Weiterentwicklung Netzwerkplattformen „Next Generation Hosting Produkte“

Studiengang: MAS Cyber Security

Die Swisscom Schweiz AG betreibt eine sichere und stabile Datacenter-Netzwerkinfrastruktur . Sie entwickelt diese laufend weiter, um sie für Anforderungen wie Kommunikation aus dem Homeoffice oder Vernetzung von Daten fit zu machen. Mit Software Defined Networking (SDN) sollen diese Anforderungen erreicht werden. Die explorative Masterthesis liefert eine Situationsanalyse, testet im Labor neue SDN Funktionalitäten und gibt Empfehlungen für das Hosting der Zukunft.

Ausgangslage

Das Team Datacenter Network betreibt und entwickelt in der Swisscom Schweiz AG die Datacenter-Netzwerkinfrastruktur und setzt dafür das Produkt Application Centric Infrastructure (ACI), eine SDN Lösung von Cisco, ein. Mit der explorativen Masterthesis wird untersucht, welche Möglichkeiten bestehen, um eine «Next Generation Hosting Fabric» aufzubauen und welche Funktionalitäten dazu eingesetzt werden müssten. Es wird die Hypothese aufgestellt, dass mit mehreren Funktionalitäten des Cisco ACI Produktes die Anliegen der Swisscom Schweiz AG im technischen Umfeld unterstützt werden können.

Situationsanalyse

Mit SDN wird die Netzwerksteuerungsebene von der Weiterleitungsebene physisch getrennt, d.h. neben dem Infrastruktur-Layer, gibt es sowohl einen virtuellen Kontroll- als auch einen Applikations-Layer. Sobald ein zentralisierter Controller das gewünschte Weiterleitungsverhalten ableitet, werden bei diesem Modell Weiterleitungsanweisungen für Pakete auf die entsprechenden Netzwerkgeräte heruntergeladen.
Mit dem Produkt ACI von Cisco können Netzwerkrichtlinien in einer zentralisierten Konsole verwaltet werden. Die Swisscom Schweiz AG setzt das Cisco Produkt ACI seit einiger Zeit ein, aber es werden noch nicht alle Funktionen verwendet. ACI bietet einerseits eine hohe Automatisierung und Skalierbarkeit, die es Netzwerkadministratoren erleichtert, schnell auf Änderungen in der Infrastruktur zu reagieren, die Netzwerklast ständig auszugleichen und die Netzwerke zu optimieren. Die Richtlinienkontrolle und die intelligente Netzwerksegmentierung gewährleisten eine hohe Verfügbarkeit und Sicherheit. Andererseits kann die Implementierung von ACI zu zusätzlichen Kosten führen, da spezielle Hardware sowie Schulungen erforderlich sind.
In der Laborumgebung konnte aufgezeigt werden, wie die Adressierung und der Transport von Datenpaketen (Layer 3) in ACI umgesetzt werden können. Die abschliessende Analyse zeigt, dass diese Integration, die Einbindung der Cloud und die Automatisierung zukunftsträchtig sind. Die Bildung einer ACI Fabrics Firewall und die Integration von Firewall und Loadbalancer sind aber noch mit zu vielen Komplexitäten behaftet. Insgesamt können ohne entsprechende Anpassungen keine der überprüften Funktionalitäten in der Swisscom Schweiz AG eingesetzt werden. Trotzdem bieten einzelne Funktionalitäten Chancen, welche die Swisscom Schweiz AG nutzen sollte.

Daniel Appenzeller

Empfehlungen und Fazit

Es wird empfohlen:

- die Layer 3 Integration in Teilbereichen einzusetzen, insbesondere in Netzen, welche lokal miteinander kommunizieren müssen;
- nicht über alle Netze eine direkte Abbildung von Firewall-Regeln in Cisco ACI vorzunehmen, da diese teilweise nur einzeln erstellt werden können und nicht alles abdecken;
- die direkte Anbindung einer Cloud einzusetzen unter der Voraussetzung, dass entsprechende Anforderungen formuliert werden;
- keine direkte Integration von Routingaspekten für die Anbindung von Firewalls und Loadbalancern vorzunehmen, da die nötigen Richtlinien und IP-Routen an ihre Skalierungsgrenzen kommen.
- die Automatisierung der Funktionalitäten einzusetzen.

Insgesamt zeigt sich, dass die Anwendungsmöglichkeiten dieser Funktionalitäten breit einsetzbar sind und auch für die Swisscom Schweiz AG zukunftsorientierte und sicherheitsrelevante Einsatzmöglichkeiten bieten. Der persönliche Wissensgewinn im Rahmen der Erarbeitung dieser Thesis war sehr hoch. Verschiedene Bereiche für weitergehendes Testing wurden identifiziert und bedürfen weiterer, fundierter Abklärungen.