WAS BEDEUTET MULTI CLOUD? CHANCEN UND NEUE SECURITY-HERAUSFORDERUNGEN

CHANCEN UND RISIKEN DER CLOUD-DIVERSIFIKATION

Cloud-Anbieter müssen sich heutzutage wie im siebten Himmel fühlen, denn ihr Markt ist in nur wenigen Jahren explosionsartig gewachsen. Er hat sich von einer Nischenplattform, die anfangs nur von mutigen Spitzentechnologieunternehmen genutzt wurde, zu einem Standardkonzept mit Cloud-Priorität für den Betrieb aller Arten von geschäftskritischen Systeme entwickelt. Laut IDC werden bis 2019 nahezu 50 % der IT-Infrastrukturausgaben auf Private und Public Clouds entfallen.[1]

Heutzutage werden diese Ausgaben für eine größere Vielfalt von Cloud-Diensten eingesetzt. Laut RightScale nutzen Unternehmen durchschnittlich 1,8 Infrastructure-as-a-Service(IaaS)-Clouds.[2] Okta fand heraus, dass Unternehmen durchschnittlich 13 Software-as-a-Service(SaaS)-Anwendungen nutzen.[3]

Da IT-Abteilungen die Einführung von Multi-Cloud-Lösungen vorantreiben, muss die Verantwortung für Anwendungen und Rechenlasten, die durch unterschiedliche Cloud-Security-Implementierungen geschützt sind, weiterhin bei den CISOs bleiben. CISOs können sich über die SLAs ihrer Cloud-Anbieter ärgern oder aber auch die Dinge selbst in die Hand nehmen, und zwar, indem sie bei der Multi-Cloud-Sicherheit einen Fabric-Ansatz verfolgen. Eine auf offenen Standards basierende Fabric aus integrierten und anpassungsfähigen Security-Produkten bietet End-to-End-Sichtbarkeit und eine koordinierte Reaktion auf Bedrohungen. Sie hilft Unternehmen, das Beste aus ihren Multi-Cloud-Umgebungen herauszuholen.

DIE FÜHRENDEN 5 PUBLIC-IAAS-ANBIETER[4]

- AWS
- Microsoft Azure
- Google Cloud
- IBM
- Oracle Cloud

DIE FÜHRENDEN 10 SAAS-ANWENDUNGEN NACH MARKTANTEIL[5]

- Salesforce
- Microsoft
- Adobe
- SAP
- ADP
- Google
- IBM
- Intuit
- Oracle
- Workday

DER AKTUELLE STAND VON MULTI CLOUD

Die Multi-Cloud-Umgebung eines Unternehmens kann alle oder beliebig viele der folgenden Punkte umfassen:

- Public und Private Clouds, die Plattform-as-a-Service(PaaS)- oder Infrastructure-as-a-Service(IaaS)-Angebote bereitstellen
- Public und Private Clouds, die Software-as-a-Service(SaaS)-Anwendungen hosten
- Hybrid Clouds, die lokale Rechenzentren mit Public oder Private Cloud-Diensten kombinieren

Unternehmen fühlen sich mit mehreren Clouds zunehmend wohler. Eine Umfrage unter Unternehmen mit mindestens 1.000 Beschäftigten ergab, dass 85 % der befragten Unternehmen entweder Hybrid Clouds (58 %), mehrere Public Clouds (20 %) oder mehrere Private Clouds (7 %) im Einsatz haben.[6] Laut einer Untersuchung von Fortinet verwenden Unternehmen mittlerweile durchschnittlich 62 verschiedenen Cloud-Anwendungen, was etwa einem Drittel ihrer Anwendungen entspricht.[7]

85 % der Unternehmen nutzen mehrere Clouds

Diese Begeisterung bei der Cloud-Nutzung bedeutet für CISOs, dass sie einen steinigen Weg vor sich haben.

INHÄRENTE HERAUSFORDERUNGEN EINER MULTI-CLOUD-EINFÜHRUNG

Die Antriebsfaktoren für eine Umstellung auf die Cloud waren schon immer die Notwendigkeit von mehr Kosteneffizienz, besserer Ausfallsicherheit und einfacherer Skalierbarkeit. Mehrere Clouds bieten den zusätzlichen Vorteil der Resilienz über Service Provider hinweg und vermeiden die Abhängigkeit von einem einzelnen Anbieter.

Es gibt jedoch einige Sicherheitsbedenken, die diese Vorteile schmälern:

Steigende Angriffsfläche. Wenn bereits die Umstellung auf nur eine Cloud die Angriffsfläche vergrößert, ist dies bei mehreren Clouds umso mehr der Fall (siehe *Abbildung 1*). Wie kann ein Unternehmen den Schutz so skalieren, dass Wachstum und Schwankungen bei Multi-Cloud-Rechenlasten berücksichtigt werden?

Eindämmung von Bedrohungen. Wenn Rechenlasten über mehrere Clouds verteilt werden, breiten sich auch Bedrohungen leichter auf Orte aus, die außerhalb der Kontrolle der IT-Abteilung liegen. Segmentierung ist eine bewährte Vorgehensweise für die Eindämmung von Bedrohungen. Aber wie kann das Security-Team Anwender und Anwendungen in lokalen, IaaS- und SaaS-Umgebungen segmentieren?

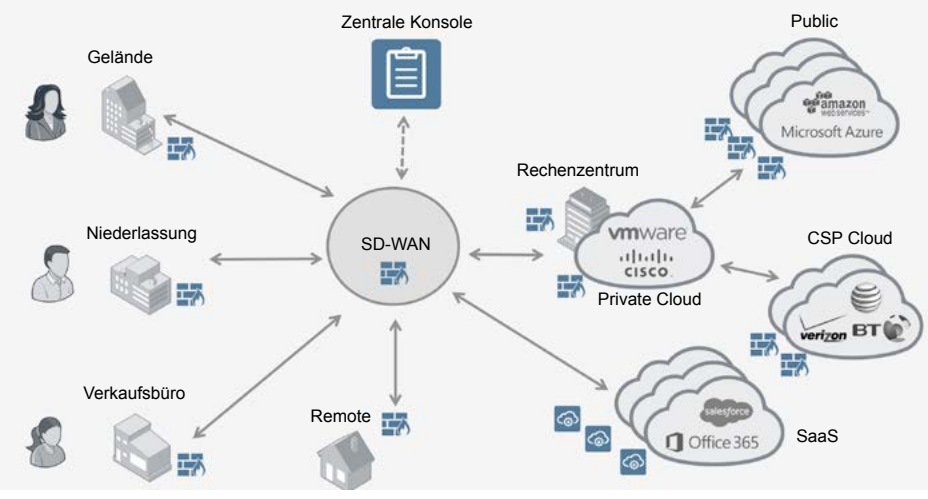

ABBILDUNG 1. DIE ERWEITERTE ANGRIFFSFLÄCHE EINER MULTI-CLOUD-UMGEBUNG

Rechenschaftspflicht. Jeder Cloud-Anbieter ist nur für die Infrastruktur oder Anwendungen verantwortlich, die er selbst hostet. Wie können CISOs die Angriffsquelle herausfinden, wenn sich Daten – und damit auch Angriffsvektoren – schnell zwischen dem Unternehmen und seinen verschiedenen Clouds hin und her bewegen? Es wird wahrscheinlich schnell mit dem Finger auf irgendwelche Anbieter gezeigt, aber letztendlich muss der CISO vor der Unternehmensleitung und den Aktionären Rede und Antwort stehen.

WARUM DIE ÜBLICHE CLOUD SECURITY FÜR MULTI CLOUD NICHT AUSREICHT

Jeder vernünftige Cloud-Anbieter hat ein großes Interesse an der Sicherheit der Anwendungen und Infrastruktur seiner Kunden. Und jeder Anbieter wird Argumente für die Vorteile seiner eigenen Cloud-Security-Funktionen vorbringen. Multi-Cloud-Anwender werden jedoch mit einer Vielzahl unterschiedlicher Sicherheitstechnologien, Plattformen und Management-Tools in Berührung kommen. Für die Security-Abteilung des Anwenderunternehmens stellt dies ein paar Herausforderungen dar:

Schlechte Sichtbarkeit Da CISOs für das gesamte Portfolio von Unternehmensanwendungen und Datenbeständen verantwortlich sind, müssen sie in der Lage sein, die Sicherheit des Portfolios in seiner Gesamtheit zu beurteilen. Selbstverständlich haben sie über cloudspezifische Portale Einblick in jede einzelne Cloud, sie können aber nicht die Bedrohungen sehen, die übergreifend über verschiedene Clouds (die normalerweise nicht miteinander kommunizieren) hinweg bestehen. Auch können sie nicht einschätzen, welche Auswirkungen die Bedrohungen in einer Cloud auf das gesamte Unternehmen haben.

Mangelnde Koordination. Da Multi-Cloud-Umgebungen einem Naben-und-Speichen-Modell (hub-and-spoke) ähneln, haben es CISOs schwer, die Bedrohungen in allen Clouds gleichzeitig zu erkennen und darauf zu reagieren. Ohne die Abstimmung von Security-Funktionen aufeinander und ohne zentrale Orchestrierung ist eine koordinierte Reaktion zur Eindämmung der Auswirkungen nicht möglich.[8]

Hohe Gesamtkosten (TCO), reaktive Sicherheit. Zweifellos tun CISOs alles in ihrer Macht stehende. Jedoch verursachen sie wahrscheinlich in einer Multi-Cloud-Umgebung viel höhere Kosten für die Konsolidierung des Security-Status als dies mit nur einer einzigen Cloud der Fall war. Außerdem drängt die Zeit. Heutzutage haben Unternehmen angesichts von Zero-Day-Bedrohungen und immer kürzeren Zeitfenstern zwischen Eindringen und Sicherheitsverstoß nicht den Luxus, Stunden damit zu verbringen, Daten aus unterschiedlichen Cloud-Management-Portalen abzugleichen und zu aggregieren oder Signale aus verschiedenen Clouds zu vergleichen und dann über geeignete Maßnahmen zu entscheiden.

DIE ZUKUNFT DER MULTI CLOUD SECURITY: EIN FABRIC-ANSATZ

Die Bewältigung der Herausforderungen einer Multi-Cloud-Umgebung erfordert einen ganzheitlicheren Ansatz, der die Kontrolle wieder in die Hände der Security-Abteilung des Unternehmens legt. Es wird also eine umfassende Suite von Tools zur Prävention, Erkennung und Abwehr von Bedrohungen benötigt, die sich in alle wichtigen Cloud-Dienste integrieren lässt und innerhalb des Unternehmens über eine zentrale Konsole verwaltet werden können.

Das mag sich zwar wie eine Plattformlösung anhören, es ist aber keine. Eine Plattform ist einfach ein locker zusammenhängendes Set von Produkten. Eine Security Fabricjedoch ist kein Produkt, sondern vielmehr ein architektonischer Ansatz, der auf offenen Standards und Protokollen basiert und verschiedene Security-Produkte – einschließlich Security-Plattformen – zu einem zentralen, das Multi-Cloud-Netzwerk überspannende Sicherheitssystem zusammenfügt. Anstatt der Naben-und-Speichen-Struktur des Multi-Cloud-Netzwerks zu folgen, handelt es sich bei der Fabric um ein maschenartiges Sicherheitsnetzwerk, in dem alle Security-Funktionen untereinander und mit einer zentralen Verwaltungskonsole kommunizieren können.

Eine Security Fabricbietet nicht nur End-to-End-Sichtbarkeit, sondern ermöglicht auch End-to-End-Erreichbarkeit. Die Security-Abteilung kann Patches verwalten und priorisieren, ein Eindringen, egal wo es auftritt, schnell identifizieren und stoppen und dessen Auswirkungen auf den Rest des Netzwerks mildern. Schließlich ermöglicht die zentral verwaltete Security Fabric eine umfassende Ereignisanalyse und verschafft CISOs ein klares Bild über den Security-Status des gesamten Unternehmens, das sie selbstbewusst in den Sitzungssaal mitnehmen können.

[1] „Growth in Cloud IT Infrastructure Spending Will Accelerate in 2017 Driven by Public Cloud Datacenters and On-Premises Private Cloud Environments“, IDC, 13. Januar 2017.

[2] „RightScale 2017 State of the Cloud Report“, RightScale, 2017.

[3] Chris Burt, „Slack May be Sexier, but Office 365 Most Used Cloud-based Business App“, WHIR, 29. März 2016.

[4] „RightScale 2017 State of the Cloud Report“, RightScale, 2017.

[5] „Microsoft Leads in SaaS Market; Salesforce, Adobe, Oracle and SAP Follow“, Synergy Research Group, 31. August 2017.

[6] „RightScale 2017 State of the Cloud Report“, abgerufen am 29. November 2017.

[7] „Fortinet Threat Landscape Report Q3 2017“, abgerufen am 29. November 2017.

[8] Matthew Pley, „Securing the Multi-Cloud: It’s Harder Than It Looks“, SDxCentral, 17. November 2017.

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Telefon:
+49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Telefon:
+41 44 833 68 48

ÖSTERREICH
Wienerbergstr. 11
Turm A 9.OG
1100 Wien
Österreich
Verkaufsabteilung:
+43 1 3760013-0

HAUPTSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Telefon:
+1 408 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Telefon:
+33 4 8987 0500

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Telefon:
+65 6513 3730

LATEINAMERIKA ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Telefon:
+1 954 368 9990

September7,20182:32nachm.

wp-multi-cloud-update-a4_DE