Drei wichtige Anforderungen einer Multi-Cloud-IT-Infrastruktur an Netzwerk und Security

Über 90 % der Unternehmen verfolgen eine Multi-Cloud-Strategie.[1] Wird jedoch mit mehreren IaaS-Cloud-Anbietern (Infrastructure-as-a-Service) gearbeitet, müssen Netzwerk- und Security-Architekturen angepasst werden, um Cyber-Sicherheitsrisiken zu verringern. Unternehmen suchen daher nach einfacheren, einheitlicheren Möglichkeiten, um Anwendungen und Workloads miteinander zu verbinden, die Anwendungserfahrung für Benutzer zu verbessern, Betriebsabläufe und Kosten durch Automatisierung zu optimieren, die Transparenz über Verkehrsmuster zu verbessern und konsequentere Kontrollen effektiv anzuwenden.

Netzwerk und Security sollten folgende drei Kernanforderungen erfüllen, wenn Anwendungen in mehreren IaaS-Clouds bereitgestellt werden:

1. **Gemeinsame Netzwerk- und Security-Richtlinien mit einheitlicher Durchsetzung für wiederholbare Implementierungen:** Eine der zentralen Herausforderungen bei Multi-Cloud-Implementierungen sind die unterschiedlichen Architekturen von Public-Cloud-Anbietern – und jede dieser proprietären Umgebungen kommt mit eigenen Frameworks, APIs und speziellen Tools. Die richtige Multi-Cloud-Lösung muss deshalb eine cloudübergreifende Netzwerk- und Security-Architektur bieten, die die nativen Merkmale und Funktionen jeder Cloud nutzt, diese Funktionalität mit APIs abstrahiert und Verbindungen per Automatisierung dynamisch verwalten kann.
2. **Anwendungsorientiertes Netzwerk für eine bessere Benutzererfahrung:** Die Verbindungen zwischen Clouds müssen für die Netzwerk-Technologie transparent sein. Das Netzwerk muss erkennen können, zu welcher Anwendung der Traffic gehört, und die Übertragung entsprechend abstimmen. Diese Anwendungsorientierung ist entscheidend, um vorhandene Ressourcen maximal nutzen zu können.

Aktuelle Studien zeigen, dass 8 von 10 Unternehmen längst nicht mehr „eine Cloud für alles“ verwenden, sondern mindestens zwei Clouds implementiert haben, um die digitale Transformation zu beschleunigen.

Warum sich Unternehmen für Multi-Clouds entscheiden:

1. Höhere Redundanz und Belastbarkeit
2. Mehr Unabhängigkeit bei der Wahl der Cloud-Anbieter
3. Vorteile durch spezialisierte Anbieter und erstklassige, moderne Dienste
4. Gewährleistung der Datenhoheit
5. Kostensenkungen

Die Performance wird so optimal auf die aktuellen Netzwerk-Bedingungen und -Kapazitäten abgestimmt. Auch lässt sich dann unwichtiger Datenverkehr umleiten und die Endanwender-Erfahrung nachvollziehen, um eine stabile Leistung für kritische Unternehmensanwendungen zu gewährleisten.

3. **Integrierte Netzwerk- und Security-Architektur für mehr Effektivität und Effizienz:** Bei einer Trennung von Netzwerk- und Security-Funktionen, bleibt die Multi-Cloud-Leistung hinter den Erwartungen zurück. Da jeder Layer tendenziell mit anderen Anbieter-Technologien arbeitet, entstehen Sicherheitslücken, wodurch die Implementierung anfällig für Angriffe wird. Durch eine zentrale Überwachung, koordinierte Durchsetzung und integrierte Kommunikation zwischen Netzwerk- und Security-Layern werden diese Lücken geschlossen. Zudem lässt sich mit einer intelligenten, cloudübergreifenden Deep Packet Inspection und Segmentierung des Netzwerk-Traffics zwischen Anwendungen und Workloads das Angriffspotenzial erheblich verringern.

Überlegungen für die nächste Phase

Die Architekturen von On-Premises-, Hybrid-Cloud- und Multi-Cloud-Implementierungsmodellen unterscheiden sich grundlegend. Die Cloud-Infrastruktur ist weitgehend API-gesteuert und für horizontale Skalierungen (oder Scale-out) und schnelle Änderungen ausgelegt. Darüber hinaus ist eine umfassende Integration in die zugrunde liegenden Cloud-Plattformen notwendig.

Die Security muss in den Netzwerk-Layer integriert werden und sowohl cloudnative Konstrukte (z. B. Security-Gruppen) als auch eine verbesserte Sicherheit wie ein Intrusion Prevention System (IPS) oder eine leistungsstarke End-to-End-Verschlüsslung zum Schutz des Netzwerk-Verkehrs bieten.

Bei Multi-Cloud-Modellen profitieren Unternehmen daher beim Wide Area Networking von einer softwaredefinierten SD-WAN-Lösung: Ein Secure SD-WAN bietet ein programmierbares, einheitliches und kostengünstiges Framework, das speziell für Multi-Cloud-Implementierungen entwickelt wurde.

[1] Kim Weins: „Cloud Computing Trends: 2020 State of the Cloud Report“. Flexera, 21. Mai 2020.

FORTINET

www.fortinet.com/de

7. Dezember 2020, 11:24 Uhr

799457-0-1-DE