geschützt werden, die auf bestimmte Anwendungsplattformen und -logik abzielen. Auch ist ein Schutz vor Bedrohungen notwendig, die Sicherheitslücken in Benutzeroberflächen (UIs) und APIs im Visier haben.

Cloudbasierte Web Application Firewalls (WAFs) sind eine Schlüsselkomponente bei der Anwendungssicherheit, da sie Web-Anwendungen und APIs gleichermaßen schützen – Stichwort „Web Application and API Protection (WAAP)“. Wichtig ist, dass in AWS bereitgestellte WAFs dynamische Regelsätze beherrschen, um Anwendungen

vor den OWASP Top 10 Threats zu schützen („OWASP“ steht für „Open Web Application Security Project“). Weiter sollten sie die Möglichkeit bieten, eine anwendungsspezifische Geschäftslogik zu definieren und durchzusetzen.

Wird mit Mobilgeräten auf Anwendungen zugegriffen, werden APIs plötzlich über das Internet zugänglich. Security-Architekten sollten daher bei einer WAF Wert auf einen robusten API-Schutz legen. Zum Beispiel sollte ein dynamisches virtuelles Patching bekannter und unbekannter Schwachstellen möglich sein, damit Apps auch während der Aktualisierung von Application-Servern ausgeführt werden können. Weiter sollte eine gute WAF ein Application Profiling bieten, um ein abnormales Anwendungsverhalten – das möglicherweise auf einen Bot hinweist – zu lokalisieren und zu beenden.

Schließlich ist Flexibilität unerlässlich. Wie genau WAFs und andere Sicherheitslösungen für Web-Anwendungen bereitgestellt werden, hängt von der Art der Anwendungsumgebungen und der Arbeitsweise des Entwicklerteams ab. Zur Umsetzung einer effektiven WAAP-Strategie sollten Security-Architekten in der Lage sein, für jede Anwendung und jedes Team die am besten geeignete Form der Bereitstellung auszuwählen. Dabei sollten alle kundenseitigen Sicherheitslösungen unabhängig vom Formfaktor – VM, Docker-Container oder SaaS-Lösung – zusammenarbeiten, damit einheitliche Sicherheitsrichtlinien implementiert werden können.

48 % aller Datenpannen werden durch das Hacken von webbasierten Anwendungen verursacht.[7]

Transparenz und Kontrolle über die Plattform

Die vielen Vorteile des umfangreichen AWS-Angebots bringen jedoch auch Risiken mit sich. Das Einrichten eines EC2, S3 oder eines anderen Dienstes ist mit wenigen Klicks erledigt. Das Konfigurieren der Sicherheitseinstellungen für jeden Dienst erfordert jedoch einen genauen Blick fürs Detail. Denn durch Fehlkonfigurationen kann es leicht zu Sicherheitslücken kommen, die viel Schaden anrichten und Angreifern Tür und Tor öffnen können. Selbst korrekte, aber uneinheitliche Konfigurationen können dazu führen, dass die Sicherheitsrichtlinien des Unternehmens und die gesetzlichen Datenschutzbestimmungen nicht eingehalten werden.

Aufgrund ihrer Komplexität darf die Sicherheitskonfiguration nicht Geschäftsanwendern oder unerfahrenen Security-Mitarbeitern überlassen werden. Die CloudFormation Templates (CFTs) in AWS sollten ausschließlich Sicherheitsexperten erstellen, damit alle neu implementierten Cloud-Dienste von Anfang an einheitlich konfiguriert werden. Für einen minimalen Aufwand bei der Vorlagenerstellung in komplexen AWS-Umgebungen sind vertrauenswürdige, vorkonfigurierte CFTs sinnvoll, die bereits Best Practices für die Security berücksichtigen.

Da auch Vorlagen Fehler enthalten können und sich die Bedrohungslage sowie Cloud-Umgebungen ständig ändern, müssen Unternehmen für AWS eine Cloud Workload Protection Platform (CWPP) und ein Cloud Security Posture Management (CSPM) implementieren. Für eine optimale Transparenz und Kontrolle über die Cloud-Plattform sollten Security-Architekten daher darauf achten, dass CWPP- und CSPM-Lösungen Folgendes bieten:

- Konfigurationsbewertungen, die Konfigurationsfehler aufdecken und Konfigurationen anhand von Best Practices, Konformitätsregelungen und Unternehmensrichtlinien validieren
- umfassendes Compliance-Reporting
- Überwachung der Aktivität in Cloud-Konten sowie des Cloud-Netzwerkverkehrs
- sichere Speicherung unerwünschter Daten, um ein Aktivieren eingebetteter Malware zu verhindern

70 % der Cloud-Datenpannen gehen auf Fehlkonfigurationen zurück – eine Zahl, die im Jahresvergleich um 424 % gestiegen ist.[8]

Maximale Sicherheit mit minimalem Management

Die lange Liste der Anforderungen für einen angemessenen Schutz von AWS-Umgebungen wird – angesichts des anhaltenden Fachkräftemangels im Bereich Cyber-Sicherheit mit weltweit über 4 Millionen unbesetzten Stellen – in vielen Unternehmen als überwältigend empfunden.[9] Eine umfassende Cloud-Sicherheitslösung kann Security-Architekten sinnvoll entlasten, indem sie optimierte Abläufe, konsequente Richtlinien, einheitliche Security-Workflows und umfassende Transparenz über die AWS-Umgebung ermöglicht.

Dafür muss die Lösung aber die Dynamik von Cloud-Implementierungen berücksichtigen. Obwohl viele Unternehmen ihre AWS-Infrastruktur erweitern, gibt es auch den umgekehrten Trend: Einige cloudnative oder in die Cloud migrierte Anwendungen und Workloads werden jetzt wieder On-Premises bereitgestellt. Diese Entwicklung bestätigen auch 74 % der Befragten in einer Umfrage vom Vorjahr.[10]

Automatisierung – ein Muss für personell begrenzte Teams

Überall dort, wo Anwendungen und Workloads ausgeführt werden, muss die Sicherheit gewährleistet sein. Eine dynamische Cloud-Security-Lösung muss dies in Echtzeit mit minimalem Personaleinsatz ermöglichen. Beispielsweise sollten sich Richtlinien für die Anwendungssicherheit und den Benutzerzugriff aus On-Premises-Security-Geräten automatisch in geeignete virtuelle Tools importieren lassen, wenn Anwendungen auf AWS migriert werden. Gleiches sollte bei Migrationen von der Cloud- zur On-Premises-Ausführung geschehen. Erfordert das Wachstum innerhalb von AWS zusätzliche Sicherheitsmaßnahmen, sollte die Security-Plattform zudem einen Mechanismus für die automatische Skalierung bereitstellen und mit CFTs einheitliche Sicherheitskonfigurationen gewährleisten.

Zentrale Transparenz und Kontrolle mit einer einzigen Konsole

Alle AWS- und lokalen Sicherheitskomponenten sollten für ein zentrales Security-Management-System sichtbar und kontrollierbar sein, damit sich eine wachsende Hybrid-Cloud-Sicherheitsinfrastruktur selbst mit kleinen Security-Teams kompetent verwalten lässt. Können z. B. automatisierte Workflows direkt im Management-System gestartet werden, gewinnen Security-Manager durch diese Entlastung Zeit für geschäftliche Aufgaben. Dinge, die bislang vom Security-Management ablenkten – wie die Umsetzung von Audit-Ergebnissen, internes Reporting und häufige Änderungen der Netzwerk-Zugriffsrechte – können dann in Ruhe erledigt werden.

Cloud-Umgebungen sind dynamisch:

74 %

der Unternehmen haben eine Anwendung in die Cloud verlagert – und dann wieder On-Premises bereitgestellt.[11]

Alle Sicherheitsfunktionen – von NGFWs und WAFs bis hin zu CWPP und CSPM – sollten in AWS genauso funktionieren wie On-Premises. Dies minimiert den Bedarf an abteilungsübergreifenden Schulungen und reduziert letztendlich die Kosten der Cloud-Agilität.

Weiter sollte eine dynamische Cloud-Security-Lösung vorgefertigte Integrationen mit den AWS-Tools bieten, mit denen Security-Administratoren bereits vertraut sind. Dann können Komponenten der Security-Plattform auch mit anderen Tools angezeigt und konfiguriert werden. Auch sollten sich Daten und Objekte nahtlos gemeinsam nutzen lassen, da dies die unternehmensweite Erkennung, Analyse und Abwehr von Bedrohungen in Echtzeit vereinfacht.

Der Schutz von AWS-Umgebungen kann angesichts des Fachkräftemangels im Bereich Cyber-Sicherheit überwältigend sein – weltweit sind mehr als 4 Millionen Stellen unbesetzt.[12]

Fazit: Komplette, konsequente Cloud-Security

Paradoxerweise stellt dieselbe Cloud-Dynamik, die Kunden und Mitarbeitern ein unkompliziertes Arbeiten und mehr Produktivität ermöglicht, Security-Teams vor gewaltige Herausforderungen. Security-Architekten benötigen deshalb eine dynamische Sicherheitslösung, mit der sich jede Anwendung in einer beliebigen AWS-Region oder On-Premises (sowie in anderen Cloud-Diensten) bereitstellen und gleichzeitig überall das gleiche Sicherheitsniveau gewährleisten lässt.

Eine solche Lösung sollte umfassend, integriert und automatisiert sein, muss aber nicht zwangsläufig von einem einzigen Technologie-Anbieter stammen. Besser ist, wenn die Security-Lösung erstklassige Technologien verschiedener führender Anbieter und der Open-Source-Community in sich vereint.

[1] „Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018“. Gartner, 29. Juli 2019.

[2] „About AWS“. aws.amazon.com, abgerufen am 20. November 2019.

[3] „Shared Responsibility Model“. aws.amazon.com, abgerufen am 20. November 2019.

[4] Omar Yaacoubi: „The hidden threat in GDPR's encryption push“. PrivSec Report, 8. Januar 2019.

[5] Ebd.

‘[6] „A Network Operations Guide for Intent-based Segmentation: Essential Practices for Risk Mitigation and Compliance Across the Attack Surface“. Fortinet, 6. Februar 2019.

[7] „2018 Data Breach Investigations Report“. Verizon, April 2018.

[8] Phil Muncaster: „Breached Records Fall 25% as Cloud Misconfigurations Soar“. Infosecurity, 6. April 2018.

[9] „Strategies for Building and Growing Strong Cybersecurity Teams (ISC)²: Cybersecurity Workforce Study 2019“. (ISC)², 2019.

[10] Jeff Wilson: „The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments“. IHS Markit, Q2 2019.

[11] Ebd.

[12] „Strategies for Building and Growing Strong Cybersecurity Teams (ISC)²: Cybersecurity Workforce Study 2019“. (ISC)², 2019.

www.fortinet.com/de

545978-0-A-DE

5. Mai 2020, 11:45 Uhr