FORTINET

WHITEPAPER

Schutz von dynamischen Cloud-Umgebungen

Paradigmenwechsel: Neue Anforderungen an Ihre Checkliste für Sicherheitslösungen

Cloud Computing hat die Art und Weise verändert, wie wir IT-Lösungen nutzen und bereitstellen. In rasantem Tempo entwickelt sich Rechenleistung immer mehr zu einem „Versorgermodell“, das auf einer gemeinsamen Infrastruktur basiert. Diese gemeinsame Infrastruktur bildet nicht nur das Fundament der Cloud-Revolution, sondern hat auch zu einer grundlegenden Veränderung bei der Entwicklung von Technologie und ihrer Implementierung im Rechenzentrum geführt. Server, Speicher, Netzwerke und sogar das Rechenzentrum selbst haben die physischen Grenzen überschritten und sind zu virtualisierten Diensten geworden, die sich auf physischer Hardware befinden. Mit diesem neuen virtuellen, gemeinsam genutzten Infrastrukturmodell gehen jedoch auch neue Risiken einher.

Laut IDC erwägen 75 % der Unternehmen die Implementierung einer Public Cloud oder haben diesen Schritt bereits getan. Weiter hat IDC prognostiziert, dass 50 % der Workloads bis 2018 in die Cloud verlagert werden. Gleichzeitig steigt die Zahl der Bedrohungen unablässig. Security-Teams müssen heutzutage weitaus gefährlichere Bedrohungen abwehren als vereinzelte Hacker, die ein Schlupfloch ins Netzwerk suchen. Der Ost-West-Traffic – der Datenverkehr zwischen Systemen innerhalb des Netzwerks – dominiert jetzt den Datenfluss im Unternehmen. Hybrid-Cloud-Umgebungen verbinden Unternehmenssysteme und -anwendungen mit externen Datenquellen und Kunden. Privat-Cloud-Implementierungen bieten Anwendungsentwicklern Rechenleistung „as a Service“, um neue Funktionen für interne und externe Benutzer bereitzustellen. Das Netzwerk-Designparadigma für Rechenzentren ist mittlerweile flacher. Die Folge: Dringen jetzt Kriminelle in das Unternehmensnetzwerk ein, wird das Netzwerk Bedrohungen ausgesetzt, die tage- oder wochenlang unentdeckt bleiben und manchmal wie terroristische Schläfer nur auf den richtigen Moment warten, um Chaos zu verursachen oder vertrauliche Daten abzugreifen. Es überrascht kaum, das diese Art von Bedrohungen den Cloud-Security-Verantwortlichen schlaflose Nächte bereiten.

Im Folgenden werden die wesentlichen Elemente umrissen, die bei einer Cloud-Security-Lösung zu berücksichtigen sind. Dabei darf nicht vergessen werden, dass das vorrangige Ziel oft nicht nur die Verhinderung einer Sicherheitsverletzung ist. Auch muss realistischerweise davon ausgegangen werden, dass Sicherheitsverletzungen unvermeidbar sind – und trotzdem gewährleistet werden kann, dass alle Komponenten einer Cloud-Lösung jederzeit ausfallsicher und geschützt sind.

Sicherheit für Public Clouds

Die Public-Cloud-Security ist das Sicherheitsrisiko Nr. 1. Sowohl Führungskräfte als auch Benutzer haben erst kürzlich die tief verwurzelte Skepsis überwunden, Systeme und Bandbreite mit unbekannten Dritten zu teilen. Bedenken hinsichtlich der Cloud-Security waren bis vor kurzem ein Grund, warum viele sich nur zögerlich auf die Public Cloud wagten. Für eine effektive Public-Cloud-Security müssen zwei Hauptelemente berücksichtigt werden: ein gemeinsames Sicherheitsmodell und die Integration von Anbietern.

Gemeinsames Sicherheitsmodell: Das gemeinsame Sicherheitsmodell muss nicht nur der Ansatz sein, den Security-Teams beim Schutz der Cloud verfolgen. Auch müssen von Unternehmen implementierte Lösungen flexibel genug sein, um gemeinsame Security-Funktionen zu unterstützen. Das gemeinsame Sicherheitsmodell besteht aus zwei Kernelementen: der Sicherheit der Cloud-Plattform, die alle Rechenzentrums-Komponenten des Cloud-Anbieters umfasst, und der Sicherheit in der Cloud, die alles betrifft, was Sie in der Cloud bereitstellen. Sie sind für die Kundenseite zuständig: für Ihre Daten und Anwendungen, Betriebssysteme, das Zugangs- und Identitätsmanagement, die Verschlüsselung und den Netzwerk-Datenverkehr. Eine sinnvolle Sicherheitslösung muss mit dem Security-Framework des Cloud-Anbieters integriert werden – das den Schutz von Rechenleistung, Speicher und Netzwerk übernimmt – und zudem ein gemeinsames Dashboard umfassen, das die Anbieterseite *und* die Kundenseite der Cloud-Security anzeigt und das Management aller Aspekte der Lösung erlaubt.

Die Beantwortung dieser drei Fragen bildet einen Startpunkt, von dem aus Security-Experten die Anforderungen an eine IoT-Sicherheitslösung definieren können. Die Transformation der IoT-Grenze in eine gehärtete Außengrenze – oder zumindest der Gewinn von Transparenz, um Bedrohungen zu erkennen und einen Angriff zu verhindern – ist der Ausgangspunkt für jede neue Lösung.

Anbieter-Integration: Neben der Abgrenzung der Verantwortungsbereiche und der Vergewisserung, dass der Schutz keine Lücken aufweist, müssen die Lösungen eng mit dem Public-Cloud-Anbieter integriert werden. Nur das gewährleistet die Sicherheit der Public Cloud. Das alte Paradigma – die Bereitstellung von Appliances oder hostbasierten Agenten – funktioniert für die Public-Cloud-Security nicht mehr. Solche Lösungen bieten keine End-to-End-Transparenz über alle Knoten hinweg und lassen sich selten mit der für eine Cloud-Lösung notwendigen Elastizität skalieren. Wer z. B. Amazon Web Services nutzt, kennt das Konzept der „Sicherheitsgruppen“ für eine

rudimentäre Segmentierung. Selbst AWS rät jedoch zu externen Security-Lösungen, um Funktionen wie Application Control, Antivirus, Webfilter, DLP und neueste Bedrohungsdaten hinzuzufügen. Im Kontext der Public Cloud müssen diese Lösungen automatisch mit der Cloud anhand von Vorlagen skaliert werden, damit bei einer dynamischen Erweiterung der Cloud-Ressourcen weiterhin ein hohes Maß an Verfügbarkeit und Leistung gegeben ist. Bei Microsoft Azure muss eine Sicherheitslösung dagegen per Plug-and-Play mit den APIs für den Microsoft Azure Resource Manager integrierbar sein, um von sämtlichen Security-Funktionen zu profitieren.

Sicherheit für Private Clouds

Die Grundlage jeder Private Cloud ist die Virtualisierung – de facto dient die Virtualisierung als Baustein für alle Formen des Cloud Computing. Zudem hat die Virtualisierung zu stärker softwareorientierten Computer-Umgebungen geführt, was eine Cloud-Security-Lösung ebenfalls berücksichtigen muss.

Software-Defined Security: Mit dem Wachstum von Software Defined Networking (SDN) sind Netzwerk-Ressourcen – ähnlich wie die Cloud selbst – nicht mehr physisch an bestimmte Hardware gebunden. Netzwerk-Ressourcen werden jetzt als Dienste im Rechenzentrum ausgeführt und können über physische Elemente oder Standorte hinweg arbeiten. Dieser Aspekt sollte bei einer Cloud-Security-Lösung von Grund auf berücksichtigt worden sein. In anderen Worten: Die Lösung muss mehr bieten als spezielle Appliances, um Ressourcen effektiv zu schützen. Security-Funktionen müssen „as a Service“ dynamisch konfiguriert und bereitgestellt werden können.

Erfüllt Ihre Lösung die funktionellen Anforderungen von Public, Private und Hybrid Clouds?

Sicherheit für Public Clouds

- Gemeinsames Sicherheitsmodell
- Anbieter-Integration

Sicherheit für Private Clouds

- Software-Defined Security
- Anwendungszentrierte Security

Hybrid Clouds

- Zentrale Konsole
- Segmentierung
- Sichere Konnektivität

Anwendungszentrierte Security: Nicht alle Anwendungen sind gleich. Obwohl viele Anwendungen dieselbe physische Infrastruktur einer Private Cloud nutzen, unterscheidet sich ihr Risikoprofil. Genau deshalb ist die Segmentierung von entscheidender Bedeutung. Darüber hinaus muss die Security-Lösung auf die Anwendung abstimmbar sein. Jede cloudbasierte Security-Lösung muss zudem Daten und Anwendungen isolieren können und gleichzeitig die Konsolidierung des Rechenzentrums unterstützen. Da der Ost-West-Verkehr in softwaredefinierten Umgebungen zunimmt, wird auch die Mikrosegmentierung – die Fähigkeit zur weiteren Trennung spezifischer Verkehrsarten – zu einer kritischen Anforderung.

Hybrid Clouds

Die Hybrid Cloud ist womöglich das größte Problem bei der Entscheidung für die am besten geeignete Security-Lösung. Da eine Hybrid Cloud sowohl vom Unternehmen kontrollierte Ressourcen als auch die Public-Cloud-Infrastruktur oder bestimmte SaaS- oder Datenressourcen umfasst, ist Transparenz entscheidend. Nur so kann Ihr Security-Team die Gesamtlage von „A bis Z“ überblicken. Ein End-to-End-Management, Möglichkeiten zur Segmentierung und der Schutz externer Verbindungen sind die wichtigsten Elemente einer Security-Lösung für Hybrid Clouds.

Verwaltung über eine zentrale Konsole: Da die Ressourcen sowohl im physischen als auch im virtuellen Raum verteilt sind, sollten Security-Experten jederzeit den Überblick behalten können – und nicht ständig zwischen mehreren Dashboards hin- und herwechseln oder ohne zentrale Analysefunktionen für Bedrohungsdaten arbeiten müssen. Isolierte Einzellösungen mit getrennten Management-Schnittstellen reichen nicht aus. Eine Cloud-Security-Lösung muss alle in der Cloud betriebenen Systeme in eine zentrale Verwaltung integrieren und in einer einheitlichen Übersicht abbilden. Denn mit einem zentralisierten Management lassen sich Datenströme im gesamten Netzwerk in einem Format verfolgen, das diese Informationen relevant und verwertbar macht. Dazu sollten auch zentralisierte Bedrohungsdaten gehören, die informierte Entscheidungen je nach Entwicklungen im Netzwerk oder in der „Außenwelt“ unterstützen.

Segmentierung: Die Segmentierung von Systemen und Datenverkehr innerhalb und außerhalb der Cloud ist am kritischsten, wenn sich interne Ressourcen in einem Netzwerk befinden, das für die Öffentlichkeit oder Dritte zugänglich ist. In diesen gemischten Umgebungen – die sowohl permanente externe Verbindungen als auch temporäre Datenbewegungen umfassen – müssen Geschäftsbereiche und kritische Anwendungen, die nicht direkt mit der Hybrid-Umgebung verbunden sind, segmentiert werden, um die Folgen einer Sicherheitsverletzung proaktiv zu minimieren.

Sichere Konnektivität: Jede hybride Lösung muss eine robuste VPN-Funktionalität unterstützen, um bei Bedarf einen sicheren temporären Zugriff auf Ressourcen zu erlauben und zugleich das restliche Netzwerk zu schützen. Die Migration von Daten zwischen Standorten, das Laden großer Datenmengen aus externen Quellen und die Nutzung von externen cloudbasierten Analyse-Diensten erfordern diskrete Verbindungen zu externen Netzwerken, die mit besonderen Risiken einhergehen. Eine Lösung muss in der Lage sein, den richtigen Schutz basierend auf dem Risikoprofil dieser spezifischen Netzwerk-Verbindungen zu bieten.

Sicherheit im Einklang mit dem Cloud-Paradigma

Neben dem Schutz der Cloud in ihren verschiedenen Implementierungsformen (Public, Private und Hybrid) muss eine Cloud-Security-Lösung auch so funktionieren, dass sie dem Wesen der Cloud entspricht: als elastische, dynamische Ressource, die sich rasch ändern kann. Die Lösung sollte daher drei wesentliche Aspekte der Cloud berücksichtigen:

Skalierbar: Da die Cloud dynamisch ist und ihre Skalierbarkeit oft der Grund für die Verlagerung von Anwendungen in die Cloud ist, sollte das Design einer Security-Lösung der Skalierbarkeit und Elastizität von Cloud-Workloads entsprechen. Lösungen, die statisch sind oder keine Automatisierung aufweisen und manuelle Eingriffe zur Erweiterung oder Anpassung an neue Anforderungen erfordern, behindern die Sicherheit – und die maximale Wertschöpfung aus einer Cloud-Lösung. Bei der Bewertung sollte unbedingt darauf geachtet werden, dass die Cloud-Security-Lösung umfassend automatisierbar ist. Auch müssen sich Risiko- und Zugriffsrichtlinien vorab definieren lassen, damit neue Geräte im Netzwerk automatisch konfiguriert werden können, wenn mehr Benutzer oder zusätzliche Bandbreite in der Cloud-Umgebung hinzukommen. Kann die Lösung an die Elastizität und das dynamische Wachstum einer Cloud-Umgebung angepasst werden?

Einheitlich: Bedrohungen werden dann zu einer verheerenden Gefahr, wenn Zeitpunkt und Gelegenheit stimmen. Oft werden uneinheitliche oder inkonsequent durchgesetzte Richtlinien ausgenutzt, um sich zu Ihrem Netzwerk Zugang zu verschaffen. Mit der Cloud steigen die Anforderungen an eine einheitliche, konsequente Security um ein Vielfaches: Clouds bringen neue Variablen ins Spiel, wie temporäre oder wiederkehrende Verbindungen zu externen Ressourcen oder auch ein dynamisches, bedarfsorientiertes Erweitern oder Deaktivieren von Ressourcen. Richtlinien, Durchsetzung und deren Automatisierung müssen einheitlich für statische und dynamische Ressourcen angewendet werden. Workloads oder Systeme, die mit dem gleichen Risikoprofil kategorisiert sind, müssen beim Eintritt in das Netzwerk und beim Verlassen des Netzwerks identisch behandelt werden – unabhängig davon, ob sie sich in Ihrem Rechenzentrum oder bei externen Anbietern befinden. Kann die einheitliche Durchsetzung von Richtlinien, Transparenz und Security in der gesamten Cloud jederzeit gewährleistet werden?

Segmentiert: Unabhängig davon, ob Sie das Geschäftsrisiko minimieren oder gesetzliche Vorschriften erfüllen müssen – mit der Cloud kommen neue Elemente beim Sicherheitsprotokoll auf Sie zu. Die Möglichkeit, Systeme, Workloads oder sogar bestimmte Netzwerk-Komponenten zu segmentieren, ist für das geschäftliche Risiko-Management entscheidend. Die Cloud bringt zudem neue Probleme bei der Compliance-Erfüllung mit sich: Werden Daten nicht nur in Ihrem Netzwerk übertragen, sondern können das interne Netzwerk über die Public Cloud verlassen, muss die Datenkonformität durchsetzbar sein. Nur so lässt sich sicherstellen, dass Sie bestimmten Datenverkehr, bestimmte Anwendungen und spezielle Arten von Daten überwachen und kontrollieren können. Für eine korrekte Segmentierung in der Cloud muss auch der persistente Datenverkehr zwischen Cloud-Segmenten auf Datenverluste überprüfbar und die Weiterleitung von Daten basierend auf Risiken und Richtlinien gegeben sein. Lassen sich kritische Systeme, Workloads und Anwendungen anhand eindeutiger Risikoprofile trennen?

Reflektiert Ihre Lösungsplanung das Security-Paradigma der Cloud?

Skalierbar

Kann die Lösung an die Elastizität und das dynamische Wachstum einer Cloud-Umgebung angepasst werden?

Einheitlich

Kann die einheitliche Durchsetzung von Richtlinien, Transparenz und Security in der gesamten Cloud jederzeit gewährleistet werden?

Segmentiert

Lassen sich kritische Systeme, Workloads und Anwendungen anhand eindeutiger Risikoprofile trennen?

Fazit

Das Cloud Computing hat das Paradigma für IT- und Security-Experten geändert. Die Zeiten von Netzwerken mit genau definierten Perimetern, in denen der Schutz vor externen Bedrohungen sich ausschließlich auf die Firewall konzentrierte, sind vorbei. Cloud-Security-Lösungen müssen die speziellen Anforderungen jeder Cloud-Computing-Variante erfüllen: von Public Clouds mit ihrer Abhängigkeit von einer gemeinsamen Infrastruktur und der Notwendigkeit, mit einem gemeinsamen Sicherheitsmodell zu arbeiten, von Privat Clouds mit den inhärenten Risiken des Ost-West-Verkehrs und virtualisierter Dienste, die einen softwaredefinierten Sicherheitsansatz erfordern, und von Hybrid Clouds, die eine kombinierte Security für kritische interne Ressourcen, externe Verbindungen und Datenquellen benötigen und zunehmend die Segmentierung von Netzwerk-Ressourcen unabdingbar machen.

Zugleich muss eine Security-Lösung der Skalierbarkeit der Cloud entsprechen, Richtlinien einheitlich anwenden und diese über interne wie externe segmentierte Ressourcen hinweg konsequent durchsetzen können. Mit einer solchen Mischung aus Funktionalität und struktureller Stringenz lassen sich cloudimmanente Sicherheitsprobleme erfolgreich in den Griff bekommen. Gleichzeitig kann das Unternehmen so maximal von den Vorteilen der Cloud profitieren und die geschäftlichen Risiken einer gemeinsam genutzten öffentlichen Infrastruktur auf ein Minimum begrenzen.

FORTINET

www.fortinet.com/de

29. Juni 2020, 11:10 Uhr

122915-B-0-DE