HPE GreenLake

Kann die Hybrid Cloud das richtige Maß an Sicherheit für Unternehmensdaten bieten?

Wenn es um Sicherheit geht, bestimmen die individuellen Anforderungen jedes Unternehmens die Architektur.

Wenn Sie vor fünf Jahren einen CIO oder CTO eines großen Unternehmens gefragt hätten, warum sie vor der Migration in die Cloud zurückschrecken, wäre die Sicherheit wahrscheinlich eines der Hauptanliegen gewesen.

Die Dinge haben sich in wenigen Jahren stark verändert. Die Sicherheit in der Cloud hat sich erheblich verbessert, und Unternehmen können ihre Daten inzwischen bequemer in der Cloud speichern. Dennoch bleibt die Situation kompliziert, wie eine Untersuchung von HPE zeigt.

Zu Beginn des Jahres 2023 befragte Hewlett Packard Enterprise mehr als 900 IT-Entscheider aus aller Welt zu ihrer Einstellung zur Hybrid Cloud.[1] Ein wichtiger Teil der Studie befasste sich mit der Frage, wie zufrieden Unternehmen mit der Sicherheit in der Cloud sind. Die Ergebnisse könnten Sie überraschen.

Wenn es darum geht, das richtige Maß an Sicherheit zu bieten, bewerteten die Befragten, die verschiedene Arten von Cloud- oder On-Premises-Strategien verwendeten, deren Sicherheit wie folgt:

75 %
der Nutzer einer Private Cloud gaben an, dass ihre Strategie das richtige Maß an Sicherheit bietet – die erste Wahl

63 %
der Nutzer vor Ort stufen ihre Strategie als sehr sicher ein

60 %
der Hybrid Cloud-Nutzer (eine Kombination aus Private Cloud, Public Cloud und vor Ort) bewerteten ihre Sicherheit als solide

59 %
von Public Clouds und 53 % der Nutzer, die Private und Public Clouds mischten, hatten hohe Bewertungen für ihre Sicherheitsbereitschaft

Diese Ergebnisse sagen weniger etwas über die Fähigkeiten der einzelnen Infrastrukturtypen aus als vielmehr über den relativen Reifegrad der Sicherheitsvorkehrungen eines Unternehmens, so Matt Maccaux, Global Field CTO bei HPE.

„Die Cloud ist nicht mehr oder weniger sicher als ein VPN-Zugang zu Ihrem Rechenzentrum“, sagt er. „Es gibt viele Unternehmen, die ihre Anwendungen und Daten in die öffentliche Cloud stellen und bei denen noch nie ein Einbruch stattgefunden hat. Es kommt wirklich darauf an, wie Ihr Unternehmen über Sicherheit denkt. Wenn Sie keinen ganzheitlichen Ansatz verfolgen oder keine guten Betriebsabläufe haben, sind Sie zu Recht besorgt über den Einsatz einer gemeinsam genutzten Infrastruktur

Unternehmen müssen ihre Risikotoleranz bestimmen

Logischerweise sollte es einfacher sein, alle Unternehmensdaten an einem Ort zu speichern, um sie zu schützen. Darüber hinaus bedeutet der Betrieb in nur einer Umgebung in der Regel eine geringere Komplexität. Es werden weniger Ressourcen für die Verwaltung benötigt – daher der Eindruck, dass Private Clouds und lokale Lösungen sicherer sind. Andererseits verfügen viele Technologieführer möglicherweise nicht über das Know-how, um Daten in einer Private Cloud sicher zu verwalten. In diesen Fällen ist die Auslagerung der Sicherheit an einen erfahrenen Public Cloud-Anbieter wirtschaftlich sinnvoll.

„Wir lagern die Sicherheit an ein Cloud-Unternehmen aus, weil wir glauben, dass sie es besser machen können als wir“, so ein CIO eines großen Unternehmens. „Es ist für uns wie eine Erweiterung der Belegschaft, die es uns ermöglicht, uns auf unsere Stärken zu konzentrieren, anstatt zu versuchen, alles zu machen.“

Letztlich geht es bei der Sicherheit um Risikomanagement. Das bedeutet, dass das richtige Maß an Sicherheit für ein Unternehmen für ein Unternehmen mit einer geringeren Risikotoleranz unzureichend sein kann. Vieles hängt von der Art der Daten ab, die jedes Unternehmen sammelt, und von den rechtlichen Rahmenbedingungen, in denen es tätig ist.

„Perfekte Sicherheit gibt es nicht“, sagte ein CTO eines anderen großen Unternehmens. „Sie entwickelt sich ständig weiter. Letztendlich müssen Sie das richtige Maß an Sicherheit für Ihren Komfort finden.“

[1] Die von HPE und Publicis Insights in Zusammenarbeit mit dem Marktforschungsunternehmen Savanta durchgeführte Studie umfasste Interviews mit Technologie- und Unternehmensführern, um herauszufinden, wie die Hybrid Cloud ihre Unternehmen verändert hat.

Sicherheit ist ein ständiger Prozess

Unternehmen, die eine Hybrid Cloud-Strategie umsetzen, benötigen unterschiedliche Sicherheitsvorkehrungen für lokale Daten und für Cloud-basierte Daten. So können beispielsweise Daten vor Ort mit detaillierteren Kontrollmechanismen gesichert werden, während Cloud-Workloads die Sicherheit an einen externen Partner mit mehr Fachwissen auslagern können.

Da Unternehmen kritische Infrastrukturen in Hybrid Cloud-Umgebungen migrieren, wird die Umsetzung der Prinzipien eines Zero Trust-Frameworks für alle Arbeitslasten wichtiger denn je. Zero Trust unterwirft alle Benutzer und Geräte, sowohl innerhalb als auch außerhalb des Unternehmens, denselben kontinuierlichen Überprüfungs- und Authentifizierungsverfahren. Es gelten dieselben Zugriffsrichtlinien, unabhängig davon, wo sich der Benutzer, die Daten oder die Anwendung befinden.

Unternehmen müssen mit einer ehrlichen Bewertung ihrer Sicherheitsreife beginnen und sich dabei an einem der gängigen Zero Trust-Frameworks orientieren. Da die Einführung eines Zero Trust-Rahmens für die meisten Unternehmen eine Herausforderung darstellt, sind ein langfristiges Engagement sowie ausreichende Ressourcen und Mittel erforderlich. Diese Art von Bemühungen ist für alle Initiativen zur digitalen Transformation von entscheidender Bedeutung. Darüber hinaus hilft ein erfahrener digitaler Partner bei der Entscheidung, welche internen Systeme wiederverwendet werden können und welche ersetzt werden müssen, um den Prozess zu erleichtern und häufige Fallstricke zu vermeiden.

Die Angriffe werden immer umfangreicher und raffinierter, ganz gleich, welche Strategien Unternehmen einsetzen. Ob in einer Private Cloud, vor Ort oder mit einer Hybrid Cloud-Strategie, Wachsamkeit ist unausweichlich.

Entscheiden Sie sich für das richtige Produkt. Kontaktieren Sie unsere Presales-Experten.

Chat mit Vertrieb

Anrufen

Updates abrufen

Weitere Informationen finden Sie auf

GreenLake.HPE.com/security

HPE GreenLake besuchen

Hewlett Packard Enterprise

a50008060DEE