FORTINET

Dekonstruktion des Risikos der Public Cloud: 5 Anwendungsfälle

Was Security-Architekten bei einer Lösung beachten sollten

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Unternehmen haben Public Cloud-Plattformen aller Art in großem Stil angenommen, aber das Ergebnis ist eine erhöhte Komplexität der Sicherheitsabläufe. Eingebaute Security Tools für die verschiedenen Cloud-Anbieter sind voneinander unabhängig und inkompatibel. Ein konsequentes Risiko-Management über alle Clouds hinweg macht den Security-Betrieb in einer Multi-Cloud-Welt somit zeitaufwändig und ineffektiv. Darüber hinaus bedeutet die erweiterte Angriffsfläche, dass sich Unternehmen vor Risiken schützen müssen, die sowohl von der Anwendungsprogrammierschnittstelle (API) als auch von der Benutzeroberfläche (UI) der Cloud-Plattformen ausgehen. Und diese Risiken können nicht nur durch Konfigurations- und Management-Fehler, sondern auch durch die Anwendungselemente selbst entstehen.

Dieses E-Book behandelt fünf wichtige Anwendungsfälle, mit denen Security-Teams konfrontiert sind, die für die Sicherung ihrer Public Cloud-Infrastruktur verantwortlich sind: (1) Risiko-Management, (2) Datensicherheit, (3) Analyse und Untersuchung des Datenverkehrs, (4) Bedrohungserkennung und -reaktion und (5) Compliance. Jeder dieser Anwendungsfälle beschreibt die besonderen Herausforderungen in einer Public Multi-Cloud-Umgebung. Die oberste Priorität für die Sicherheit ist, die Security-Architektur zu integrieren, um zentrale Sichtbarkeit und Kontrolle zu ermöglichen. Dies kann aufgrund der Unterschiede zwischen den Public Clouds nicht manuell erfolgen. Mit einer integrierten Architektur können Unternehmen jede dieser Herausforderungen proaktiv und ganzheitlich angehen und somit die betriebliche Effizienz verbessern und das Risiko verringern.

83 %

der Workloads von Unternehmen werden bis 2020 in der Cloud verarbeitet, und 63 % der IT-Experten sehen Security als das größte Problem bei diesem Trend.[1]

Einführung: Umgang mit der Cloud-Ausbreitung

Unternehmen haben Public Cloud Computing in großem Stil angenommen: Public Cloud-Dienste sollen 2019 um 17,3 % auf 206 Milliarden Dollar weltweit wachsen, wobei Infrastructure-as-a-Service (IaaS) mit 27,6 % das am schnellsten wachsende Segment ist.[2] Während die Zahlen schwer zu erfassen sind, ist die Attraktivität von Cloud-Plattformen nicht überraschend. Unabhängig davon, welche cloudbasierten Dienste Unternehmen ausführen – Software, Infrastruktur oder Plattform – sie genießen die Vorteile einer schnellen Implementierung, schneller Skalierbarkeit, der Möglichkeit, nur für die genutzte Kapazität zu zahlen, und des Wegfalls von Investitions- und Personalkosten für den Rollout.

Nach mehr als einem Jahrzehnt aggressiven Hinzufügens von Cloud-Ressourcen leiden viele Unternehmen jedoch unter etwas, das man als Cloud-Ausbreitung bezeichnen könnte. Die meisten Unternehmen betreiben mehrere Clouds, und Netzwerk-Security-Teams haben oft Schwierigkeiten, den Überblick über Assets zu behalten und Risiken in diesen dynamischen Umgebungen genau zu identifizieren. Der dezentrale Charakter vieler Cloud-Einkäufe verschärft das Problem, da die IT-Abteilung oft nicht der endgültige Entscheider ist. Eine weitere Komplikation: Die integrierten Security Tools der verschiedenen Public Cloud-Anbieter arbeiten unterschiedlich und verfolgen unterschiedliche Security-Daten.

Dieses E-Book behandelt fünf wichtige Anwendungsfälle für die Public Cloud Security und diskutiert die Merkmale einer effektiven Lösung für jeden Anwendungsfall.

„Für dieses Jahr wird ein IaaS-Umsatzwachstum von 27,6 % erwartet.“[3]

Risiko-Management: Eine Unternehmenssicht auf Cloud-Konfigurationen

Auf dem sich schnell entwickelnden Markt von heute reicht es nicht aus, statische Vorschriften und Normen einzuhalten. Jedes Unternehmen muss sein Cyber-Risikoprofil bewerten und Security-Programme auf seine spezifische Risikotoleranz hin abstimmen. Ein wichtiger Risikofaktor für Unternehmen ist die falsche Konfiguration von Systemen – sowohl auf der Cloud-Management-Plattform als auch in den Anwendungskomponenten selbst.[4] In einem Bericht werden 70 % der Cloud-Datenschutzverletzungen auf Fehlkonfigurationen zurückgeführt – eine Zahl, die im Jahresvergleich um 424 % gestiegen ist.[5]

In statischen, lokalen Umgebungen können diese Probleme mithilfe einer Configuration Management Database (CMDB) gelöst werden. Doch schnelle Änderungen an Cloud-Diensten und -Konfigurationen bringen neue Herausforderungen mit sich. Dienste auf mehreren Clouds führen zu Isolation und fehlender Gesamttransparenz, und die Dynamik von Cloud-Implementierungen erschwert es Unternehmen, ihr Sicherheitsprofil konsequent zu bewerten. Dies führt zum Risiko von Fehlkonfigurationen in einer immer komplexeren Infrastruktur.

Bei der Lösung dieser Probleme sollte der erste Schritt sein, eine zentralisierte Transparenz zu schaffen und Änderungen des Konfigurationsstatus und des gesamten Cloud-Infrastrukturprofils zu verfolgen. Mit dieser umfassenden Sichtweise sollte eine Cloud Security-Lösung in der Lage sein, eine umfassende Risikobewertung durchzuführen, einen Risiko-Score zu erstellen und Best Practice-Empfehlungen zu dessen Verbesserung anzubieten. Nach Abschluss der Bewertung sollte die Cloud-Infrastruktur eines Unternehmens weiterhin konsequent überwacht werden, um sicherzustellen, dass Probleme rechtzeitig erkannt und gelöst werden. Schließlich sollten Analyse-Tools zur Verfügung stehen, die den Security-Teams helfen, den Lebenszyklus von Konfigurationsänderungen über die Multi-Cloud-Umgebung hinweg zu verstehen.

„Cloud führt die Liste der Initiativen zur digitalen Transformation, die 2019 von den Unternehmen zur Entwicklung angestrebt wurden, an.“[6]

Datensicherheit: Kontinuierliche Überwachung auf Datenverluste und Malware

Eine sich ausbreitende, „wuchernde“ Cloud-Infrastruktur kann bedeuten, dass Benutzer unerwünschte Daten unorganisiert über Cloud-Infrastrukturen hinweg speichern. Dies führt zu einem signifikanten unbekannten Risiko durch potenziell schädlichen und in Dateien eingebetteten Code sowie zu einem erhöhten Risiko von Datenlecks. Im letzteren Fall ist eine konsolidierte Sicht auf alle Dateien und Speicher in der gesamten Cloud-Infrastruktur erforderlich. Ausschließlich eine umfassende Multi-Cloud-Lösung zum Überprüfen und Überwachen von Dateien ist in der Lage, riskante Dateiübertragungsmuster zu identifizieren.

Dies geschieht im Kontext immer zahlreicherer und kostspieligerer Bedrohungen. Im vierten Quartal 2018 entdeckten die FortiGuard Labs fast 34.000 neue Malware-Varianten – eine Zunahme von 128 % gegenüber dem ersten Quartal des gleichen Jahres.[7] Und neue Studien schätzen die Kosten, die einem durchschnittlichen Unternehmen durch Cyber-Kriminalität im Jahr 2018 entstanden, auf 13 Millionen Dollar – ein Anstieg von 12 % gegenüber 2017 und ein Anstieg von 72 % über fünf Jahre.[8] Dateien im Cloud-Speicher zu überprüfen, ist eine von wenigen Möglichkeiten, die Verbreitung hochriskanter Inhalte zu verhindern.

Um kritische Daten in einer Multi-Cloud-Infrastruktur zu schützen, müssen Unternehmen in der Lage sein, (1) gespeicherte Dokumente ständig zu überwachen, um Malware zu identifizieren, und (2) Aktivitäten mit sensiblen Daten konsequent zu verfolgen, um Datenlecks in der Umgebung zu identifizieren und zu untersuchen.

„Durch das Verschieben von immer mehr Geräten und kritischen Daten in die Cloud ändern sich nicht unbedingt die Angriffstypen, aber die Art und Weise, wie diese Angriffe ausgeführt werden, wandelt sich.“[9]

Analyse und Untersuchung des Datenverkehrs: Eine umfassende Ansicht zur Erkennung von Angriffen

Es gibt zwei Probleme bei der Ausbreitung der Cloud: das erhöhte Risiko von unerlaubten Netzwerkzugriffen durch potenzielle Konfigurationsfehler und das Unvermögen, den Netzwerkverkehr angemessen zu überwachen. Verwurzelt sind diese Herausforderungen bei den Mitgliedern des Security-Teams, die oft nicht über eine aktuellen Bestandsübersicht über die in Public Clouds aktivierten Assets und Ressourcen verfügen – und sicherlich nicht in der Lage sind, die Veränderungen dieser Ressourcen dauerhaft zu überwachen.[10] Selbst bei einer genauen Bestandsübersicht sind für die Überwachung des Datenverkehrs innerhalb und zwischen den Clouds und das Erkennen verdächtiger Aktivitäten innerhalb dieses Datenverkehrs spezifische Tools erforderlich.

Um unerlaubte Netzwerkzugriffe effektiv zu erkennen und zu unterbinden und kritische Dienste zu schützen, benötigen Security-Teams die Möglichkeit, die aktuelle Topologie aller Cloud-Ressourcen anzuzeigen, den Netzwerkdatenverkehr zu überwachen und zu analysieren sowie bestimmte verdächtige Dienste und Verkehrsmuster zu analysieren. Insbesondere benötigen sie die Fähigkeit, den Netzwerkverkehr zu visualisieren, um besser zwischen fehlerhaften Konfigurationen und bedrohlichen Datenverkehrsmuster unterscheiden zu können.

Fast 45 % der Security-Architekten sind der Meinung, dass ihre Unternehmen zu reaktiv sind und im Umgang mit Security-Fragen proaktiver werden müssen.[11]

Bedrohungserkennung und -reaktion: Integrierte Intelligenz und Echtzeit-Sharing

Das Verschieben von immer mehr Anwendungen in die Public Cloud und die vermehrte Nutzung cloudbasierter Dienste führen zu einer Zunahme der Komplexität und damit auch des Potenzials für Konfigurationsfehler. Damit wird der Bedarf eines integrierten Ansatzes für die Erkennung von Bedrohungen und entsprechende Reaktionen weiter gesteigert – insbesondere angesichts der Komplexität der aktuellen Bedrohungslandschaft. Bedrohungen in der Public Cloud können aus verschiedenen Gründen auftreten, wie etwa der fehlerhaften Konfiguration der Cloud selbst, der Verwendung anfälliger Software-Versionen und die Implementierung von unsicherem Code in Cloud-Anwendungen.

Vorrangig sollte es darum gehen, die Fähigkeit von Cyber-Kriminellen einzudämmen, diese Schwachstellen auszunutzen. Security-Teams müssen in der Lage sein, Bedrohungen zu identifizieren und zu isolieren – und diese effektiv zu beseitigen. Da die Security-Teams die Sicherheitsprüfungen überwachen, benötigen sie Security Tools, die es ihnen erleichtern, den DevOps-Teams aussagekräftige und benutzerfreundliche Erkenntnisse zu liefern.

Es gibt heute mehr als eine Million Arten von Bedrohungen – gegenüber 50 vor einem Jahrzehnt.[12]

Compliance: Zentralisierte Berichterstellung für schnelle Gegenmaßnahmen und Auditvorbereitung

Angesichts einer zunehmenden Zahl von Vorschriften und der sich intensivierenden medialen Überprüfung der Cyber Security-Mängel von Unternehmen ist Compliance für praktisch jedes Unternehmen ein immer wichtiger werdender Faktor. Neuere Vorschriften wie die Datenschutzgrundverordnung der Europäischen Union (DSGVO) sehen hohe Bußgelder im Falle einer Nichteinhaltung vor, und ähnliche Vorschriften sind in anderen Ländern in Arbeit.[13] Andere Vorschriften können Herausforderungen mit sich bringen, wie beispielsweise der Payment Card Industry Data Security Standard (PCI DSS) zur Abwicklung von Kreditkartentransaktionen, der dazu führen kann, dass Kredit- und Debitkarten nicht akzeptiert werden – eine verheerende Auswirkung für viele Unternehmen.

Diese Vielzahl von Anforderungen macht Compliance und die Vorbereitung auf Audits zu einem komplexen Unterfangen, das in vielen Unternehmen unzählige Stunden wertvoller Arbeitszeit verschlingt. Die Compliance-Berichterstellung kann in einer Multi Cloud-Infrastruktur noch komplexer werden, wenn für jeden Cloud-Anbieter und jede IaaS-Lösung isolierte Reporting-Tools und Ereignisdaten verwendet werden. Und da die Public Cloud die Angriffsfläche vergrößert und neue Bedrohungsvektoren einführt, muss sie Teil der Compliance-Bewertungen sein.

Wie für die anderen beschriebenen Geschäftsanforderungen ist auch für eine effiziente und effektive Compliance-Berichterstellung eine Architektur erforderlich, die die Multi Cloud-Architektur für eine zentralisierte Sichtbarkeit und die Richtlinienverwaltung integriert. Diese Sichtbarkeit sollte auch die Möglichkeit umfassen, historische Snapshots von Public Cloud-Umgebungen zu erhalten. Security-Teams müssen robuste Berichterstellungs-Tools mit sofort verwendbaren Richtlinien für eine Vielzahl von Vorschriften und Standards einsetzen. Berichte müssen regelmäßig ausgeführt werden, damit die Security-Teams Richtlinienverletzungen schnell erkennen und Abhilfemaßnahmen ergreifen können. Diese Prozesse müssen auch automatisiert werden, um überlastete Security-Teams zu optimieren und gleichzeitig Risiken zu minimieren.

„Die von Rechts- und Cyber Security-Teams für die Reaktion auf unerlaubte Zugriffe aufgewendete Zeit ist im vergangenen Jahr um 20 % gestiegen.“[14]

Fazit: Integration ist der Schlüssel

Die auf jeder Seite dieses E-Books konsequent wiederholte Botschaft ist, dass die Integration der Sicherheitskontrollen von Public Cloud-Ressourcen eine der neuesten und wichtigsten Prioritäten für den Schutz der Public Cloud ist. Diese Integration hilft Unternehmen, ihre Daten zu schützen, unerlaubte Zugriffe zu verhindern, komplexe Bedrohungen zu bekämpfen und Auditoren zufriedenzustellen. Aufgrund der Art und Weise, wie Public Cloud-Infrastrukturen außerhalb der Anwendungs- und Netzwerksysteme konfiguriert werden, und da ihre integrierten Security Tools unterschiedliche Methoden verwenden, ist eine manuelle Integration praktisch unmöglich – und angesichts der Geschwindigkeit der heutigen komplexen Bedrohungen sicherlich ineffektiv. Es besteht daher ein klarer Bedarf eines speziellen Tools, das einheitlich die Transparenz und Kontrolle zur Sicherung der Public Cloud Management-Schnittstelle und der APIs bereitstellt.

Unternehmen, die eine Vielzahl von Diensten in mehreren Clouds nutzen, müssen ein einheitliches Security Tool nutzen, das neben einer nativen Integration in alle wichtigen Cloud-Plattformen die Fähigkeit bietet, Threat Intelligence aus jeder Cloud in Echtzeit zu konsolidieren, und die intelligente Überwachung des Datenverkehrs innerhalb und zwischen den Clouds sowie robuste Berichts- und Analyse-Tools bereitstellt. Mit transparenter Sichtbarkeit und zentralisierter Kontrolle über die gesamte Infrastruktur können Unternehmen die immensen Vorteile des Cloud Computing voll ausschöpfen – ohne das Risiko zu erhöhen.

„Im digitalen Unternehmen führt die strategische Fusion ehemals isolierter Bereiche zu mehr Kundenzufriedenheit, einer Beschleunigung der Geschäftsprozesse und operativer Agilität.“[15]

[1] Louis Columbus, „83% Of Enterprise Workloads Will Be In The Cloud By 2020“, Forbes, 7. Januar 2018.

[2] Louis Columbus, „Roundup Of Cloud Computing Forecasts And Market Estimates, 2018“, Forbes, 23. September 2018.

[3] Andy Patrizio, „Cloud Computing Companies“, Datamation, 9. Januar 2019.

[4] Asher Benbenisty, „Don’t Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes“, Infosecurity, 30. Oktober 2018.

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

[6] „The future of cyber survey 2019“, Deloitte, März 2019.

[7] „Threat Landscape Report Q4 2018“, Fortinet, letzter Zugriff 12. März 2019.

[8] „The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study“, Accenture Security and Ponemon Institute, letzter Zugriff 12. März 2019.

[9] Rich Campagna, „Malware’s Journey Through the Cloud“, Infosecurity, 28. September 2017.

[10] Chris Purcell, „Is Multi-Cloud Sprawl Causing Your Money to Fly Away?“, CIO, 17. September 2018.

[11] „The Security Architect and the State of Cybersecurity“, Fortinet, erscheint in Kürze.

[12] Dave DeWalt und David Petraeus, „The Cyber Security Mega Cycle Aftermath“, Optiv, 7. September 2017.

[13] Kassidy Kelley, „CCPA compliance begins with data inventory assessment“, TechTarget, Dezember 2018.

[14] „2019 Scalar Security Study: The Cyber Resilience of Canadian Organizations“, Scalar, Februar 2019.

[15] Benson Chan, „Digital transformation reimagines everything“, Strategy of Things, 7. September 2017.

www.fortinet.com/de

377156-0-0-DE

September 11, 2019 5:11 nachm.

eb-forticasb-cloud-security-use-cases_DE