EINFÜHRUNG IN DEN
CLOUD SECURITY BLUEPRINT 2.0

Inhalt

Einführung 3

Cloud Security Konzepte: Eine Einführung 5

- Das Shared-Responsibility-Modell der Public Cloud verstehen
- Zero Trust und warum Sie es übernehmen sollten

Erweiterte Herausforderungen für die Cloud-Sicherheit.....8

- Ein Mangel an Sichtbarkeit und Tracking
- Sich ständig ändernde Arbeitsbelastung
- DevOps, SecDevOps und Automation
- Multi-Cloud-Umgebung
- Granulare Berechtigungsverwaltung
- Compliance und Bestimmungen
- Attraktives Angriffsziel

Architekturprinzipien von Cloud-Sicherheits-Lösungen.....10

- Sicherheit am Netzwerkperimeter mit Advanced Threat Protection
- Andere Perimeter, die gesichert werden müssen
- Security by Design
- Segmentierung und Mikro-Segmentierung
- Agilität
- Automatisierung, Effizienz und Elastizität
- Grenzenlos
- Compliance

Zusammenfassung 15

Einführung

Wie wir durch den „Rightscale 2019 State of the Cloud Report“ von Flexera erfahren haben, ist Cloud Computing bei Unternehmen aller Größen so gut wie überall vertreten: 94 % der Umfrageteilnehmer berichteten, dass ihr Unternehmen Public Clouds verwendet. Wir konnten auch feststellen, dass Unternehmen weiterhin mit Hybrid Clouds und Multi-Cloud-Strategien arbeiten (siehe Abb. 1). Die Einführung von Hybrid Clouds stieg im letzten Jahr von 51 % auf 58 % und die von Multi-Clouds von 81 % auf 84 % an.

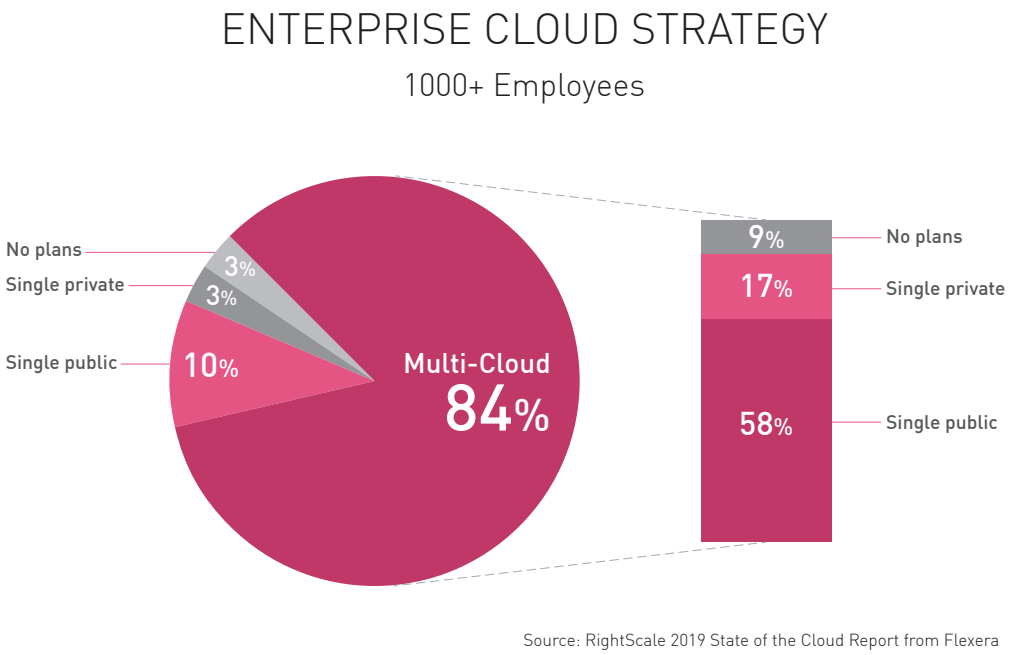

Abbildung 1: Zunahme der Hybrid- und Multi-Cloud-Infrastrukturen bei Unternehmen

Geschäftliche Agilität, Produktivität, operative Effizienz, Flexibilität und Profitabilität sind zweifelsohne die entscheidenden Faktoren für die Einführung von Public Cloud bei Unternehmen. Public Cloud ermöglicht, dass Computer-Speicher-Netzwerk-Ressourcen schneller bereitgestellt und implementiert werden können. Nachdem Sie implementiert wurden, können diese Ressourcen nach Bedarf hoch- und herunterskaliert werden.

Untersuchungen zeigen, dass bis zu 10.000 Unternehmen aufgrund einer weit verbreiteten Fehlkonfiguration in Google Groups anfällig sind.

Gleichzeitig ergab Gartners Security of the Cloud Primer for 2019, dass Cloud-Sicherheit nach wie vor ein großes Anliegen ist. Das ist nicht überraschend, wenn man sich vor Augen hält, dass Public-Cloud-Services geteilte Dienste sind, die immer verbunden und daher per se dynamisch sind. Außerdem sagte Gartner voraus, dass „bis 2022, 95 % der Sicherheitsausfälle in der Cloud auf Fehler des Kunden zurückzuführen sind." Und in der Tat kann die Mehrzahl der Vorfälle von gestohlenen Daten in der Cloud nachverfolgt und eher auf einfache menschliche Fehler zurückgeführt werden als auf geplante Angriffe. Beispielsweise zeigen Forschungen, dass bis zu 10.000 Unternehmen Schwachstellen aufgrund von weit verbreiteten Fehlkonfigurationen in den Einstellungen von Google Groups haben. Einerseits sind das alarmierende Statistiken. Sie besagen jedoch auch, dass Unternehmen ihre Organisation in Sachen Sicherheit beträchtlich verbessern können, wenn sie eine effektive Sicherheitsstrategie anwenden.

Letztes Jahr haben wir den Check Point Secure Cloud Blueprint v1.0 veröffentlicht, um Unternehmen dabei zu unterstützen, agile Cloud-Sicherheits-Architekturen zu konfigurieren
und zu implementieren. Da es seitdem eine Reihe von wichtigen Veränderungen im Cloud-Blueprint gab, haben wir eine neue Reihe von Whitepapers zu folgenden Themen veröffentlicht:

- Einführung in die fundamentalen Prinzipien des Cloud-Blueprints
- Aktivierung von Cloud-Blueprint-Lösungen
- Richtlinien zur technischen Cloud-Blueprint-Implementierung für führende Cloud-Service-Provider

Im ersten Whitepaper beschreiben wir die wichtigsten Cloud-Sicherheitskonzepte und die archetektonischen Prinzipien, die für ein Cloud-Sicherheits-Blueprint gegeben sein müssen.

Cloud-Sicherheits-Konzepte: Eine Einführung

In diesem Abschnitt untersuchen wir die zwei Schlüsselkonzepte, die ein Unternehmen kennen muss, um einen effektiven Sicherheits-Blueprint einführen zu können.

Das Shared-Responsibility-Modell der Public Cloud verstehen

Durch die Verlagerung von Worksloads und Daten in Public-Cloud-Umgebungen liegt die Verantwortung für Sicherheit sowohl in Ihren als auch den Händen Ihres Cloud-Providers. Die Sicherheit der Cloud-Infrastruktur (einschließlich der tatsächlichen Standorte von physischen Rechenzentren, Hardware für Computing/Netzwerk und Speicherung sowie der Router, Switches und Load-Balancer, HKL und Elektrizität etc.) wird vom Provider bereitgestellt. Es liegt in der Verantwortung des Kunden, die nativen Tools des Cloud-Anbieters so einzusetzen, dass die Assets und Workloads in der Cloud geschützt werden. Dazu zählen auch die Anwendungscodes, Anwendungsdaten und der Anwendungszugriff und die Einhaltung der gesetzlichen Bestimmungen und Best Practices in Bezug auf Sicherheit.

Per Definition variiert das Shared-Responsibility-Modell, je nachdem ob IaaS, PaaS oder SaaS eingesetzt werden (siehe Abb. 2, die auf einem Diagramm von der Webseite von Microsoft Azure basiert) Zur gleichen Zeit verwenden die üblichen Cloud-Implementierungen einen Mix aus diesen Service-Modellen, was oft zu einer allgemeinen Verwirrung führt: Wer ist für was verantwortlich?

Verantwortlich-keit	On-Premise	IAAS	PaaS	SaaS
Anwendungen	●	●	●	○
Daten	●	●	●	○
Runtime	●	●	○	○
Middleware	●	●	○	○
O/S	●	●	○	○
Virtualisierung	●	○	○	○
Serves	●	○	○	○
Speicher	●	○	○	○
Netzwerk	●	○	○	○

Quelle: Azure Website

Abbildung 2: Shared-Responsibility-Zonen in Cloud-Service-Modellen.

Amazon Web Services (AWS) fasst es auf seiner Webseite treffend zusammen:

> „... der Kunde muss alle erforderlichen Sicherheitskonfigurationen vornehmen und Verwaltungsaufgaben durchführen. Kunden, die eine Amazon EC2-Instanz bereitstellen, sind für die Verwaltung des Gastbetriebssystems verantwortlich (einschließlich der Aktualisierungen und der Sicherheits-Patches), für die gesamte, vom Kunden auf den Instanzen installierte Anwendungs-Software oder die Dienstprogramme und auf jeder Instanz für die Konfiguration der von AWS bereitgestellten Firewall (eine Sicherheitsgruppe genannt) ... dieses Modell der zwischen dem Kunden/AWS geteilten Verantwortung reicht bis zur IT-Kontrolle. Genauso, wie die Verantwortung für den Betrieb der IT-Umgebung zwischen AWS und seinen Kunden geteilt wird, wird die Verantwortung für das Management, den Betrieb und die Überprüfung der IT-Kontrollen geteilt ...“

Kurz gesagt, sollten Cloud-Kunden sich in dem Glauben, dass „die Cloud sicher ist“ nicht in (falscher) Sicherheit wiegen. In der Tat tragen Cloud-Kunden eine beträchtliche Verantwortung und sollten diese niemals auf die leichte Schulter nehmen.

Zero Trust und warum Sie das Konzept übernehmen sollten

Forrester formuliert in seinem Bericht „Predictions 2019 Transformation goes pragmatic“, dass „im Jahr 2019 und bis 2020 Zero Trust in den USA der Ad-hoc-Standard sein wird.“

Wie der Name schon sagt, besteht das Grundprinzip von Zero Trust darin, niemandem und nichts zu vertrauen und alles zu überprüfen. Angriffe finden sowohl innerhalb als auch außerhalb des Netzwerks statt und standardmäßig sollten Benutzer und Maschinen niemals automatisch als vertrauenswürdig eingestuft werden. Sie müssen davon ausgehen, dass jeglicher Traffic, unabhängig vom Standort, solange eine Bedrohung ist, bis er überprüft wurde (d. h. autorisiert, inspiziert und gesichert).

Zero Trust fördert beispielsweise eine „Least-Privileged“-Strategie, bei der Benutzern nur Zugriff zu den Ressourcen gegeben wird, die sie für die Durchführung ihrer Aufgaben benötigen. Darüber hinaus gewähren moderne Anwendungen Komponenten, die die verteilte Architektur beinhalten, oft umfangreiche Berechtigungen. Anwendungen mit Web-Zugriff haben besonders viele Schwachstellen. Wenn der Entwickler Ports nicht durchgängig gesperrt hat, hat beispielsweise ein Hacker, der auf die Anwendung zugreift, die Berechtigung, Daten zu lesen, zu schreiben und aus der Datenbank zu ziehen.

Darüber hinaus verwenden Zero-Trust-Netzwerke eine Mikrosegmentierung – eine Methode, die in Rechenzentren Sicherheitszonen und Cloud-Ressourcen zur Trennung von Workloads bereitstellt, alles innerhalb dieser Zone sichert und Sicherheitsrichtlinien zwischen den Zonen anwendet. Das erhöht die Granularität von Netzwerksicherheit. Es ist ebenso wichtig, den gesamten internen und externen Traffic kontinuierlich zu prüfen und aufzuzeichnen, um jegliche heimtückische Aktivität mit Echtzeit-Schutzfunktionen zu überwachen.

Der auf der vorigen Seite zitierte Forrester-Bericht macht deutlich, was zu tun ist:

> „sichere Mikroperimeter erstellen, Verschleierungsmethoden verwenden, um die Datensicherheit zu erhöhen, exzessive Benutzerberechtigungen drosseln, um Risiken zu mindern und Automatisierung und Analysen einsetzen, um die Sicherheitserkennung und Security-Response zu verbessern. **Das Konzept eines vertrauenswürdigen internen Netzwerks und eines nicht vertrauenswürdigen externen Netzwerks muss verworfen werden** [unser Schwerpunkt]. Es verlangt, dass Sicherheitsteams alle Ressourcen unabhängig vom Standort prüfen und schützen, den Zugriff begrenzen und für alle Benutzer, Geräte, Kanäle und Hosting-Modelle streng durchsetzen, und den gesamten internen und externen Traffic protokollieren und überprüfen."

Auf diese und weitere Arten fördert Zero Trust eine Sicherheit, die im gesamten Netzwerk allgegenwärtig und proaktiv ist, nicht nur am Perimeter. Die Zero-Trust-Prinzipien minimieren effektiv die Angriffsfläche, die das Netzwerk bietet.

Es ist ebenso wichtig, den gesamten internen und externen Traffic kontinuierlich zu prüfen und aufzuzeichnen, um jegliche heimtückische Aktivität mit Echtzeit-Schutzfunktionen zu überwachen.

Erweiterte Herausforderungen für die Cloud-Sicherheit

Da die Public Cloud keine klaren Perimeter oder Eingangs- bzw. Ausgangsports hat, stehen Unternehmen, die in die Cloud migrieren, vor vollkommen anderen Sicherheitsanforderungen. Diese neuen Sicherheitsanforderungen werden noch schwieriger zu bewältigen, wenn man moderne Cloud-Ansätze wie automatisierte CI/CD-Methoden, verteilte serverlose Architekturen und flüchtige Assets wie Functions as a Service und Container verwendet.

In diesem Abschnitt besprechen wir die erweiterten Sicherheitsherausforderungen und die verschiedenen Risikostufen, denen die cloud-orientierten Unternehmen von heute gegenüberstehen.

Größere Angriffsfläche

Malware, Zero Day, die Übernahme von Konten und viele weitere bösartige Bedrohungen sind alltäglich geworden. Die Public Cloud ist zu einer großen und hochgradig attraktiven Angriffsfläche für Hacker geworden, die schlecht geschützte Eingangsports für Clouds ausnutzen wollen, um Zugriff auf Workloads und Daten in der Cloud zu erlangen und diese abzufangen. Jedes Unternehmen, das sich auf die Public Cloud einlässt, muss verstehen, dass sie allein durch die Nutzung der Cloud ihre Angriffsfläche erheblich vergrößert.

Ein Mangel an Sichtbarkeit und Tracking

Im Allgemeinen sind Cloud-Infrastrukturen für Unternehmen schlechter einsehbar als On-Premise-Infrastrukturen. Insbesondere Cloud-Assets sind häufig nicht sichtbar und schwer zu verwalten, was zu schwerwiegenden Lücken in der Sicherheitsdurchsetzung führt. Ohne Orchestrierungs-Tools der nächsten Generation können Cloud-Kunden ihre Cloud-Assets nicht effektiv identifizieren und quantifizieren oder ihre Cloud-Umgebungen visualisieren.

Sich ständig ändernde Arbeitsbelastung

Cloud Assets werden dynamisch bereitgestellt und stillgelegt - in großem Umfang und mit hoher Geschwindigkeit. Herkömmliche Sicherheitstools sind einfach nicht in der Lage, Schutzrichtlinien in solch einer flexiblen und dynamischen Umgebung durchzusetzen. Es sind neue Tools und Ansätze erforderlich, um die sich heutzutage ständig ändernden und temporären Workloads zu schützen.

DevOps, DevSecOps und Automation

Unternehmen, die hochgradig automatisierte DevOps in Form von Continuous Integration und Continuous Deployment (CI/CD) übernommen haben, müssen sicherstellen, dass angemessene Sicherheitskontrollen frühzeitig im Entwicklungszyklus im Code identifiziert und eingebettet sind. Sicherheitsbezogene Änderungen, die implementiert werden, nachdem Workload in der Produktion bereitgestellt wurde, können die Sicherheit von Unternehmen untergraben und die Zeit bis zur Markteinführung verzögern.

Granulare Berechtigungs- und Schlüsselverwaltung

Es kommt häufiger vor, das Cloud-Benutzerrollen sehr locker konfiguriert werden, so dass Benutzerberechtigungen erteilt werden, die nicht erwünscht oder erforderlich sind. Ein Beispiel, das häufig vorkommt, sind Lösch- oder Schreibberechtigungen für Datenbanken für Benutzer, die nicht geschult sind oder einfach keine Assets löschen oder hinzufügen sollen.

Die Situation auf Anwendungsebene ist ähnlich, wo unsachgemäß konfigurierte Schlüssel und Berechtigungen zu Sicherheitsrisiken aufgrund von Key-Leakage und schlecht geschützten Sessions führen.

Um das Zero-Trust-Prinzip aufrechtzuerhalten, müssen Benutzer- und Anwendungsberechtigungen auf einer hochgradig granularen Ebene durch flexible und dynamische Berechtigungsverwaltungstools verwaltet werden.

Multi-Cloud-Umgebung

Jeder Cloud-Anbieter bietet Tools und Dienste an, die seine Kunden bei der Überwachung und Sicherung ihrer Cloud-Ressourcen unterstützen. Es ist gut, diese Cloud-Provider-Tools in Ihren bestehenden Sicherheits-Stack zu integrieren, um Ihren Teil des Shared-Responsibility-Modells zu erfüllen.

Man muss sich jedoch bewusst sein, dass die Sicherheitstools eines bestimmten Providers nur für seine eigenen Cloud-Services gelten. Um die Sicherheit in Hybrid- und Multi-Cloud-Umgebungen, die momentan bevorzugt werden, konsistent verwalten zu können, benötigen Unternehmen Konfigurationsmanagement-, automatische Abhilfe- und Orchestrierungs-Tools, die reibungslos mit allen Public-Cloud-Providern, Private-Cloud-Providern und On-Premise-Bereitstellungen funktionieren.

Compliance und Bestimmungen

Die Einhaltung geltender Gesetze oder branchenspezifischer Bestimmungen muss bedacht werden, wenn man die Cloud verwendet. Um Ihren Teil des Shared-Responsibility-Modells in Bezug auf die Compliance zu erfüllen, haben alle führenden Cloud-Provider ihre Services an den bekanntesten Akkreditierungsprogrammen wie PCI 3.2, NIST 800-53, HIPAA und DSGVO ausgerichtet. Die Kunden sind jedoch dafür verantwortlich, dass ihre Workloads und Daten auf konforme Weise verarbeitet werden.

Außerdem kann der Compliance-Audit-Prozess angesichts der schlechten Sichtbarkeit und Dynamik von Cloud-Umgebungen mühselig sein, wenn die Kunden keine Tools verwenden, die kontinuierliche Compliance-Prüfungen in Echtzeit durchführen, um Fehlkonfigurationen aufzudecken, zu warnen und automatische Abhilfe zu schaffen, falls erforderlich.

Weitere Informationen zu Sicherheits- und Compliance-Problemen mit der Cloud finden Sie im Cloud-Security-Repository.

Prinzipien für die Cloud-Sicherheitsarchitektur

In diesem Abschnitt sehen wir uns die Architekturprinzipien an, die von jeder Cloud-Security-Unternehmenslösung angegangen werden müssen, um die Herausforderungen zu bewältigen, die durch begrenzte Sichtbarkeit, die Notwendigkeit eines granularen Autorisierungs- und Berechtigungsmanagements, einer reibungslosen Integration von automatisierten CI/CD-Prozessen, Konsistenz in komplexen Infrastrukturen und die Compliance-Anforderungen verursacht werden.

Sicherheit am Netzwerkperimeter mit Advanced Threat Prevention

In den letzten Jahren stieg die Häufigkeit der Angriffe deutlich an. Außerdem wurden sie immer ausgefeilter. Die Cloud vergrößert die Angriffsfläche und sorgt im Allgemeinen für neue Sicherheitsherausforderungen in Bezug auf Schwachstellenscans und den Schutz von Webanwendungen.

Wie oben erwähnt (siehe „Das Shared-Responsibility-Modell verstehen“) ist beim IaaS-Modell der Provider für die Sicherheit „außerhalb“ der Cloud verantwortlich, während der Kunde für den Schutz der Assets „in“ der Cloud sorgen muss. Daher ist der Kunde im Rahmen des Shared-Responsibility-Modells dafür verantwortlich, einen fortschrittlichen Best-in-Class-Schutz vor Bedrohungen zu implementieren und zu verhindern, dass das Netzwerkperimeter (d. h. die Hauptschnittstellen, wo der Traffic auf Ressourcen in der Cloud-Umgebung zugreift und diese verlässt) angegriffen wird.

Weitere Angriffsvektoren, die gesichert werden müssen

Weitere Angriffsvektoren, die vom Cloud-Sicherheitsdesign berücksichtigt werden müssen, sind:

DATEN	Ruhende Daten müssen in Cloud-Speichern wie Amazon S3, Azure Storage und Google Cloud Storage Bucket geschützt werden. Laufende Daten sollten mit Tools wie Amazon EFS Mount Helper, Azure Client-Side oder Server-Side Encryption und GCP-Verschlüsselung während der Übertragung verschlüsselt werden.
COMPUTE	Abgesehen von standardmäßigen virtuellen Computern muss eine Cloud-Sicherheitsarchitektur die hochgradig verteilten und dynamischen Anwendungsarchitekturen von heute beachten, die hauptsächlich auf serverlosen Architekturen, Microservices, Functions as a Services (FaaS), Infrastructure as Code (IaC) usw. basieren. Das Design sollten auch Schutz für die fortschrittlichen Cloud-PaaS-Produkte bieten, die diese Architekturen und Services unterstützten, u. a. AWS Lambda, Azure Functions, Google Cloud Functions, Amazon API Gateway, Amazon Elastic Container Registry und Azure API Management.
NACH-RICHTEN	Auf ähnliche Weise verwenden moderne Webanwendungen häufig durch Ereignisse ausgelöste Nachrichten, um zwischen ihren hochgradig verteilten Komponenten zu kommunizieren. Der Perimeterschutz muss für Managed Messaging Services wie Cloud Pub/Sub von Google Cloud, Azure Service Bus und Amazon Simple Notification (SNS) implementiert werden.
IDENTITÄT	Die Identität in Cloud-Umgebungen setzt sich aus dem Zugriff auf die Cloud-Umgebung (z. B. die Bereitstellung eines neuen Rechners) sowie dem Zugriff auf jede einzelne Ressource (z. B. RDP-Zugriff auf diesen neuen Rechner) zusammen. Diese sind häufig vollkommen getrennt und unterschiedlich. Es bleibt dem Kunden überlassen, Benutzer zu identifizieren und zu autorisieren, die Zugriff auf ihre Public-Cloud-Ressourcen erlangen wollen. Ein Schutz auf Steuerebene muss für die Services der Zugriffskontrolle des Providers implementiert werden, z. B. AWS Identity and Access Management (IAM) und Azure Active Directory. Darüber hinaus muss der Kunde Sicherheitsgruppen verwenden, um den Zugriff angemeldeter Benutzer auf Ressourcen in der Cloud dynamisch zu steuern.

Security by Design

Fehlkonfigurationen sind eine der häufigsten Ursachen für Datenpannen in der Cloud. Security by Design bedeutet, dass die Cloud-Sicherheitsarchitektur wann immer möglich die Designeigenschaften der Cloud-Infrastruktur nutzen sollte, um eine unabänderliche Sicherheit zu erreichen (d. h. eine Sicherheit, die nicht durch Fehlkonfigurationen von Richtlinien oder Umgehungen kompromittiert werden kann). Es könnte z. B. eine Anforderung geben, dass ein bestimmtes Cloud Data Repository niemals dem Internet ausgesetzt wird. Statt einer Firewall-Konfiguration wäre die zu bevorzugende Best Practice gemäß Security by Design, niemals einen Kontakt zwischen dem Repository und einem Hub zum Internet zuzulassen.

Dieser Security-by-Design-Ansatz ist ein weiteres Beispiel dafür, warum Zero Trust angewendet werden sollte, um Cloud-Assets effektiv zu schützen.

Segmentierung und Mikro-Segmentierung

In einer aktuellen Proofpoint-Studie von mehr als 100.000 unautorisierten Anmeldungen bei Millionen von überwachten Konten von Cloud-Benutzern ergab, dass einer von drei Verstößen eine laterale Bewegung zwischen zwei oder mehreren Punkten im Netzwerk beinhaltete. Nach dem Eindringen in das Netzwerkperimeter konnte der Angreifer andere Rechner im gleichen Netzwerk infizieren. Dieses Verhalten macht deutlich, dass das Grundprinzip des Zero-Trust-Modells implementiert werden muss, in dem das Netzwerk basierend auf Anwendungen und Services weiter segmentiert und ein Best-in-Class-Schutz zwischen diesen Segmenten platziert wird, sodass die Angreifer sich nicht frei bewegen können.

Um die Segmentierung im Rahmen des Zero-Trust-Modells zu implementieren und gleichzeitig eine ungehinderte Kommunikation zwischen Anwendungen zuzulassen, wird die Sicherheit für jedes Netzwerksegment an zwei Sicherheitskontrollpunkten durchgesetzt:

1. **Auf Zugriffsebene wird eine Firewall konfiguriert, um Traffic auf der Zulassungsliste zuzulassen, damit Apps normal ausgeführt werden können, während gleichzeitig unerwünschter Traffic blockiert wird.**

2. **Traffic, der auf der Zugriffsebene zugelassen ist, wird dann gründlich geprüft (auch als Deep Packet Inspection bezeichnet), um bösartiges Verhalten auf dem Anwendungs-/Datenlayer zu identifizieren und zu blockieren.**

Die Cloud-Sicherheitsarchitektur eines Unternehmens muss die Automatisierung von Prozessen und Aufgaben von Grund auf fördern.

Agilität

Die On-demand-, Elastizitäts- und Größen-Eigenschaften einer Public Cloud ermöglichen es Ihnen, Workloads für Ihr Unternehmen mit höherer Geschwindigkeit und größerer Agilität auszuführen und bereitzustellen. Moderne, effiziente Geschäftspraktiken sind nicht möglich, wenn es Wochen dauert, Server und Services bereitzustellen, oder wenn die Sicherheitsworkflows mühselig und zeitaufwendig sind.

Ihre Cloud-Sicherheitsarchitektur muss agil sein und gleichzeitig sicherstellen, dass die Geschwindigkeit nicht zu einem Kontrollverlust oder Geschäftsrisiko führt. Dieses Prinzip wird aufrechterhalten durch eine Verantwortungsaufteilung unter den verschiedenen Interessengruppen in der Organisation, die DevOps, Anwendungsbesitzern und anderen höhere Berechtigungen für ihre Ressourcen und Umgebungen geben. Mit Infrastructure as Code und anderen Methoden können DevOps-Teams einen Zugriffskontrollschutz innerhalb und zwischen ihren eigenen Workloads dynamisch und programmatisch implementieren und gleichzeitig den Perimeterschutz und die erweiterten Sicherheitsaufgaben den Netzwerk- und Sicherheitsteams überlassen.

Automatisierung, Effizienz und Elastizität

Cloud-Automatisierung bezieht sich allgemein auf alle Prozesse und Tools, die ein Unternehmen verwendet, um die manuellen Vorgänge bei der Bereitstellung und Verwaltung von Cloud-Ressourcen zu reduzieren. Das steht im starken Gegensatz zu herkömmlichen Sicherheitsansätzen, die sich größtenteils auf einen manuellen Schutz der Workloads und Ressourcen verlassen. Wenn die geschäftliche Agilität durch Sicherheitsengpässe behindert wird, werden diese umgangen oder einfach weit genug geöffnet. Beides kann Unternehmen einem erhöhten Risiko aussetzen.

Die Reduzierung des menschlichen Faktors in der Cloud-Sicherheit durch Automatisierung und programmatische Vorgänge unterstützt nicht nur die geschäftliche Agilität und die betriebliche Effizienz, sondern mindert auch das Risiko menschlicher Fehler (d. h. Fehlkonfigurationen), die eine bedeutende Rolle bei Sicherheitsverstößen spielen. Die Cloud-Sicherheitsarchitektur eines Unternehmens muss die Automatisierung von Prozessen und Aufgaben von Grund auf fördern. Angefangen in der Umgebungsbereitstellungsphase (z. B. durch vorkonfigurierte Vorlagen) und weiter im alltäglichen Betrieb, z. B. durch dynamische, adaptive Sicherheitsrichtlinien, die keine menschlichen Eingriffe erfordern.

Grenzenlos

Sehr viele Unternehmenskunden verwenden heutzutage eine Multi-Cloud-Strategie (d. h. mehrere Cloud-Provider in einer einzelnen und heterogenen Umgebung). Obwohl diese Strategie viele Vorteile hat, bringt die Nutzung einer Fülle neuer und aufkommender Technologien über mehrere Cloud-Provider an verschiedenen geografischen Standorten mehrere Sicherheitsherausforderungen mit sich, z. B.:

- Durchsetzung einer konsistenten Sicherheitsrichtlinie in allen Umgebungen.
- Etablierung einer einheitlichen und zentralisierten Verwaltung der Sicherheit des Unternehmens (d. h. Sicherheitsvorfälle von einer Stelle aus identifizieren und beheben)
- Sichere Verknüpfung verschiedener Cloud-Umgebungen über mehrere Standorte hinweg.
- Ermöglichung einer einfachen und sicheren Kommunikation zwischen Anwendungen, unabhängig vom Standort.
- Sichtbarkeit der Traffic-Flows innerhalb und zwischen den Standorten.

Daher muss eine effektive Cloud-Sicherheitsarchitektur plattformagnostisch sein. Die Architektur sollte eine einheitliche Richtlinie für alle Umgebungen (Public Cloud, Private Cloud und On-Premise) unterstützen, damit die Sicherheitsteams sich auf die Sicherheit konzentrieren können, anstatt sich mit dem wechselnden Kontext der providerspezifischen Sicherheitstools und -services aufzuhalten.

Compliance

Wie oben im Abschnitt „Compliance und Bestimmungen“ besprochen, stellt die Cloud die Compliance und Compliance-Audits vor große Herausforderungen. Die Cloud-Sicherheitsarchitektur eines Unternehmens muss sicherstellen, dass Workloads und Daten konform sind und dass Audits reibungslos durchgeführt werden können, sogar in komplexen Multi-Cloud- und Hybridinfrastrukturen.

Zusammenfassung

Die Hauptfaktoren für die Einführung von Clouds sind normalerweise Agilität, kürzere Markteinführungszeiten und die Möglichkeit schnellerer Innovationen. CISOs stehen vor der Herausforderung, die geschäftlichen Anforderungen an die Cloud-Übernahme und -Transformationen zu unterstützen, ohne Abstriche bei Sicherheit und Geschwindigkeit machen zu müssen.

In diesem Whitepaper erklären wir, warum Kunden ihre Cloud-Sicherheitsstrategie überdenken und Cloud-Sicherheitsarchitekturen implementieren müssen, die:

- Flexiblere und agilere Sicherheitslösungen ermöglichen
- Alle geschäftlichen Vorteile der Cloud auf sichere Weise bieten
- Einen fortschrittlichen und umfassenden Bedrohungsschutz bieten

Bei der Migration moderner und herkömmlicher Workloads in die Public Clouds müssen Unternehmen jedoch ihre Rolle im Shared-Responsibility-Modell verstehen. Beim IaaS-Modell ist der Provider z. B. für den Schutz der Infrastruktur selbst verantwortlich, während Kunden ihre eigenen Daten, Anwendungen und Workloads schützen müssen. Diese Aufgabe wird sogar noch komplexer, wenn man andere Cloud-native Services wie PaaS und SaaS hinzufügt.

Die von Cloud-Providern angebotenen Tools, die Kunden bei der Implementierung sicherer Cloud-Bereitstellungen helfen sollen, sind häufig angesichts der fortschrittlichen Bedrohungen von heute ungenügend. Es ist auch schwierig, Multi-Cloud- und Hybridumgebungen mit einem fragmentierten Stack aus providerspezifischen Tools zu verwalten.

In Anbetracht der Fortschrittlichkeit und der Menge der heutigen Bedrohungen muss die Cloud-Sicherheit einen Zero-Trust-Ansatz übernehmen, bei dem Benutzern oder Computern nicht automatisch vertraut wird. Benutzer sollten nur minimale Berechtigungen erhalten, d. h. nur diejenigen, die sie für ihre Aufgaben benötigen. Der gesamte Traffic muss überprüft und die Angriffsflächen durch eine effektive Netzwerksegmentierung minimiert werden. Mikrosegmentierungen von softwaredefinierten Netzwerken und verteilten App-Architekturen erhöhen die Sicherheit weiter.

Es gibt mehrere Grundprinzipien, auf denen jede Cloud-Sicherheitsarchitektur basieren sollte:

- Fortschrittliche Sicherheit für Netzwerke sowie die Angriffsvektoren Daten, Compute, Nachrichten und Identität.
- Systematische Separation aller Traffic-Flows (an, aus und innerhalb von Cloud-Umgebungen).
- Segmentierung durch Anwendungen oder Services und Mikrosegmentierung von Hosts, die im gleichen Segment oder remote ausgeführt werden.
- Erhöhte Agilität für DevOps und Geschäftszweige, ohne die Sicherheit des gesamten Unternehmens zu beeinträchtigen.
- Automatisierung, Effizienz und Elastizität, um die Geschwindigkeit des Geschäfts aufrechtzuerhalten, während das Risiko durch menschliche Fehler und Fehlkonfigurationen durch eine Einbettung der Sicherheit im Code reduziert wird.
- Eine plattformagnostische, grenzenlose Architektur, in der Sicherheitsrichtlinien konsistent über alle Umgebungen hinweg durchgesetzt werden können.

Sie finden eine Diskussion zum Blueprint 2.0 Implementierungsmodell und praktischen Lösungen unter hier. Detaillierte Leitfäden zur technischen Implementierung von Blueprint 2.0 für führende Cloud-Service provider finden Sie unter hier und hier.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: +972 3-753-4555 | Fax: 972-3-624-1100 | E-Mail: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070, USA | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2019 Check Point Software Technologies Ltd. Alle Rechte vorbehalten.