DAS RZ DER ZUKUNFT – OFFEN UND EFFIZIENT DANK SDN

Unternehmen profitieren bei der Virtualisierung von Vorteilen wie Skalierbarkeit, Agilität und Effizienz. Durch die Umsetzung von Software Defined Network (SDN) mittels VMware und der geeigneten Fabric-Architektur von Juniper entsteht ein einfaches, offenes und intelligentes Rechenzentrum, das flexibel angepasst werden kann und maximalen Investitionsschutz bietet.

→ **VON UMBERTO ANNINO**

Die drei grossen Trends Cloud Computing, Virtualisierung und Big Data sorgen für grundlegende Veränderungen im Unternehmensnetzwerk. Denn traditionelle, mehrstufige Netzwerkarchitekturen sind komplex und stossen zunehmend an ihre Grenzen. Das Netzwerk der Zukunft ist möglichst einfach und hat eine flache Struktur, die alle Netzwerkelemente zu einer logischen Einheit vereint. Es verbindet Systeme und sogar Rechenzentren zu virtuellen Cloud Computing Infrastrukturen, die global verteilte Rechen-, Speicher- und Anwendungsressourcen in einem zentralen Pool zur Verfügung stellen. Der Einzug der Virtualisierung im Compute-Stack hat in den letzten Jahren sehr viel zur Effizienzsteigerung der ICT beigetragen und neue Server können so binnen weniger Minuten in Betrieb genommen werden. Diese Vorteile lassen sich aber auch in anderen Datacenter-Bereichen wie Netzwerk und Security nutzen. Es erfordert aber ein Umdenken in der Netzwerk- und Sicherheitsarchitektur, nur so kann eine solide Grundlage für stabile und zukunftsorientierte Rechenzentren gelegt werden.

SDN FORDERT DIE NETZWERKSICHERHEIT HERAUS

Um schneller und flexibler auf neue Anforderungen reagieren zu können, muss also die IT-Infrastruktur der Zukunft vereinfacht werden. Dies lässt sich dank Technologien wie Software Defined Networking (SDN) erreichen, mit welcher die physischen- und virtuellen Komponenten optimal aufeinander abgestimmt werden. Die Einführung von NFV (Network Functions Virtualization) führt zu einer weiteren Dynamisierung des Netzes. Diese Technologie ermöglicht den Ersatz von Netzwerk-Hardware durch Software-Appliances, die auf jedem im Netz erreichbaren Standard-Server ausgeführt werden können. Wenn sich die Anforderungen verändern, müssen sich die Ressourcen schnell und optimal an die neuen Herausforderungen anpassen lassen.

Zum Autor

Umberto Annino: ist Senior Security Consultant bei InfoGuard AG

Zum Unternehmen: InfoGuard AG ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Zu unseren Kompetenzen zählen massgeschneiderte Dienstleistungen nach internationalen Sicherheitsstandards sowie die Entwicklung und Implementierung technischer Sicherheits- und Netzwerklösungen. Die eingesetzten Produkte stammen aus langjährigen Partnerschaften mit ausgewählten Herstellern, wie beispielsweise Juniper Networks oder ADVA Optical Networking und aus eigener Entwicklung.

Mehr Informationen: www.infoguard.ch

Heutige Rechenzentren werden durch statische Übertragungssystemen mit hoher Kapazität verbunden. Dank der SDN-Technologie lassen sich die Netzwerkverbindungen über Software bedarfsabhängig automatisiert steuern. Dies ermöglicht den Aufbau von Netzwerken, welche die erforderliche Flexibilität hinsichtlich dynamisch zugewiesenen Speicher- und Rechenressourcen erfüllen.

Beide Technologien versprechen erhebliche betriebliche Vereinfachungen, Kostenvorteile sowie schnellen Service Roll-out. Denn ein solches agiles, programmierbares Netzwerk ermöglicht die Zuordnung von Netzwerkfunktionen wo immer Server- und Storage-Kapazität zur Verfügung steht.

Die Vorteile welche SDN im Netzwerkbetrieb ermöglichen, werden leider gleichzeitig mit einem neuen Sicherheitsrisiko erkauft. Daten, die zuvor in einer gut geschützten Umgebung innerhalb einer Sicherheitszone verarbeitet wurden, werden jetzt plötzlich über öffentliche Netzwerke übertragen. SDN und NFV erhöht aber auch die Zahl der involvierten Parteien bei der Verwaltung und Orchestrierung des Kommunikationsnetzwerks, was nach ausgefeilten Mitteln zur Authentifizierung und Autorisierung ruft. Um diese neuen und zusätzlichen Risiken in Schach zu halten, werden zwingend Verschlüsselungstechnologien benötigen: Nur so können die Vertraulichkeit und Integrität des Datenverkehrs sowie die Verfügbarkeit der Netzwerkverbindungen sichergestellt werden. Heutige leistungsstarke 100Gbit/s Bulk-Verschlüsselungslösungen, beispielsweise von ADVA Optical Networking, sichern zuverlässig und effizient den Inter- und Intra-Rechenzentrumsverkehr in kritischen Kommunikationsnetzwerken.

BILDER: XXX

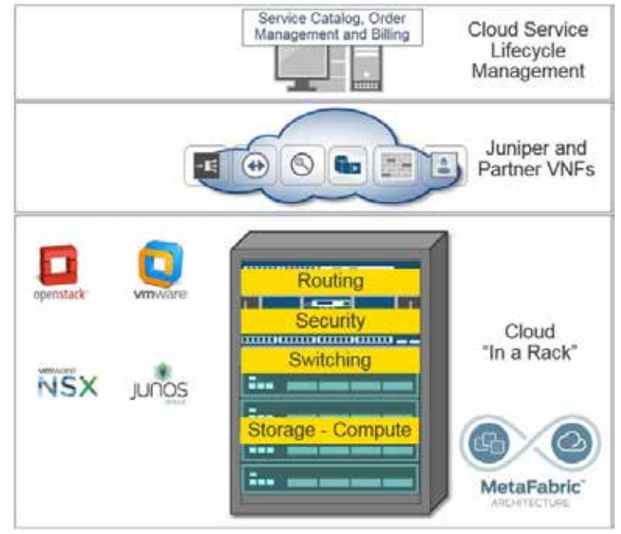
SICHERHEIT IM DATA CENTER DER ZUKUNFT

Agilität lässt sich wie bereits ausgeführt durch Vereinfachung der gesamten IT-Landschaft erreichen. Mit modernen und skalierbaren Netzwerk-Lösungen, wie diejenigen von Juniper Networks können je nach Kundenbedürfnis verschiedene Fabric-Architekturen implementiert werden, beispielsweise als Virtual Chassis Fabric. Sie hat den Vorteil, dass sich die Fabric gegenüber der Infrastruktur und der Administration als ein logischer Switch präsentiert, was den Aufwand und die Komplexität im Rechenzentrum massiv reduziert. Die Fabric bildet auch das Fundament für moderne Rechenzentren und kann über eine Orchestrierungslösung von VMware in Kombination mit einem Juniper Network Director zentral verwaltet werden.

Dank dieser Flexibilität und Skalierbarkeit können sowohl Schweizer Mittelstandsunternehmen, als auch Grossunternehmen ganz nach dem Motto «pay as you grow» ein Rechenzentrum aufbauen. Dieses besteht mindestens aus einem Rack, welches für den Betrieb von mehreren hundert Servern ausgelegt ist und kann auf mehrere Racks mit bis zu tausend Ports hochskaliert werden. Jedes zusätzliche Rechenzentrum lässt sich dann über einen beliebigen IP-Backbone erschliessen. Mit einer NSX-basierten Virtualisierung von VMware lassen sich zudem innert kürzester Zeit Desaster Recovery-fähige Netzwerksegmente über die Grenzen einzelner Rechenzentren hinweg ausrollen.

Auch die Architektur in virtualisierten Netzwerken muss höchsten Ansprüchen hinsichtlich der Sicherheit und Zuverlässigkeit erfüllen. Um gezielte Angriffe zu erkennen und vor allem zu unterbinden, werden moderne Rechenzentrumsarchitekturen in Sicherheitszonen unterteilt. Dank der Virtualisierung des Netzwerkes können innerhalb des VMware Overlay-Netzwerks perfomante Zonen-Übergänge realisiert werden. Durch die Integration von Security Edge Gateway Services lassen sich zur Trennung an den Zonenübergängen innerhalb des Rechenzentrums und bei Verbindungen nach aussen VM-basierte oder physische Sicherheitslösungen implementieren. Auch hier lassen sich dank der Netzwerk-Virtualisierung hoch performante «East – West» Zonen-Separierungen in den beiden Rechenzentren binnen Minuten ausrollen. Wenn all dies berücksichtigt wird, können Unternehmen ihre virtuellen Maschinen beliebig bewegen, ohne sich über Leistungseinbussen, Ausfallzeiten und den damit verbundenen Folgekosten Sorgen machen zu müssen.

Für Organisationen welche die Möglichkeiten von Cloud Computing, Mobilität und Big Data für die Optimierung ihres Unternehmens nutzen möchten und gleichzeitig dem Sicherheitsaspekt genügend Rechnung tragen wollen, ist eine Juniper Fabric-Architektur auf der Basis von VMware NSX genau die richtige Lösung. In Kombination mit Verschlüsselungstechnologien für die Übertragung der Daten entsteht ein sicheres und dynamisches Speichernetzwerk. ←



Die Juniper Fabric bietet eine optimale Basis zur Vereinfachung und Flexibilisierung von Rechenzentren.