Entwicklung der Cloud-Nutzung

Praktische Hinweise und der Stand der Dinge bei Cloud-Sicherheit

Kurzfassung

Während Verarbeitung, Speicherung und Zusammenarbeit zunehmend Cloud-basiert erfolgen, kämpfen IT-Experten damit, die Sicherheit ihrer Ressourcen zu gewährleisten. 97 % aller Unternehmen weltweit nutzen irgendeine Form von Cloud-Dienst und kämpfen mit Herausforderungen in Bezug auf Transparenz und Kontrolle. Einige Führungskräfte vollziehen den Wechsel in die Cloud aufgrund der unzureichenden Transparenz nur langsam, während andere trotz des Wissens um die Sicherheitsrisiken energisch voranschreiten.

Für diesen Jahresbericht zum Stand der Dinge bei der Cloud-Sicherheit und der Migration zur Cloud führte McAfee® Ende 2017 eine Umfrage unter 1.400 IT-Experten aus unterschiedlichen Branchen und Ländern sowie Unternehmen verschiedenster Größen durch. Das wichtigste Ziel des diesjährigen Berichts besteht in praktischen Hinweisen zu den empfohlenen Vorgehensweisen zur Cloud-Sicherheit. Daher haben wir die aktuellen Nutzungsmuster, Sorgen sowie Zwischenfälle untersucht und liefern gezielt Erkenntnisse zu den drängendsten Herausforderungen für Unternehmen.

Sicherheitszwischenfälle sind allgemein verbreitet. Bemerkenswert ist hier besonders, dass 25 Prozent der Unternehmen, die Infrastructure-as-a-Service (IaaS) oder Software-as-a-Service (SaaS) nutzen, von Datendiebstählen berichten und 20 Prozent einen hochentwickelten Angriff auf ihre öffentliche Cloud-Infrastruktur verzeichneten. Da sich etliche Unternehmen auf die Datenschutz-Grundverordnung (DSGVO) der Europäischen

Wichtige Fakten der Umfrage[1]

97 % aller Unternehmen nutzen Cloud-Dienste (öffentliche, private oder eine Kombination beider Formen) – ein Anstieg gegenüber den 93 % vom vergangenen Jahr.

65 % setzen auf eine „Cloud First"-Strategie – ein Rückgang gegenüber den 82 % vom vergangenen Jahr.

83 % speichern vertrauliche Daten in der öffentlichen Cloud.

69 % vertrauen darauf, dass die vertraulichen Daten in der öffentlichen Cloud geschützt sind.

25 % verzeichneten bereits einen Datendiebstahl aus der öffentlichen Cloud (sowohl bei Software-as-a-Service als auch bei Infrastructure-as-a-Service).

20 % verzeichneten bereits einen hochentwickelten Angriff auf ihre öffentliche Cloud-Infrastruktur.

Union vorbereiten, fragten wir zudem, wie sich dieses neue Gesetz ihrer Meinung nach auf die Einführung von Cloud-Systemen auswirken wird.

Durchgeführt wurde die Umfrage unter IT-Entscheidungsträgern bei kleinen (500 bis 1.000 Mitarbeiter), mittleren (1.000 bis 5.000 Mitarbeiter) und großen Unternehmen (mehr als 5.000 Mitarbeiter) aus Australien, Brasilien, Deutschland, Frankreich, Großbritannien, Indien, Japan, Kanada, Mexiko, Singapur und den USA.

Schlussfolgerungen und Empfehlungen

Durch die bessere Transparenz können Unternehmen sicherheitsbewusster und früher transformative Cloud-Dienste einführen, schneller auf Sicherheitsbedrohungen reagieren und von den Kosteneinsparmöglichkeiten der Cloud profitieren. Es ist besser, einen vollen Überblick über die Cloud zu erhalten als zu versuchen, nur einen Teil davon zu kontrollieren.

Transparenz-orientierte Unternehmen verwenden die volle Bandbreite von Cloud-Diensten, um für das eigene Unternehmen die beste Lösung zu finden. Sie sind gegenüber Schatten-IT tendenziell entspannter und sehen sie eher als frühen Indikator für zukünftige Trends und nützliche Anwendungen statt als Gegner, der so schnell wie möglich ausgeschaltet werden muss. Sie möchten einen möglichst vollständigen Überblick erhalten und basierend darauf fundierte Entscheidungen über den optimalen Kontrollansatz treffen.

Basierend auf den Ergebnissen der diesjährigen Umfrage endet der Bericht mit empfohlenen Vorgehensweisen dazu, wie alle Unternehmen aktiv die Cloud-Sicherheit verbessern können:

1. DevSecOps-Prozesse. Es hat sich erwiesen, dass DevOps und DevSecOps die Code-Qualität verbessern und Exploits sowie Schwachstellen verringern. Die Integration von Entwicklung, Qualitätssicherung und Sicherheitsprozessen in die Geschäftseinheit oder das Anwendungsteam ist dringend erforderlich, um mit der Geschwindigkeit heutiger Geschäftsumgebungen Schritt halten zu können.
2. Bereitstellungsautomatisierung und Verwaltungs-Tools (z. B. Chef, Puppet oder Ansible). Selbst äußerst erfahrenen Sicherheitsexperten fällt es schwer, mit dem Volumen und Tempo der eigenen Cloud-Bereitstellungen Schritt zu halten. Automatisierungsfunktionen, die menschliche Vorteile mit maschinellen Vorteilen ergänzen, stellen eine grundlegende Komponente heutiger IT-Abläufe dar.
3. Vereinheitlichung der Sicherheit durch zentrale Verwaltung für alle Cloud-Dienste und -Anbieter. Wenn Sie mehrere Verwaltungs-Tools verwenden, können schnell Details verloren gehen. Mit einem zentralen Verwaltungssystem für mehrere Clouds und einer offenen Integrationsebene wird die Komplexität verringert.

Den vollständigen Bericht können Sie hier herunterladen.

40 % der IT-Leiter bremsen die Cloud-Implementierung wegen fehlender Cyber-Sicherheitskompetenzen.

2x so hoch ist die Wahrscheinlichkeit einer Strategie für die Absicherung von Containern und serverlosem Computing, wenn DevSecOps-Funktionen verwendet werden.

27 % der IT-Sicherheitsbudgets werden im Durchschnitt für Cloud-Sicherheit zur Verfügung gestellt – in 12 Monaten voraussichtlich bereits 37 %.

<10 % aller Unternehmen rechnen mit einem Rückgang bei Cloud-Investitionen als Folge der EU-Datenschutz-Grundverordnung (DSGVO).

[1]Details zu Methodik und Demographie der Umfrage finden Sie im Anhang des vollständigen Berichts.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de