Cloud-Lösungen für Unternehmen: Diese 6 Punkte sind zu beachten

OVHcloud vmware®

Cloud Computing ist in der IT vieler Unternehmen inzwischen fest verankert. Die digitale Transformation, die in alle Branchen Einzug gehalten hat, treibt Unternehmen an, auf Multi-Cloud-Strategien umzusteigen, um sich so besser auf die neuen Anforderungen der Märkte einzustellen. Eines der Kernelemente für Unternehmen ist die Private Cloud, die als grundsätzlich sicherer als die Public Cloud eingestuft wird .

Obwohl eine Private Cloud für Unternehmen mehr Kontrolle über ihre physische Umgebung bietet und sich am besten individuell anpassen lässt, hat auch die Einrichtung einer Private Cloud ihre ganz eigenen Tücken...

Sicherheitslücken

Datenkriminalität, kompromittierte Authentifizierungsdaten, defekte Authentifizierungen, gehackte Oberflächen und APIs – 2018 gab es mehr als genug massive Sicherheitsbedrohungen. Wöchentliche Berichte über Cyberangriffe und Sicherheitslücken halfen nicht gerade dabei, die Sicherheitsbedenken bezüglich der Cloud auszuräumen.

Viele Unternehmen glaubten also, dass ihre Daten intern, in der selbst aufgebauten Cloud-Umgebung am sichersten sind. Tatsächlich sind jedoch gehostete Umgebungen genau so sicher wie On-Premise-Infrastrukturen, wenn nicht sogar noch sicherer. Sie werden von Sicherheitsexperten aufgebaut und gewartet, die die Sicherheitsfragen der Cloud verstehen und genau wissen, wie sie diese lösen müssen.

DDoS-Angriffe

Distributed-Denial-of-Service-Angriffe (DDoS) sind eines der hauptsächlichen Sicherheitsprobleme digitaler Unternehmen. Die Methoden bei diesen Angriffen wurden über die Jahre hinweg immer ausgeklügelter und mit neuen Technologien wie dem Internet of Things (IoT) kommen auch neue Bedrohungen.

Bei einem DDoS-Angriff wird gleichzeitig eine große Anzahl von Anfragen an einen Server versandt. Wenn der Angriff Erfolg hat, ist eine Website für Stunden oder sogar Tage nicht mehr verfügbar. Das führt zu Umsatzeinbrüchen und zu einem Vertrauensverlust bei den Kunden. Ein DDoS-Schutz ist für Unternehmen daher nicht mehr länger nur „nice to have“, sondern gehört unbedingt zum Sicherheitssystem. On-Premise-Schutz wird jedoch nie die Kapazität führender Systeme erreichen, um Angriffe erfolgreich abzuwehren.

[1] *IDC- Informationsschreiben, Juni 2019*

“Als Cloud-Anbieter wehren wir täglich mehr als 2000 DDoS-Angriffe ab. Unser Anti-DDoS-System ist für alle Kunden standardmäßig implementiert. Der Grund hierfür ist ganz einfach: Wenn ein DDoS-Angriff nicht abgewehrt wird, kann es zu Kollateralschäden kommen. Das bedeutet, dass nicht nur das eigentliche Angriffsziel geschädigt wird, sondern auch alle benachbarten Server im Rack betroffen sind. Unser VAC (eine Kombination von Technologien, die von OVHcloud zum Schutz vor DDoS-Angriffen entwickelt wurde) wird nur dann aktiv, wenn ein Angriff entdeckt wird. Für Kunden, die spezifische Sicherheitsanforderungen haben, bieten wir aber auch eine andauernde Filterung des Traffics an; oder anders gesagt, eine permanente Aktivierung des VAC”

Jakub Słociński, Network Innovation Manager at OVHcloud.

Physische Sicherheit und Redundanz

Die meisten Unternehmen haben keine solchen von Drittanbietern zur Verfügung gestellten physischen Sicherheitsfunktionen, wodurch wichtige Daten gefährdet sein könnten. Seriöse Rechenzentren sind wie eine Festung, die einen streng überwachten Eingang hat und mit Stacheldraht umzäunt ist. Videoüberwachung und Systeme für Bewegungserkennung sind genauwie Feuermelder und Löschsysteme ständig in Betrieb.

Heutzutage gehören Erreichbarkeit, hohe Verfügbarkeit und Ausfallsicherheit für viele IT-Services zu den Kernelementen. Bei einer internen Private Cloud das gleiche Redundanzniveau zu erreichen wie bei einer gehosteten Cloud, wäre eine sehr ehrgeizige Aufgabe. Doppelte Stromverbindungen, Stromaggregate, USV-Geräte und redundante Netzwerkverbindungen: All diese Maßnahmen führen zu hohen Wartungskosten, ganz zu schweigen vom internen Know-how, das sie erfordern.

Compliance-Bedenken

Der PCI-DSS-Standard enthält mehr als 250 Kontroll- und Sicherheitsmerkmale, die eingehalten werden müssen, um Kartendaten sicher zu verarbeiten. Bei Private Clouds wird Kontrolle über die Sicherheit gestellt, aber das macht es nicht unbedingt einfacher, die gesetzlichen Bestimmungen einzuhalten.

Das Einhalten von Compliance-Bestimmungen sollte bei der Planung immer an erster Stelle stehen, insbesondere dann, wenn es um vertrauliche Daten wie Zahlungskartendaten, sensible unternehmensinterne Informationen und Kundendaten geht. Die Umsetzung der Bestimmungen ist sehr zeit- und kostenintensiv und häufig müssen Unternehmen einen IT-Experten einstellen, der sich mit diesen Bestimmungen genau auskennt. Zudem muss das IT-Team die Systeme permanent überwachen, klare Notfallpläne für Sicherheitsvorfälle aufstellen und Datenverschlüsselung nutzen, um sicherzustellen, dass die Compliance-Bestimmungen stets eingehalten werden.

Performance-Probleme

Probleme mit der Performance sind in dynamischen virtualisierten Umgebungen nicht gerade selten. Es ist schwer vorauszusagen, wie Änderungen an der Infrastruktur die Anwendungsperformance beeinflussen, da selbst ein einfaches Software-Update ein geschlossenes Ökosystem aus dem Gleichgewicht bringen kann. Um die maximal mögliche Performance seiner Infrastruktur zu erhalten, ist es daher entscheidend, einen kontinuierlichen Prozess einzurichten, der die Performance der Cloud überprüft. Für jedes neue Deployment und für wesentliche Änderungen ist ein realistischer, am besten automatisierter Performance-Test notwendig, mit dem Probleme gleich in einem frühen Stadium aufgedeckt werden können. Ein solcher Prozess schützt Ihr Unternehmen vor unnötigen Kosten und ermöglicht die volle Kontrolle über das Preis-Leistungs-Verhältnis.

Zu viel Investitionen in Kapazität

Egal, ob Sie Ihre Private Cloud mit OpenStack oder VMware erstellen, eine Frage stellt sich dabei immer: Wie kann ich Agilität und Skalierbarkeit für eine interne Infrastruktur erreichen?
Bei einer eigenen Infrastruktur erfordert mehr Kapazität auch mehr Hardware. Wenn die benötigte Kapazität nicht genau vorausgesagt werden kann, investieren IT-Teams oftmals zu viel in die Hardware, um sicherzustellen, dass die erwarteten Ressourcen bei Bedarf auch vorhanden sind. Am Ende hat das Unternehmen hohe Investitionskosten und schwache Aussichten auf hohe Skalierbarkeit.

Wenn man von der Definition einer Cloud als besonders flexible und skalierbare Infrastruktur ausgeht, dann ist es fragwürdig, ob eine On-Premise-Infrastruktur dem gerecht werden kann, wenn nicht in zusätzliche Hardware investiert wurde. Auch wenn viele annehmen, dass eine Private Cloud nur „On-Premise-Infrastrukturen“ meint, muss das nicht der Fall sein. Eine Private Cloud ist eine Infrastruktur, die von nur einer Organisation genutzt wird. Die Ressourcen werden nicht geteilt und sind isoliert und dediziert. Eine gehostete Private Cloud liefert Organisationen die notwendigen Mittel für mehr Agilität und eine Steigerung der Betriebseffizienz, wobei die allgemeinen Risiken bei der Einrichtung von Clouds in Unternehmen minimiert werden. Bei einer gehosteten Private Cloud werden Kontrolle und Verantwortung für die Sicherheit teilweise an einen zuverlässigen Cloud-Anbieter übertragen. In diesem Zusammenhang ist die Wahl des richtigen Anbieters, der sich bei Sicherheitsfragen bereits bewährt hat, grundlegend, um alle Herausforderungen zu meistern.

OVHcloud ist ein globaler und führender europäischer Cloud-Anbieter, der 400.000 Server in 32 eigenen Rechenzentren auf 4 Kontinenten betreibt. Seit 20 Jahren nutzt das Unternehmen ein integriertes Modell, das die vollständige Kontrolle über die Wertschöpfungskette sichert – von der Entwicklung der eigenen Server über die Verwaltung der eigenen Rechenzentren bis hin zur Orchestrierung des eigenen Glasfasernetzwerks. Dieser einzigartige Ansatz ermöglicht es OVHcloud, vollkommen unabhängig, das gesamte Anwendungsspektrum für 1,6 Millionen Kunden in mehr als 140 Ländern abzudecken. OVHcloud bietet Kunden Lösungen der neuesten Generation, die hohe Leistung, transparente Preise und vollständige Datenhoheit miteinander verbinden, um ihr ungehindertes Wachstum zu unterstützen.