ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Juli 2019

Systematische Weiterbildung für Netzwerk- und IT-Professionals

VMware NSX und Mikrosegmentierung in Theorie und Praxis

Grundlagen, Technik und Betrieb

von Dr. Markus Ermes

Virtualisierung hat in alle Bereiche des modernen Rechenzentrums Einzug gefunden. Nach Software Defined Compute und Software Defined Storage wird Software Defined Networking (SDN) und mit Letzterem auch „Network Function Virtualization“ (NFV) immer häufiger eingesetzt. In diesem Artikel sollen die einzelnen Komponenten und Grundlagen kurz beschrieben werden, die sowohl SDN als auch NFV ausmachen. Am Beispiel des Produktes VMware NSX werden die Eigenschaften und Möglichkeiten sowie die betrieblichen Aspekte des Einsatzes von SDN detaillierter betrachtet. Dabei wird ein Fokus auf der sogenannten „Mikrosegmentierung“ liegen, die in vielen Fällen ein Treiber für die Einführung von SDN und NFV ist.

In einem modernen Rechenzentrum wird die Virtualisierung auf allen Ebenen immer ausgeprägter. Während Software Defined Compute (SDC) durch Virtualisierungslösungen wie Hyper-V, VMware vSphere oder KVM schon die Norm ist, werden Software Defined Storage (SDS) und Software Defined Networking (SDN) – Letzteres in Verbindung mit Network Function Virtualization (NFV) – erst langsam eingeführt. Ein Grund für die zögerliche Einführung: SDN und NFV stellen einen besonders tiefen Einschnitt sowohl in die Architektur als auch für den Betrieb dar. Dieser Artikel wird sich mit diesen Einflüssen beschäftigen. Dazu sollen zunächst die grundlegenden Eigenschaften und Funktionen von SDN und NFV erläutert werden.

weiter auf Seite 6

Kommunikation im Wandel

Wie Cloud Produkte die bekannte Telefonie ersetzen

von Markus Geller

Wer den Kommunikationsmarkt in den vergangenen 10 Jahren beobachtet hat, der konnte zwei bestimmende Strömungen wahrnehmen:

1. **VoIP und UC haben in modernen Büro-Umgebungen die Kommunikation stark vereinfacht und flexible Arbeitsmodelle kostengünstig ermöglicht.**
2. **Die klassische Kanalvermittlung, incl. DECT, ist im Bereich der Produktion nur schwer zu ersetzen.**

Was aber beide Strömungen gemein haben, ist die Tatsache, dass sie bis heute meist auf lokale Infrastrukturen aufsetzen.

Dieser Umstand ist ja auch zunächst nicht verwunderlich. Warum sollte ein Service wie die Telefonie anders bereitgestellt werden als zum Beispiel die Infrastruktur eines LANs?

Beide Dienste stellen Anforderungen an die lokale Verfügbarkeit. Hier der LAN Port am Switch, dort das Tischtelefon. Daher scheint es nur logisch, solche Dienste lokal zu betreiben.

Diese Sichtweise gerät jedoch seit nunmehr fünf Jahren immer härter unter Beschuss.

Wie konnte das passieren?

weiter auf Seite 23

Geleit

Warum jede Organisation einen CTO braucht

auf Seite 2

Standpunkt

Die Personalabteilung als Schmelztiegel von Informationssicherheit und Datenschutz

auf Seite 21

Aktuelle Kongresse

ComConsult Technologie-Tage

ComConsult UC-Forum

auf Seite 4 und Seite 20

Frühbucherphase

ComConsult Wireless Forum

auf Seite 18

Geleit

Warum jede Organisation einen CTO braucht

An keinem Bereich des Lebens geht der technologische Wandel spurlos vorbei. Arbeiten und Abläufe, die Jahrtausende lang kaum Änderungen unterlagen, werden durch die Digitalisierung verändert. Internet of Things bedeutet wirklich die digitale Erfassung aller Dinge. Sind wir darauf vorbereitet? Die Antwort darauf ist ein klares Nein. Diese Aussage basiert auf Erfahrungen aus den letzten drei Jahrzehnten, in denen wir fast alle Branchen und Typen von Organisation beratend begleitet haben. Immer wurden viele Organisationen vom technologischen Wandel überrascht. Sie haben auf große Trends im Markt erst mit Verzug reagiert. Bleibt es auch in Zukunft so, werden viele Unternehmen den technologischen Wandel nicht überleben. Eine Organisation, die diesem Schicksal entgehen will, braucht einen Mechanismus für die Früherkennung der sie betreffenden Technologietrends. Dieser Mechanismus muss ein dauerhafter sein. An einem Chief Technology Officer (CTO) und der dazu gehörigen Organisationsstruktur geht kein Weg vorbei.

Bisher haben sich viele Organisationen damit begnügt, hin und wieder Reden und Schriften sogenannter Gurus Aufmerksamkeit zu schenken. Prognosen aus dem Munde oder der Feder dieser Propheten sind beliebt. Allein der Umstand, dass es jemand im Glücksspiel der Wirtschaft zum Milliardär schaffte, reicht aus, um ihm teure Vortragshonorare zu sichern.

Dabei lagen die berühmtesten Technik-Propheten weit häufiger daneben als richtig. Ein kleiner Ausschnitt aus der Reihe falscher Prophezeiungen:

- „Wir werden nie ein 32-Bit-Betriebssystem bauen.“ (Bill Gates, Mitbegründer von Microsoft, 1989)
- „Wireless Computing wird ein Flop sein – dauerhaft.“ (Bob Metcalfe, Mitbegründer von 3Com, auch bekannt als „Vater des Ethernet“, 1993)
- „Es gibt keine Chance, dass das iPhone einen signifikanten Marktanteil bekommen wird.“ (Steve Ballmer, damaliger Microsoft-Chef, 2007)
- „Ich würde Apple zumachen und das Geld den Anteilseignern zurückgeben.“ (Michael Dell, Inhaber der gleichnamigen Firma, 1997)
- „In zwei Jahren wird Spam der Vergangenheit angehören.“ (Bill Gates, 2004)

- „Die Amerikaner brauchen das Telefon, wir nicht. Wir haben jede Menge Boten.“ (Sir William Preece, Chefingenieur des königlichen britischen Postamts, 1878)
- „Dieses sogenannte ‚Telefon‘ hat zu viele Nachteile, um als ein ernstzunehmendes Mittel zur Kommunikation zu gelten. Dieses Gerät ist an sich für uns wertlos.“ (interne Note der US-Telegrafengesellschaft Western Union, 1876)
- „Bevor der Mensch den Mond erreicht, wird Ihre Post binnen Stunden mittels gelenkter Raketen von New York bis Australien transportiert werden. Wir stehen an der Schwelle zur Raketenpost.“ (Arthur Summerfield, Chef der US-Post, 1959)
- „Herumbasteln an Wechselstrom ist nur Zeitverschwendung. Niemand wird sie nutzen, niemals.“ (Thomas Edison, 1889)

Nachher ist man immer schlauer. Es wäre unfair, diesen Propheten mit Hohngelächter zu begegnen, wenn sie – oft lange nach dem Zenit ihres Erfolgs – nicht ein Geschäft daraus gemacht hätten, ihre Prognosen an den Mann zu bringen. Gesunde Skepsis gegenüber Kristallkugeln hat aber nie geschadet.

Der Job des CTO ist aber keine Konsultation der Glaskugel. Mehr als auf Prognosen sollte sich die CTO-Organisation auf bereits vorhandene Markt- und Technologieentwicklungen achten. Nicht Science Fiction, sondern aufmerksame Markt- und Technikbeobachtung ist gefragt.

Technologische Entwicklungen kommen äußerst selten wie der Blitz aus heiterem Himmel. Sie geben uns fast immer Monate, wenn nicht sogar ein, zwei Jahre Zeit, um sie zu erkennen. Schauen wir uns einige der wichtigsten Entwicklungen der letzten Jahrzehnte an:

- Dem Siegeszug des Personal Computer (PC) war in den 1980er Jahren einiger Hersteller von Heim-Rechnern wie Commodore und Atari vorausgegangen.
- Das iPhone hatte im iPod einen Vorgänger, der jahrelang millionenfach verkauft wurde und Apple erst die Möglichkeit gab, das bisher beliebteste mobile Gerät zu entwickeln. Und das zu einer Zeit, in der einige Pioniere des Mobiltelefons keine richtige Lust verspürten, mehr aus ihrem technologischen Vorsprung zu machen.
- Google war nicht die erste Internet-Suchmaschine. Jahre vor der Gründung von Google gab es schon die Suchmaschinen von Alta Vista and Yahoo.
- Packet Voice gehörte schon zu den ersten Anwendungen im Arpanet, dem Vorgänger des Internet. Vierzig Jahre später nennen wir es Voice over IP.

Wir hätten keine Propheten gebraucht, um die Bedeutung dieser Entwicklungen zu sehen. Sie waren vor unseren Augen. Und viele haben das gesehen. In den 1980er Jahren entwickelte ein Freund von mir auf der Basis von Commodore 64 ein sehr brauchbares Textverarbeitungssystem, das ich jahrelang genutzt habe. Lange wurde in der Branche darüber spekuliert, ob Apple in das Mobiltelefongeschäft einsteige, bevor dies Realität wurde. Ich habe die Suchmaschinen vor Google jahrelang genutzt, trotz

August 16, 1993 Seite 48

"After the wireless mobile bubble bursts this year, we will get back to stringing fibers."

InfoWorld

Auszug aus dem Artikel "Wireless computing will flop - permanently"
von Bob Metcalfe (bekannt als „Vater des Ethernet“)

Abbildung 1: Wenn die Kristallkugel täuscht

VMware NSX in Theorie und Praxis

Fortsetzung von Seite 1

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

Einige Aspekte davon wurden schon in früheren Artikeln des Netzwerk-Insiders erläutert, beispielsweise in [1]. Aus diesem Grund, und um den Umfang des Artikels zu begrenzen, wird hier nicht genau auf zugrundeliegende Techniken wie Netzwerk-Verkapselung oder „klassische“ Virtualisierung von Servern eingegangen. Es werden lediglich die kritischen Aspekte und die Konsequenzen für den Einsatz von SDN und NFV erwähnt werden.

Am Beispiel von VMware NSX werden dann diese Eigenschaften und Funktionen dargestellt. Die daraus resultierenden technischen und betrieblichen Auswirkungen werden anhand von Beispielarchitekturen und -prozessen genauer beleuchtet, wie sie typischerweise in einem Unternehmen auftreten.

Ein besonderer Fokus wird auf der sogenannten Mikrosegmentierung liegen, da sie neue Ansätze zur Netzwerksegmentierung bietet, die auch in bestehenden Umgebungen große Vorteile bieten kann. Ein Beispiel hierfür ist der Umzug eines Systems zwischen verschiedenen Netzwerksegmenten ohne die Änderung einer IP-Adresse.

1.1 Netzwerkvirtualisierung

SDN und NFV sind zwei Aspekte, die oft gemeinsam genutzt werden, insbesondere bei einer tiefen Integration in eine Virtualisierungsumgebung, wie es z.B. bei VMware NSX der Fall ist. Dabei werden die Aspekte des „klassischen“ Netzwerks wie folgt aufgeteilt:

- SDN:
  SDN hat das Ziel, die Control-Ebene von der Datenebene des Netzwerks zu trennen. Das Hauptziel dieser Technologie ist, Netzwerke aus einer zentralen Kontrollinstanz flexibel zu konfigurieren und nicht jede einzelne Netzwerkkomponente manuell anpassen zu müssen. Ein weiterer großer Vorteil neben der Flexibilität ist die geringere Fehleranfälligkeit.

- NFV:
  Bei NFV werden Netzwerkdienste virtualisiert, für die im „klassischen“ Netzwerk dedizierte Appliances betrieben werden. Darunter fallen beispielsweise Routing, Load-Balancing, Firewalls, Spam-Filter, Threat Intelligence zur Erkennung von Angriffen und andere.

Dabei ist in den allermeisten Fällen – so auch bei VMware NSX – die Kontrolle des Netzwerks bis auf Ebene der einzelnen VMs oder für einzelne Container möglich. Dadurch werden sowohl die Sichtbarkeit als auch die Sicherheit bei korrekter Nutzung verbessert. Das Troubleshooting bietet durch die verbesserte Sichtbarkeit neue Möglichkeiten und wird deutlich erweitert. Durch den Einsatz von Netzwerkverkapselung und häufig auch von herstellerspezifischen Erweiterungen ergeben sich aber auch neue Herausforderungen. Der Einsatz von speziellen Tools kann hier Abhilfe schaffen. Diese Tools werden typischerweise vom Hersteller der jeweiligen Netzwerk-Virtualisierungslösung (NVL) angeboten.

Im Netzwerk werden bei SDN und NFV typischerweise die folgenden drei Ebenen unterschieden, wie sie in Abbildung 1 dargestellt sind:

- Management-Ebene:
  Auf dieser Ebene interagieren Nutzer bzw. Administrator mit der NVL. Hier wird die Konfiguration vorgenommen, gespeichert und an die Controller-Ebene weitergeleitet. Dies beinhaltet Firewall-Regeln, Zugriffslisten, Netzwerk-Routen zu allen angeschlossenen (auch virtuellen) Systemen und so weiter. Um eine Automatisierung und/oder eine Kommunikation mit anderen Software-Tools zu ermöglichen, bieten NVLs im Allgemeinen auch eine Rest-API, welche die einzelnen Funktionen von außen ansprechbar macht.

- Controller-Ebene:
  Die Controller-Ebene leitet die Konfiguration der Management-Ebene an die beteiligten Endpunkte weiter. Die Controller-Ebene kann, je nach konkreter Umsetzung, sowohl zentral als auch dezentral umgesetzt sein. Im zentralen Fall werden ein oder mehrere Controller-Instanzen als virtuelle Appliances eingesetzt. Bei diesem zentralen Ansatz ist im produktiven Fall der Einsatz von mehreren Instanzen die Regel, um beim Ausfall einer Instanz weiterhin den Betrieb sicherzustellen. Ein Beispiel für eine verteilte Controller-Ebene ist BGP-EVPN, wie es von der IETF standardisiert, in den Produkten führender Hersteller implementiert und bei einigen Providern im Einsatz ist.

- Daten-Ebene:
  Auf dieser Ebene wird der eigentliche Netzwerk-Verkehr zwischen den verschiedenen beteiligten Hosts weitergeleitet.

Die NVL nutzt Overlay-Netzwerke, um die Trennung von Netzwerken ohne Einfluss auf das zugrundeliegende physische Netzwerk zu realisieren. Diese verkapseln den Netzwerkverkehr zwischen zwei (virtuellen) Systemen so, dass er für das physische (Layer-3-)Netzwerk transparent ist. Der Einsatz von Overlays bedeutet, dass der Header der Netzwerkpakete vergrößert werden muss, da zusätzliche Header eingeführt werden. Um die Größe der Nutzdaten nicht zu beeinträchtigen, muss die maximal mögliche Paket-

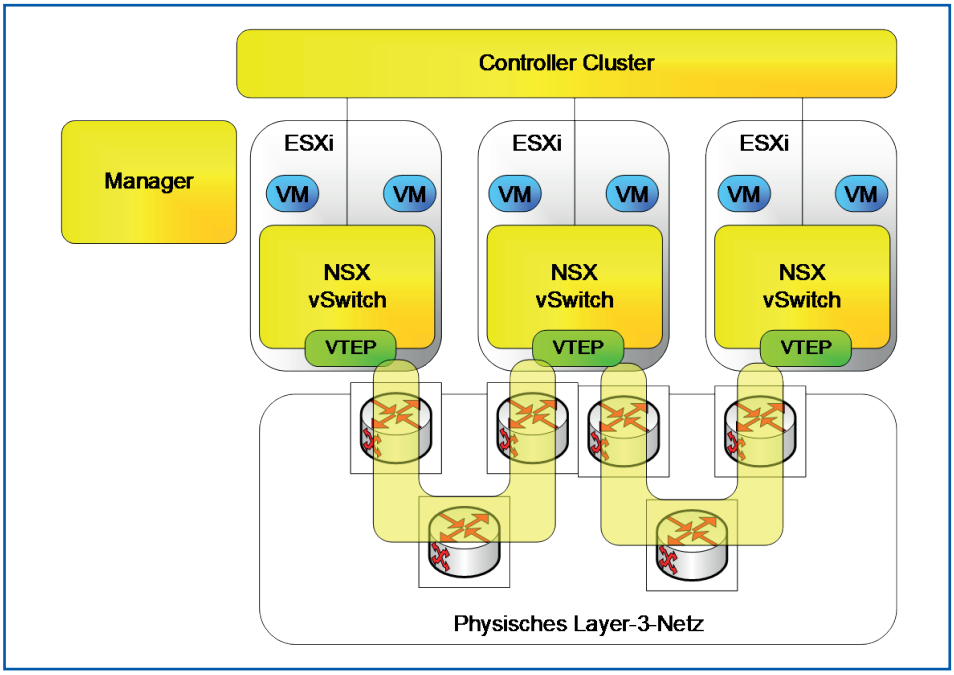

Abbildung 1: Schematische Darstellung der verschiedenen Ebenen in einer NVL am Beispiel VMware NSX (Quelle: Moayeri, Behrooz, Cisco ACI kontra VMware NSX, Netzwerk Insider, Dezember 2015)

größe (Maximum Transmission Unit, MTU) entsprechend groß sein. Ein typischer Wert für die minimale MTU bei der Nutzung von Overlay-Netzen wie VXLAN oder Geneve ist 1600 Bytes. Sollten also nicht flächendeckend Jumbo Frames im Netzwerk genutzt werden, kann dies eine Anpassung an den physischen Netzwerk-Komponenten bedeuten. Zur Realisierung von Overlays können verschiedene Technologien zum Einsatz kommen. Die häufigste Verkapselungs-Technologie ist VXLAN. VXLAN und andere Verkapselungsmechanismen ermöglichen eine Virtualisierung von Layer-2-Netzwerken innerhalb eines bestehenden Layer-3-Netzwerks. Die Ver- und Entkapselung werden dabei – je nach Produkt bzw. Hersteller – an verschiedenen Stellen durchgeführt. Bei VMware NSX als Lösung für virtualisierte Umgebungen sind dies die Virtualisierungshosts. Bei Cisco ACI erfolgt dieser Schritt auf den Access-Switches. Gängige Server-Betriebssysteme unterstützen ebenfalls die Nutzung von VXLAN-Overlays.

Zunächst werden NFV und eine dadurch mögliche „Mikrosegmentierung“ genauer beschrieben.

Als konkretes Beispiel wird in diesem Artikel VMware NSX präsentiert und die typischen Komponenten dieser Netzwerk-Virtualisierungslösung genauer beschrieben.

Eine Besonderheit bei VMware NSX ist die Tatsache, dass diese Lösung in zwei Versionen angeboten wird: NSX-T und NSX-V. Es werden die Unterschiede, Gemeinsamkeiten und Einsatzszenarien für beide Versionen dargestellt und die strategische Position der beiden Produkte betrachtet.

1.2 Network Function Virtualization

Wie bereits im letzten Kapitel beschrieben, löst NFV verschiedene Dienste innerhalb des Netzwerks von spezialisierter und meist kostenintensiver Hardware. Darunter können viele Dienste aus den verschiedensten Bereichen fallen. Von typischen Netzwerkdiensten wie Load Balancing, Routing und Firewalling bis zu netzwerkbasierter Threat Intelligence, Spam-Filter, Anti-Virus, Data Loss Prevention und vielem mehr. Für typische Virtualisierungslösungen im Data-Center-Umfeld spielen v.a. die folgenden Funktionen bzw. Netzwerkkomponenten eine wichtige Rolle:

- Router
- Firewall
- Load Balancing

Diese Komponenten können in einer NVL unterschiedlich realisiert werden. Bei einer ausreichend tiefgreifenden Integration in die Architektur bietet sich hier eine verteilte Architektur an, da hierdurch die Ressourcen einer typischerweise zentralisierten, sehr performanten und kostenintensiven Komponente auf viele, weniger leistungsfähige Komponenten verteilt werden können. Dabei werden an den Endgeräten (bei NSX den Virtualisierungshosts) maximal ca. 10% der Leistung benötigt. Außerdem ergibt diese Verschiebung hin zum Endpunkt und damit so nahe wie möglich an die Endgeräte des Netzwerks (VMs und physische Systeme) eine wesentlich bessere Sichtbarkeit. Dies ermöglicht eine Überwachung der Endgeräte im Netzwerk in einer Art und Weise, die bisher nur sehr umständlich möglich war.

Besonders interessant ist dies im Bereich der Firewalls, da diese im „klassischen“ Netzwerk außerhalb der Virtualisierungsumgebung verortet sind und sich besondere Herausforderungen bei der Durchsetzung von Firewall-Regeln auf VM-Ebene ergeben:

Sämtlicher Traffic aller Systeme müsste zu einer (oder mehreren) zentralen Firewall(s) geführt werden, die eine ausreichende Leistung dafür besitzen müsste. Diese Übertragung des Traffics ist nur sehr umständlich möglich, indem beispielsweise Private VLANs auf VM-Ebene oder sehr kleine Subnetze genutzt werden. Der Betrieb einer solchen Lösung ist extrem aufwendig und wenig erprobt und ist daher nicht zu empfehlen.

Die Skalierbarkeit, bedingt durch die verteilte Funktionalität und damit Vermeidung zentraler Instanzen für Firewalling, Load Balancing etc. ist ein wesentliche Vorteil einer NVL gegenüber Hardware-basierten Netzfunktionen. Der weitere wesentliche Vorteil besteht darin, dass durch die Positionierung der Netzvirtualisierung im Kern des Hypervisors Netzfunktionen wie Segmentierung und Lastverteilung auf der Ebene virtueller Maschinen (VM-Ebene) wahrgenommen werden.

Diese Genauigkeit bietet die Möglichkeit, mit begrenztem Aufwand Firewall-Regeln auf Ebene einzelner VMs durchzusetzen.

1.3 Mikrosegmentierung

Eine der Möglichkeiten beim Einsatz einer NVL, die eine Sichtbarkeit des Netzwerkverkehrs bis auf VM-Ebene ermöglicht, ist die „Mikrosegmentierung“. Diese Technologie ist eines der größten Alleinstellungsmerkmale für kombinierte Lösungen für SDN und NFV, z.B. VMware NSX. In vielen Umgebungen stellt die Mikrosegmentierung sogar einen der Hauptgründe für die Einführung einer NVL dar.

In einer Architektur, welche die Firewall näher an die VM rückt und in der die notwendige Leistung nicht zentral bereitgestellt werden muss, ist dies gegenüber zentralisierten Komponenten stark vereinfacht. Bei einer entsprechenden Integration per API ist es möglich, die vorhandenen Endgeräte ohne eine feste Bindung an eine IP-Adresse aufzulisten. Speziell die Abkehr von Firewall-Regeln auf Basis von IP-Adressen ist hier der

Kommunikation im Wandel - Wie Cloud Produkte die bekannte Telefonie ersetzen

Fortsetzung von Seite 1

Seit über 10 Jahren ist Markus Geller bei der ComConsult GmbH einer der führenden Referenten für die Themen VoIP und Daten-Netzwerke. Der Schwerpunkt seiner Trainer Tätigkeit liegt dabei auf den Gebieten SIP, PSTN Migration, WebRTC sowie Layer 2 und 3 Techniken für MAN und LAN. Markus Geller verfügt über eine langjährige Erfahrung beim Aufbau und der Planung von Netzwerken im large Enterprise Umfeld, inkl. RZ-Netzwerken, WLAN und Multicastverfahren. In seiner über 20-jährigen IT-Laufbahn beschäftigt er sich mit der Evaluierung neuer Technologien und deren Einsatz in der Praxis. Zudem ist er als Autor diverser Fachartikel für den ComConsult Netzwerk Insider und das Wissensportal tätig.
E-Mail: geller@comconsult.com

Nun, aus der Vergangenheit kennen wir Centrex Dienste. Diese Dienste beruhten auf der Bereitstellung einer vollständigen, unternehmensweiten Telefon-Infrastruktur durch einen Provider. Die ersten dieser Services wurden in den 1960er Jahren in New York eingerichtet und hatten in der Spitze weltweit bis zu 20 Millionen Nutzer. Davon entfielen jedoch fast 85% auf die USA und Kanada, so dass man wohl von einem lokalen Phänomen sprechen konnte.

Jedoch ist diese Grundidee nicht mit der Kanalvermittlung verschwunden. Mit dem Aufkommen der Kommunikation über IP sollte diese Art der Bereitstellung einen neuen Schwung aufnehmen, den sie bis heute trägt und immer beliebter macht.

Durch den Einsatz eines unabhängigen Transportnetzes, welches genau wie vormals die Telefonie mit dem Rest der Welt verbunden ist, stellt sich nicht mehr die Frage „Wo“ ein Dienst angeboten wird.

Ein solcher Service kann heute geographisch unabhängig für alle Teilnehmer erbracht werden.

Dieses Grundprinzip kennen wir alle durch den Einsatz unternehmensweiter, zentraler VoIP- und UC-Lösungen. Warum also nicht die eigene Infrastruktur durch einen zentralen Dienst beim Provider ersetzen? Also den eignen zentralen Ansatz konsequent weiterentwickeln?

Und genau an diesem Punkt sind wir heute angekommen.

Schauen wir daher einmal näher auf den Markt der PBX Anbieter. Alle wichtigen Marktteilnehmer haben ihr Produktportfolio in Richtung von Cloud-Angeboten erweitert, und das bisher noch unter Beibehaltung ihrer klassischen Produkte und Lösungen.

Aber einige von ihnen haben sich schon auf den Weg gemacht, diese bisherigen Angebote auszudünnen bzw. zukünftig den Bereich der lokalen Installationen vollständig einzustellen oder auslaufen zu lassen.

Ein gutes Beispiel für eine solche Entwicklung ist die Firma Microsoft. Seit der Einführung von Office 365 gehörte zum festen Bestandteil der kompletten Lösung immer auch die lokale Verfügbarkeit eines Lync- oder Skype-for-Business-Servers. Mit der Entwicklung des cloudbasierten Telefon-Services hat sich diese Betrachtung jedoch massiv verändert.

Der aktuelle Skype for Business Server, der im letzten Jahr vorgestellt wurde, ist voraussichtlich die letzte Variante, die noch für eine lokale Installation vertrieben wird.

Derzeitige Aussagen von Microsoft lassen vermuten, dass es keinen Nachfolger für dieses Produkt geben wird, so dass wir heute schon sagen können, dass ab 2024 oder 2025 das Ende der lokalen Telefonie im Rahmen von Microsoft-Lösungen eingeläutet wird.

Diese Betrachtung führt uns aber noch weiter, denn ähnlich wie es dem Skype for Business Server ergehen wird, so wird auch das lokal installierte Office Paket in der Zukunft vom Markt verschwinden. (siehe Abbildung 1)

Es sind die Aussagen von Satya Nadella, dem Chef von Microsoft, die diese Entwicklung unterstreichen: Mobile First, Cloud First!

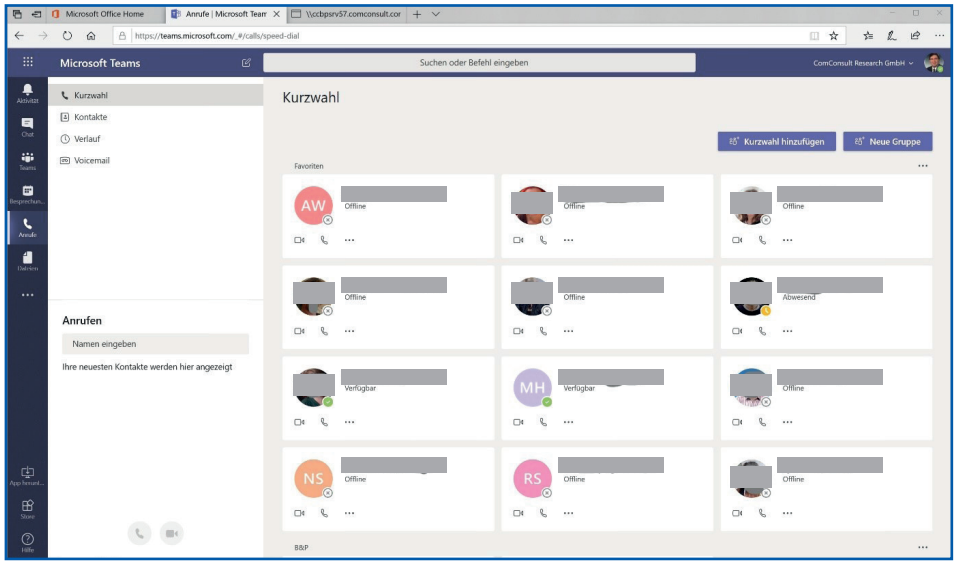

Abbildung 1: Microsoft Teams

Kommunikation im Wandel - Wie Cloud Produkte die bekannte Telefonie ersetzen

In diesem Szenario werden am Ende weltweit über 80% aller Unternehmen ihr Office aus der Cloud beziehen. Schon heute ist Office 365 eine Voice-, Video-, Unified-Communications- und Collaboration-Plattform, die eine klassische TK- und UC-Lösung überflüssig macht.

In Kombination mit dem im Consumer-Markt beheimateten Skype könnte somit eine Plattform entstehen, über die mehrere 100 Millionen Nutzer weltweit direkt miteinander kommunizieren können.

Die daraus resultierende und – zugegeben – recht ketzerische Frage lautet dann folgerichtig:

- Wozu benötige ich dann noch einen Telefonie-Provider?

Denn eine Grundvoraussetzung für die Nutzung dieser Dienste ist der Zugang zur Office-Cloud über das Internet.

Nun wird der ein oder andere Leser vehement mit dem Kopf schütteln und einwenden, dass „sowas“ über das Internet nicht funktionieren kann, da man die Kontrolle über den Datenaustausch verliert.

Aber stimmt das wirklich?

Unternehmen wie NFON oder sipgate betreiben auf dieser Basis erfolgreich seit Jahren ihr Geschäftsmodell. Viele von unseren Lesern haben, wie auch wir, die Erfahrung gemacht, dass solche Lösungen durchaus eine ausgereifte, technisch verlässliche Plattform darstellen.

Und machen wir uns nichts vor: die Ressourcen, die im Internet zur Verfügung gestellt werden, übersteigen oft die doch recht teuren MPLS-Netze, die wir von unseren Providern anmieten.

Allerdings stellen Provider wie Microsoft auch gewisse Anforderungen an die Konnektivität. So müssen Jitter- und Delay-Voraussetzungen erfüllt werden, und es ist ausreichend Bandbreite beim Internetzugang zu berücksichtigen. Tabelle 1 und 2 sollen dabei die Situation verdeutlichen, in die wir uns bei einer entsprechenden Umstellung begeben.

Tabelle 1 verweist auf klassische QoS Paramater, die eingehalten werden müssen. Interessant ist dabei der Hinweis auf den Microsoft Edge. Welche Aussage verbirgt sich dahinter?

Bisher sind wir immer davon ausgegangen, dass wir eine Internetverbindung zur Kommunikation nutzen.

Value	Client to Microsoft Edge	Customer Edge to Microsoft Edge
Latency (one way)	< 50 ms	< 30 ms
Latency (round-trip time, or RTT)	< 100 ms	< 60 ms
Burst packet loss	<10% during any 200-ms interval	<1% during any 200-ms interval
Packet loss	<1% during any 15-sec interval	<0.1% during any 15-sec interval
Packet inter-arrival jitter	<30 ms during any 15-sec interval	<15 ms during any 15-sec interval
Packet reorder	<0.05% out-of-order packets	<0.01% out-of-order packets

Tabelle 1: Jitter und Delay Anforderungen Quelle: Microsoft

Activity	Download bandwidth	Upload bandwidth	Traffic flow
Peer-to-peer audio call	0.1 Mbps	0.1 Mbps	Client <> Client
Peer-to-peer video call (full screen)	4 Mbps	4 Mbps	Client <> Client
Peer-to-peer desktop sharing (1920×1080 resolution)	4 Mbps	4 Mbps	Client <> Client
Two-participant meeting	4 Mbps	4 Mbps	Client <> Office 365
Three-participant meeting	8 Mbps	6.5 Mbps	Client <> Office 365
Four-participant meeting	5.5 Mbps	4 Mbps	Client <> Office 365
Five or more–participant meeting	6 Mbps	1.5 Mbps	Client <> Office 365

Tabelle 2: Bandbreiten Anforderung Quelle: Microsoft

Ist das aber wirklich so? Nein, nicht so ganz, denn über das Internet wird nicht wirklich eine Ende-zu-Ende-Kommunikation etabliert.

Zunächst einmal nutzen wir unser eigenes Unternehmens-LAN bis zur Internet DMZ. Von dort aus geht der Weg über den ISP zum Cloud Anbieter.

Dieser Cloud Anbieter, in unserem Fall Microsoft, unterhält ein eigenes weltumspannendes Cloud-Netzwerk, man könnte es auch als Corporate WAN bezeichnen. Dieses Cloud WAN hat an vielen öffentlichen Internetknoten weltweit direkte Zugänge und Verbindungen zu Providernetzen (PoP, Point of Presence). Dies bedeutet für einen Kunden z.B. in Deutschland, dass er das Internet tatsächlich nur von seinem Anschluss-Punkt bis zum DE CIX in Frankfurt nutzt und dort direkt in das Cloud-Netzwerk des Anbieters geroutet wird.

Dieser Microsoft PoP (Point of Presence) in Frankfurt wäre dann der in der Tabelle erwähnte Microsoft Edge. Dies erklärt dann auch die - im Verhältnis zu den ITU-Vorgaben - kurzen Zeiten für die Verzögerung von lediglich 30 bzw. 50ms statt der bekannten 180ms aus der ITU Empfehlung.

Die restliche Zeit wird für den Transport durch das Microsoft Backbone benötigt.

Der zweite wichtige Faktor ist eine ausreichende Bandbreite des Internetzuganges. Um diese kalkulieren zu können, müssen zunächst die zu erwartenden Kommunikations-Beziehungen mit den dazugehörigen Bandbreiten berechnet werden.

Um ein Gespür dafür zu bekommen, was uns erwartet, müssen wir uns Tabelle 2 anschauen.

Hierbei erkennen wir sehr schnell, dass gerade die intensive Nutzung von Video-Konferenzen den Bedarf an Bandbreite explodieren lassen kann. Während eine Punkt-zu-Punkt-Kommunikation wie bisher lokal stattfindet und somit nur die Signalisierung über die Cloud realisiert wird, gehen bei Konferenzen sämtliche Verkehrsströme über das Internet zum Cloud Anbieter.

Dieser Umstand stellt daher sehr hohe Anforderungen an die Bandbreite. Anschlüsse jenseits von 100 Mbit/s bis zu n-fach Gbit/s werden in einem solchen Szenario eher die Regel als die Ausnahme bilden.

Anmeldung

ComConsult Informationsservice

Verpassen Sie keine wichtigen Informationen mehr und tragen Sie sich in unserem ComConsult Informationsservice ein.

Unser Informationsservice informiert Sie regelmäßig per E-Mail und per Post über aktuelle Entwicklungen in der IT-Branche und über unsere Veranstaltungen und Neuerscheinungen. Der Service umfasst unser monatliches Magazin „Der Netzwerk Insider“, sowie regelmäßige E-Mails über unser aktuelles Produktangebot. Darüber hinaus senden wir Ihnen im Bedarfsfall unsere Technologie-Standpunkte und Technologie-Warnungen zu aktuellen Entwicklungen zu.

Anrede	
Name	
Firma	
E-Mail-Adresse	

oder online unter
https://www.comconsult-research.de/insider-2/