ComConsult Research

Der Netzwerk Insider

November 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

SDN in Unternehmensnetzen

von Dipl.-Math. Cornelius Höchel-Winter

SDN weckt immer noch so viele Emotionen wie kaum ein anderes Netzwerkthema in den letzten Jahrzenten. Je nach Sichtweise wird die Technologie zum Heilsbringer, zur Spinnerei technologiegläubiger Akademiker oder gar zum Jobvernichter hochstilisiert

Bei so großen Unterschieden in der Bewertung und Argumentation lohnt es sich in der Regel, mal kurz durchzuatmen, einen Schritt zurückzutreten und mit einem etwas größerem Abstand die Materie zu betrachten. Dies ist das Ziel dieses Artikels.

Was ist SDN?

Getrieben werden die unterschiedlichen Meinung über SDN natürlich nicht zuletzt von der Tatsache, dass SDN eben **kein** standardisiertes Protokoll oder fertiges Produkt eines Herstellers, das man bewerten könnte, ist. Es gibt noch nicht einmal irgendein Dokument, das SDN umfassend und abschließend festschreibt, denn mit SDN wird eher diffus eine Architektur zur zentralisierten Steuerung von Netzen bezeichnet als eine konkrete Technik.

weiter auf Seite 6

Zweitthema

Internet-DMZ in der Cloud

von Dr. Simon Hoff und Dipl.-Math. Simon Oberem

Mit der Verlagerung von Anwendungen und Daten in eine Cloud, müssen auch entsprechende Sicherheitskomponenten in der Cloud zur Verfügung stehen. Wenn beispielsweise Web-Anwendungen und Web-Services in einer Private Cloud, Public Cloud oder Hybrid Cloud realisiert werden, dann müssen hier auch Firewalls, Intrusion-Prevention-Systeme und Web Application Firewalls (WAFs) bzw. Reverse Proxies integriert werden. Damit wandert automatisch ein Teil der Systeme, die in der Vergangenheit im lokalen Rechenzentrum (RZ) im Bereich der Internet-Anbindung aufgebaut wurden, in die Cloud, und dieser Trend zeigt sich inzwischen in praktisch allen Bereichen der Internet-Anbindung.

1. Traditioneller Aufbau von Internet-DMZs

Eine Demilitarized Zone (DMZ) ist ein Zwischennetz, das als Pufferzone den Übergang zwischen Netzen unterschiedlichen Sicherheitsniveaus schafft. Typisches Beispiel ist eine DMZ zwischen dem Internet und dem internen Netz. Ausprägungen und Spielarten von DMZs sind vielfältig und auch am Internet-Übergang gibt es keine Standards, sondern unterschiedliche Best-Practices. Generell kann man Internet-DMZs grob in DMZs klassifizieren, die nur ausgehenden Verkehr, nur eingehenden oder ein- und ausgehenden Verkehr behandeln, wie in Abbildung 1 skizziert. Am Internet-Zugang ist der Aufbau einer zweistufigen Firewall-Architektur gebräuchlich, und die Systeme im DMZ-Bereich, die direkt mit dem Internet und mit internen Systemen kommunizieren (z.B. Proxies, VPN-Gateways und Reverse Proxies), werden typischerweise dual-homed angebunden.

weiter auf Seite 18

Geleit

Funktechnologien: es kommt eine Revolution

auf Seite 2

Standpunkt

Universelle Mobilität – ist das gesund?

auf Seite 14

Aktueller Kongress

UC-Forum 2016

ab Seite 12

Aktuelle Sonderveranstaltungen

Wireless und Mobility Winterschule 2016

ab Seite 3 und ab Seite 15

Geleit

Funktechnologien: es kommt eine Revolution

Funk-Netzwerke oder auf Neudeutsch Wireless-LANs kämpfen seit ihrer Markteinführung mit den Grenzen der Physik: entweder hohe Leistung oder große Entfernungen. Dies ist dann noch zu kombinieren mit den daraus abgeleiteten Zellplanungen und der Integration unterschiedlicher Teilnehmermengen. Denn wir haben nicht nur die Grenzen der Physik, wir haben auch Anforderungen, die verschiedener nicht sein können. Vom Büro über das Hotel bis zur Fertigung. Und natürlich soll es zuverlässig und sicher sein, zwei Attribute, die nun gar nicht zur Funktechnik passen. Damit wären wir wieder bei der Physik.

Bisher entwickelt sich der Markt zweigeteilt. Auf der einen Seite haben wir den Mobilfunk, auf der anderen die WLANs. Die technischen Konzepte könnten unterschiedlicher nicht sein, auch wenn beide Welten mit der Physik kämpfen und versuchen die Grenzen des Machbaren immer weiter auszudehnen.

Im WLAN-Bereich werden wir in den nächsten Jahren mit der Umsetzung von 11ad und 11ax einen weiteren Leistungsschub erleben. Die ersten neuen Chip-Generationen sind da und von hier an gibt es nur noch einen Weg: noch mehr Leistung mit noch mehr Einschränkungen. Die entsprechenden Produkte sind schon auf dem Markt oder kommen in den nächsten Monaten. Dementsprechend muss die Planung bereits darauf ausgelegt werden. Aber das ist im WLAN nicht neu, aufgrund der permanenten Weiterentwicklung brauchen wir immer schon Planungsansätze, die über den Tellerrand hinaus gehen. Interessanterweise erhalten wir schon bald ein Verkabelungsproblem. Die gerade für den WLAN-Bereich eingeführten Ethernet-Standards mit 2,5 und 5 Gigabit sind aus heutiger Sicht bereits unzureichend und wir werden bald 10 Gigabit brauchen. Natürlich wieder in Abhängigkeit vom Szenario. Aber speziell Industrie 4.0 wird neue Türen öffnen und einen bisher unbekannten Bandbreitenbedarf auch in die Produktion bringen. Dies muss bereits jetzt vorbereitet und durchdacht werden.

Die gleiche Entwicklung erleben wir im Mobilfunk, nur anders. Auch hier haben wir sehr widersprüchliche Szenerien, die sich in sehr verschiedenen Bedarfsgruppen aufgeteilt nach Reichweite, Teilnehmerzahl und Bandbreite einteilen lassen. Und klar ist schon seit längerem, dass LTE dem sich entwickelnden Bedarf nicht gerecht wird. SmartCity und Autonomes Fahren werden Anforderungen generieren, die wir mit keiner aktuellen Funktechnik abdecken können. Wir haben eben zu große Wiedersprüche im Design. Auf der einen Seite die preiswerte Integration von Sensoren und auf der anderen Seite Gigabit über große Entfernungen.

Wohin wird es von hier aus gehen und werden wir vielleicht endlich auch eine bessere Integration von Mobilfunk und WLAN sehen? Die Antwort ist ganz einfach: wir werden in den nächsten fünf Jahren eine Revolution der Funktechnik erleben. Die Kombination aus der Weiterentwicklung von WLAN mit 11ax und Mobilfunk mit 5G wird völlig neue Voraussetzungen schaffen.

Was ist anders? Nun, die Technologie akzeptiert endlich, dass wir sehr verschiedenen Bedarfs-Situationen haben. Und anstelle der Kombination inkompatibler Einzeltechnologien wird es ein Gesamtpaket geben. Dies wird sich aus heutiger Sicht um 5G herum gruppieren.

Diese Entwicklungen sind so brisant, dass wir eine aktuelle Sonderverstaltung zu diesem Thema aufgesetzt haben: Wireless und Mobility. Diese findet am 12. und 13.12. in Köln statt und beleuchtet alle aktuellen Entwicklungen, vom heutigen Bedarf bis hin zu den Extrem-Anforderungen der Zukunft.

Wir sind fest davon überzeugt, dass Funktechnik/Wireless den Netzwerk-Markt stark verändern werden. Diskutieren Sie mit unseren Experten diese aktuelle Entwicklung und die Konsequenzen für Ihre Netzwerke.

Viel Erfolg dabei

Ihr
Dr. Jürgen Suppan

Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 12.12.-13.12.16 in Köln

Die ComConsult Akademie veranstaltet vom 12.12. bis 13.12.16 ihre Sonderveranstaltung "Wireless und Mobility" in Köln.

Die permanente Steigerung der Anzahl mobiler Endgeräte mit immer mehr Leistung ist ein längst nicht mehr aufzuhaltender Trend. Provider sind schon seit einiger Zeit dabei, die Mobilfunknetze deutlich aufzurüsten. Dies betrifft auch Betreiber privater wireless Infrastrukturen. Sie werden kaum Videos oder Spiele in großem Umfang unterstützen müssen. Man kann aber davon ausgehen, dass die hohe Leistung der mobilen Endgeräte auch für die Realisierung eines verbesserten Benutzer-Erlebnisses bei bestehenden und neuen Anwendungen genutzt wird. Die vielen unterschiedlichen Ansätze für Augmented Reality sprechen z.B. eine deutliche Sprache. Ist eine Technologie, wie in diesem Falle die mobile Anbindung intelligenter Endgeräte verfügbar und erfolgreich, kommen im Laufe der Zeit sozusagen „natürlich“ neue Anwendungen hinzu.

Mega-Treiber: Cloud, Video und IoT

Moderne Arbeitsplatzmodelle gehen von vollständig mobilen Endgeräten aus. Es darf auf die Dauer keine spürbaren qualitativen Unterschiede bei der Benutzung Cloud-basierter oder sonstiger Dienste und Kollaborationstechniken in Abhängigkeit vom Ort oder dem grade vorliegenden Mobilitätsgrad geben.

Es besteht die quasi unabwendbare Tendenz, drahtlose Netze zur Lieferung immer reicherer Inhalte an immer mehr Endgeräte zu benutzen. Dies erzeugt einen erheblichen Druck auf die Ressource, über die wir liefern: die Kapazität des (drahtlosen) Netzes und der dahinter liegenden Infrastruktur.

Ein weiterer Mega-Treiber ist das IoT, die automatische Kommunikation von Maschinen, Sensoren und Aktoren untereinander. Viele IoT-Konzepte könnten ohne drahtlose Verbindungen nicht implementiert werden. Das erzeugt eine völlig neue Dimension von Anforderungen, Leistungsprofilen und Spezial-Technologien.

Private flächendeckende WLAN-Versorgungsstrukturen nach IEEE 802.11ac: mehr Fragen als Antworten!

Mit IEEE 802.11ac Wave2 steht eine neue Evolutionsstufe für WLANs zur Verfügung. Vereinzelt wurde auch schon Wave3 mit einer theoretischen Leistung von 10 Gbps angekündigt. Die wichtigen neuen Funktionen von Wave2 und 3 müssen auf den Prüfstand. Was können sie bewirken? Und: ist ihre Nutzung überhaupt erlaubt? Für die Nutzung von 160 MHz breiten Kanälen in flächendeckenden Infrastrukturen ist eine Erweiterung der bisher zulässigen Frequenzbereiche notwendig. Die ist auf dem Weg, aber erreicht sie uns rechtzeitig?

Man kann behaupten, dass Wave2 und Wave3 die ersten wirklich für den professionellen Einsatz gedachten Varianten von IEEE 802.11ac sind. Was bedeutet das in der Praxis? Welche Steuerungsmöglichkeiten bieten uns die einschlägigen Hersteller an?

Eine wesentliche Frage ist: wie werden die neuen Systeme in die Gesamt-Architektur integriert? Die oftmals propagierte „gesteigerte Benutzererfahrung“ ist ja gut und schön, aber welche Anforderungen stellt sie an die betriebliche Logik der Infrastrukturen?

Nach wie vor sollte doch der sichere und wirtschaftliche Betrieb der privaten drahtlosen Infrastrukturen im Vordergrund stehen. Provider erwarten die Möglichkeit, ihre Strukturen aus der Cloud mittels SDN/NFV zu steuern und z.B. Instanzen virtueller Small Cells dynamisch auf der physikalischen Infrastruktur zu schaffen. Sind derartige Funktionen für „normale“ private Betreiber wirklich erforderlich? Wie können Sicherheitskonzepte elegant und wirkungsvoll umgesetzt werden?

Es gab in den letzten Monaten eine Menge von Mergern zwischen Infrastruktur-Anbietern und WLAN-Spezialisten. Cisco hat sich Meraki einverleibt, Aruba gehört jetzt zu HP Enterprise, Brocade funkt jetzt mit Ruckus und auch Extreme/Enterasys haben sich noch einen kleinen WLAN-Spezialisten organisiert. Die Erwartung ist, dass dadurch Synergien zwischen den WLAN-Lösungen und der notwendigen Switching-Infrastruktur entstehen. Wie sieht das aber genau aus? Welche Vorteile ergeben sich möglicherweise für den Betreiber?

Mobilfunk: letztlich das Ende der privaten WLANs?

Schließlich: wie geht es weiter mit dem Mobilfunk? Ausgehend von LTE entwickeln sich nicht nur die nächsten Releases mit deutlich erhöhter Funktionalität bis hin zu 5G, sondern parallel dazu auch Begehrlichkeiten hinsichtlich der bislang den WLANs vorbehaltenen lizenzfreien Frequenzbereiche. Um nämlich die hochgesteckten Ziele von 5G erreichen zu können, brauchen die Provider alle Frequenzen, die nicht bei „3“ auf dem Baum sind, von stillgelegten TV-Kanälen bis hin zu gelegentlichen Lücken in systematischen Funkdiensten. Die Zukunft gehört dem dynamisch etablierten virtuellen Spektrum. Treffen aber konventionelle WLANs mit LTE oder 5G-Signalen zusammen, werden sie höchst wahrscheinlich den Kürzeren ziehen. Oder kann man vorbeugen?

Schon vor über fünf Jahren wurde der Standard IEEE 802.11ad für die Multi-Gigabit-Kommunikation im 60 GHz Millimeterwellen-Bereich definiert. Auch Small Cells werden zunehmend im Millimeterwellenbereich aufgesetzt. Wie sind derartige Trends für private Betreiber zu werten?

Die Entwicklung internationaler Mobilfunkstandards ist deutlich aufwändiger als z.B. eine neue Ethernet-Norm. Die meis-

ten Kunden bekommen heute LTE nach Release.10. Rel. 10 bis ca. Rel .12 heißen auch „LTE Advanced“. Schon in diesen Versionen wird das Konzept aufgegriffen, die Leistung von LTE durch die Hinzunahme von passenden Zellenkonzepten zu erhöhen. Unter Voraussetzung eines guten Interferenz-Managements steigt die mögliche Leistung eines LTE-Versorgungsbereiches (einer Basis-Station) deutlich mit der Anzahl von kleinen Zellen (Small Cells). Richtig spannend wird es mit den Versionen ab Rel. 13 und 5G.
Wie könnte sich das auswirken? Normalerweise wird ein LTE Netz von einem Provider betrieben und auch WLAN oder auf anderer Technik beruhende Small Cells werden auch von ihm kontrolliert.

Gravierende Auswirkungen auf die unterstützende Infrastruktur

Die Anforderungen an die mobile Versorgung steigen stark und man wird darauf Antworten finden müssen. Es wird sicher nicht zu weniger, sondern eher zu mehr WLAN-Zellen kommen. Das wird glücklicherweise durch die entsprechenden Ethernet-Technologien für die Integration der vielen APs unterstützt.

Allgemein werden heute WLAN-Access Points mit 1 GbE und PoE versorgt. Im letzten Jahr wurden neue Ethernet Datenraten definiert, nämlich 2,5 und 5 GbE, die für die Versorgung anspruchsvollerer Access Points nach 802.11ac noch über ältere Kabel gedacht sind. Betrachtet man aber die jetzt schon in Entwicklung befindlichen Nachfolgestandards IEEE 802.11 ad (schon längst fertig), ax und ay, sieht man schnell, dass 5 GbE viel zu kurz greifen. Provider nutzen optische Infrastrukturen, alleine wegen der Latenzen. Ist das auch der Weg für ambitionierte private Betreiber?

Sie sehen: viele Entwicklungen, viele Technologien, Fragen über Fragen. Auf unserer einzigartigen Sonderveranstaltung hören Sie, was erfahrene Top-Spezialisten, Planer, Hersteller und Berater empfehlen. Nutzen Sie die Gelegenheit auch zur ausführlichen Diskussion, bevor die Wireless Welle Sie überflutet.

Die Referenten


Dr. Jan Byok


Dipl.-Ing. Stefan Bien


Dr. Johannes Dams


Christian Goldberg


Dipl.-Ing. Olaf Hagemann


Dr. Simon Hoff


Dr. Franz-Joachim Kauffels


Reinhard Lichte


Dipl.-Ing. Markus Nispel


Dipl.-Ing. Michael Schneiders


Dr. Joachim Wetzlar


Dipl.-Ing. Dominik Zöller

Anmeldung an kundenservice@comonsult-research.de

Sonderveranstaltung Wireless und Mobility

Ich buche die Sonderveranstaltung
Wireless und Mobility

☐ 12.12.-13.12.16 in Köln
zum Preis von € 1.990,--

☐ inklusive Report "Wireless-Systeme der nächsten Generation"
zum Teilnehmer Sonderpreis von 174,- €

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht Sonderveranstaltung Wireless und Mobility

Montag 12.12.2016

9:30 - 10:15 Uhr
Wireless World: Anforderungen der Digitalen Zukunft
- Implikationen der wachsenden Cloud-Nutzung
- Neue Anwendungen und Anforderungen an Multi-Gigabit WLANs
- IoT und die enge Verbindung zu Mobilfunktechnologie (5G)
- Strukturelle Aspekte unterstützender Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:15 - 11:00 Uhr
Stand der Technik bei WLAN
- IEEE 802.11ac in den verschiedenen Geschmacksrichtungen
- Ist mit 10 Gbit/s auf 2,4 und 5 GHz Schluss oder geht zukünftig noch mehr?
- WLAN im 60-GHz-Band: Es gibt Standards aber kaum Anwendungen • Was sagt die IEEE zur Mobilfunk-Integration?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
WLAN, ein Medium für alle Anwendungen?
- Mobilität und Einfachheit sind Triebfedern für die WLAN-Vernetzung
- Hohe Verfügbarkeit, Reaktivität und Bitrate: Geht das überhaupt mit WLAN?
- Wie bekommt man die optimale Ausleuchtung in Büros und Hallen am besten hin?
- Welche Frequenzen sollen für welche Anwendungen genutzt werden? • An allen Ecken funkt es: Lassen sich Störungen überhaupt vermeiden?
- „Fremde" Funkanwendungen sickern unbemerkt ein! Wie geht man damit um?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
Einführung in Cloud Managed IT
- Cloud Management, was bedeutet das?
- Mehrwerte für Unternehmen jeder Größe
- Hybride Infrastrukturen – Realität oder Wunschdenken
- Anwendungsbeispiele

Christian Goldberg, Cisco Systems GmbH

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:30 Uhr
WLAN-Zellplanung auf dem Prüfstand
- Welchen Stellenwert hat die WLAN-Zellplanung bei der Konzeptionierung einer WLAN-Infrastruktur?
- Welche Parameter sind bei einer professionellen WLAN-Zellplanung zu berücksichtigen?
- Ausleuchtungsmessung vs. Simulation
- Häufige Fehler, die Sie unbedingt vermeiden sollten. Dos and Don'ts

Dipl.-Ing. Stephan Bien und Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 17:00 Uhr
All-IP: ein einheitlicher Access für jegliche Sprachkommunikation. Sind DECT und VoWLAN tot?
- Die Rolle von LTE und 5G im All-IP-Netz
- Mobilfunk in Enterprise-Kommunikationslösungen
- VoLTE und 5G als Ersatz für VoWLAN und (IP-)DECT

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

17:00 - 18:00 Uhr
Von LTE Advanced zu 5G
- Mobilfunk: Stütze der nächsten digitalen Revolution
- Techniken von LTE Advanced
- Koexistenz von LTE / 5G und WLANs
- 5G: Konzepte, Technologien, Feldversuche, Standardisierung

Dr. Franz-Joachim Kauffels, Technologie-Analyst

ab 18:00 Uhr Happy Hour

Dienstag 13.12.2016

9:00 - 10:30 Uhr
Wireless / Mobile / Cloud Security: Ganzheitliche Konzepte sind gefragt
- Sicherheit im WLAN: Ein alter Hut?
- Warum es trotz Hotspot 2.0 kaum sichere Hotspots gibt
- Absicherung von iOS und Android
- Sichere Integration mobiler Endgeräte
- Schlüsselelement sichere Cloud-Dienste
- Rolle von MDM und WLAN Management aus der Cloud

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Auf dem Weg zum All Wireless Office
- WLAN als normales Office Connect muss wie Strom, Wasser, Klima als Infrastruktur leistungsstark zur Verfügung stehen
- Nutzung der WLAN Infrastruktur von allen User- und Gerätetypen
- WLAN und dann ... – Analytics, Locationbased Serivces. Beispiel: der intelligente Meetingraum
- WLAN als Offload von Mobilnetzen in empfangsschwachen Officebereichen
- On-premise, private Cloud oder Public Cloud Lösungen – eine Portfolio für alles

Reinhard Lichte, Aruba - a Hewlett Packard Enterprise Company

11:45 - 12:30 Uhr
Moderne flächendeckende Enterprise WLANs
- Neue Anforderungen durch Cloud und Hybrid Enterprise
- Rolle von SDN/NFV bei der WLAN-Steuerung
- Integriertes Produktspektrum für Zellen und Infrastruktur
- Anwendungsbeispiele

Dipl.-Ing. Markus Nispel, Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 15:00 Uhr
Netz-Architekturen für (High Speed) WLANs
- Welche Anforderungen bestehen an die Netzarchitektur für den Aufbau von WLANs
- Der WLAN-Controller: Flaschenhals oder Mittel der Wahl?
- Alternativen zum WLAN Controller: Was bieten die Hersteller?
- IEEE 802.3bz: Seit dem 27.09.2016 gibt es „Breitreifen" für Access Points

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

15:00 - 16:00 Uhr
Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen
- Grundlagen der deutschen Störerhaftung nach ständiger BGH-Rechtsprechung (Neueste Entwicklungen im Bereich der Störerhaftung)
- Gesetzesänderung des TMG aus Sommer 2016
- EuGH Urteil aus Herbst 2016 (Zukunft der deutschen Störerhaftung, Gestaltungstipps für Betreiber privater WLAN-Infrastrukturen)

Dr. Jan Byok, Bird & Bird LLP

16:00 Uhr der Veranstaltung

Schwerpunktthema

SDN in Unternehmens-netzen

Fortsetzung von Seite 1

Dipl.-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Diese fehlende allgemein anerkannte Definition führt eben auch dazu, dass jeder mit einem zentralen Managementtool dieses Produkt in letzter Zeit gerne mal in der Nähe von SDN positioniert. Aber so einfach ist es nicht.

SDN steht für „Software Defined Networking“, der Begriff reicht bis in die 1990er Jahre zurück. Die Basis dessen, was wir heute unter SDN verstehen, wurde jedoch erst 2007/2008 an den amerikanischen Universitäten Berkeley und Stanford gelegt und ist eng verbunden mit den Namen Martîn Casado, Nick McKeown und Scott Shenker, dem Unternehmen Nicira und dem Protokoll OpenFlow.

OpenFlow ist ein Kommunikationsprotokoll zur Steuerung von Layer-2- und Layer-3-Swiches und Routern im Netzwerk. Das Protokoll wird von der ONF (Open Networking Foundation) entwickelt und ist historisch gesehen im Grunde der Startpunkt der modernen SDN-Entwicklung.

Das Protokoll basiert auf „Anweisungen“ an die Netzwerkkomponenten, wie mit welchen eingehenden Paketen zu verfahren ist. Diese „Anweisungen“ bestehen jeweils aus einer Mustererkennung und einer oder mehreren Aktionen. Die Aktionen werden von der OpenFlow-Komponente durchgeführt, wenn das eintreffende Paket zu dem jeweiligen Muster passt. Als Muster kommen alle Layer-2-, Layer-3- und Layer-4-Headerkomponenten in Frage, insbesondere also die MAC- und IP-Adressen sowie die Portnummern von UDP und TCP, typische Aktionen sind „Paket an Port x weiterleiten“ oder „Paket wegwerfen“, aber auch Änderungen des Pakets selbst wie VLAN-Zuordnung oder QoS-Markierungen sind möglich.
An den Universitäten stand man damals vor der Aufgabe, neue Netzwerkprotokolle und -verfahren testen zu wollen, ohne aufwändige, dedizierte Testumgebungen aufbauen zu müssen. Die Idee war daher, das Produktiv- bzw. Campusnetz (mit) zu nutzen und pro Anwendung zu steuern, wie die jeweiligen Kommunikationsströme im Netz behandelt werden. Schnell waren die wesentlichen Eckpunkte gefunden, wie man so etwas umsetzen könnte. Man nehme:

- OpenFlow,
- einen zentralen Controller, der die Netzwerkströme jetzt via OpenFlow steuert, und
- Netzwerkkomponenten, die die OpenFlow-Anweisungen des Controllers umsetzen und die einzelnen Pakete entsprechend bearbeiten und weiterleiten können.

Eine wichtige Anmerkung vorweg: Wenn an dieser Stelle und auch später im Artikel von „einem“ oder „dem“ Controller die Rede ist, bedeutet das nicht, dass es sich physisch um ein einzelnes System handelt. Vielmehr ist damit eine zentrale Control Plane gemeint, die natürlich sowohl redundant als auch verteilt aufgebaut werden kann.

Damit ist das Grundgerüst von SDN im Wesentlichen skizziert (siehe Abbildung 1).

1. Paket kommt beim ersten Switch (Ingress-Switch) an.
2. Falls der Switch keine Regel kennt, wie das Paket behandelt werden muss, fragt er beim Controller nach. Hierzu leitet er wahlweise das komplette Paket oder nur Metadaten (Header-Daten) an den Controller weiter.
3. Der Controller entscheidet über Bearbeitungs- und Weiterleitungsregeln und schickt diese Regeln an alle betroffenen Systeme.
4. Das Paket wird entsprechend dieser Regeln bearbeitet und durch das Netzwerk geschleust.

Schon aus diesem recht einfachen Basiskonzept lassen sich wesentliche Merkmale der ursprünglichen Idee ableiten:

1. Das Konzept ist **flowbasierend.**
   Das heißt, der Controller muss Bearbeitungs- und Weiterleitungsregeln nicht für jedes einzelne Paket ableiten und verteilen, sondern nur für ganze Klassen von Verkehrsströmen oder Kommunikationsbeziehungen (sogenannte Flows), die anders behandelt werden müssen als andere. Konkret: die über einen anderen Weg durch das Netz geschleust oder die sonst wie anderes bearbeitet werden sollen.

   Diese Flows werden natürlich durch die Mustererkennung von OpenFlow definiert.
2. Da die OpenFlow-Regeln auch auf nachfolgende Pakete angewendet werden sollen, muss der Switch oder Router diese Regelsätze zwischenspeichern. Das bedeutet einerseits einen völlig neuen Tabellentyp („Flow Table“) für diese Informationen im Speicher der Netzwerkkomponenten, bietet andererseits aber auch die Chance, die unterschiedlichen Forwarding-Tabellen von MAC-Adressen über IPv4- und IPv6-Adressen bis hinzu ACLs, die man heutzutage alle in Switches findet, zu vereinheitlichen und so eine **einheitliche Speicherstruktur** (Data Plane) zu schaffen.

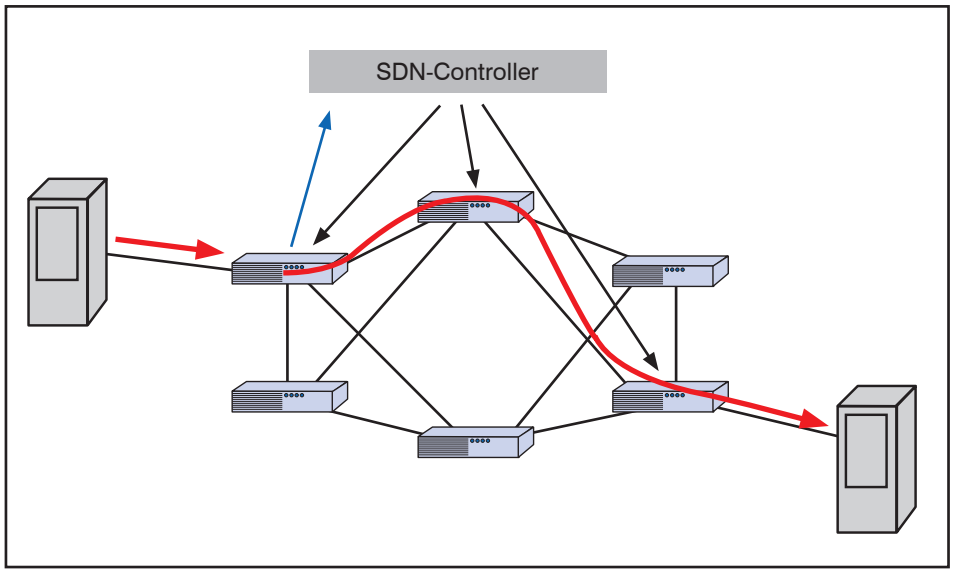

Abbildung 1: Basiskonzept von SDN: zentrale Netzwerksteuerung

3. Aus architektonischer Sichtweise gestattet es OpenFlow von außen die Forwarding Plane von Netzwerkkomponenten zu manipulieren oder gar komplett zu verwalten. Die sogenannte **Control Plane**, die für diese Aufgabe zuständig ist, wird also praktisch auf den Controller **ausgelagert**.

Hier deutet sich bereits an, dass dieses Konzept einige Freiheitsgrade besitzt, die gerne übersehen werden. Stellt man insbesondere den Controller ins Zentrum des Konzepts, wird schnell klar, dass OpenFlow nur eine mögliche Ausprägung der Schnittstelle zu den Hardware-Geräten ist. Wählt oder entwickelt man eine andere Schnittstelle, kann man sich zum Beispiel von OpenFlow-spezifischen Einschränkungen befreien, insbesondere von der Beschränkung auf Layer-2- bis Layer-4-Merkmale:

- Theoretisch lassen sich nämlich alle klassischen Netzwerkgeräte vom Switch und Router bis hin zu Firewall und Loadbalancer steuern bzw. deren Regelwerk bedarfsgerecht anpassen.

- Das Konzept (auch mit OpenFlow) erzwingt keineswegs, dass jeglicher Datenverkehr vom Controller gesteuert werden muss. Wir werden diesen Aspekt weiter unten noch diskutieren.

- Und das Konzept erzwingt keineswegs, dass es nur einen Controller gibt. Es gibt tatsächlich Lösungen mit spezialisierten Controllern für bestimmte Gerätetypen oder Protokolle. Auch diesen Punkt werden wir unten etwas genauer beleuchten.

Was hierbei auf den ersten Blick komplex aussieht, ist das genaue Gegenteil. Es macht überhaupt keinen Sinn Firewalling-Funktionalität in eine Lösung zu bringen, die im Kern die Wegewahl durch das Netzwerk regeln soll. Andererseits wäre es schade, Firewalls prinzipiell auszuschließen.

Die spannende Frage ist also, wie dieses Grundgerüst in der Praxis umgesetzt wird. Tatsächlich gibt es eine breite Palette von Möglichkeiten, die die Bandbreite von SDN aufzeigen, aber gerade auf Grund dieser Bandbreite auch für viel Verwirrung und Unsicherheit im Markt sorgen.

Die Vision: SDN überall

Den Entwicklern von SDN schwebte schon früh die Vision vor, den beschriebene Entwurf auf der Basis von OpenFlow flächendeckend für gesamte Unternehmens- oder Campusnetze einzusetzen und alle Netzwerkkomponenten über einen zentralen Controller zu steuern.

Nick McKeown, einer der Gründungsväter, hatte in seinen Präsentationen folgende Definition von SDN:

> A network in which the control plane is physically separate from the forwarding plane.
>
> and
>
> A single control plane controls several forwarding devices.
>
> (That's it)

Mit anderen Worten: „Dumme" Netzwerkkomponenten, die nur das reine Packet Forwarding umsetzen, werden von einer zentralen Controller-Instanz gesteuert, wo die komplette Netzwerkintelligenz und alle Statusinformationen des Netzes zusammengeführt werden.

Die Erwartungen an dieses allumfassende und sehr strikte Modell waren sehr groß und wurden mit entsprechend markigen Worten vorgetragen:

- Ablösung der statischen und dezentralen Netzwerkkonzepte aus den 50er- und 60er-Jahren durch dynamische, zentral gesteuerte Strukturen,

- Ablösung der „Mainframe-artigen", proprietären und komplexen Netzwerkkomponenten durch einfache und günstige „Forwarding Devices", möglichst auf Basis von i386-Standardkomponenten,

- Ablösung von standardsbasierenden Netzwerkprotokollen mit Innovationszyklen in der Größenordnung von Jahrzehnten (Was ja mit Blick auf die IEEE und IETF durchaus realistisch ist!) durch moderne, schnellentwickelte Softwaremodule im Controller, möglichst auf Open-Source-Basis.

Kurz: Alles wird einfacher und alles wird billiger.

Was bedeutet ein solches Modell für das Netzwerk?

Bleiben wir hierzu kurz noch bei der Vorstellung, dass alle mit der Bearbeitung und Weiterleitung von Netzwerkverkehr beschäftigten Geräte in eine gemeinsame SDN-Architektur eingebunden sind und von einer einzigen übergeordneten Controller-Instanz gesteuert werden.

Ein solches Netz hat beeindruckende neue Eigenschaften: Es gibt im Grunde keine Layer-2- oder Layer-3-Domänen mehr!

Der Controller definiert nämlich für jede Kommunikationsbeziehung, zum Beispiel für eine Datenbankverbindung zwischen zwei Servern oder für eine Anwendung zwischen Server und Client, je einen Pfad von Endpunkt zu Endpunkt quer durch das Netzwerk und verteilt die dazugehörenden Weiterleitungsregeln entlang dieses Wegs.

Und da er das für alle Datenverbindungen macht, heißt das, unser Netzwerk besteht nur noch aus bedarfsgerecht, dynamisch aufgebauten Punkt-zu-Punkt-Verbindungen (gegebenenfalls auch Punkt-zu-Mehrpunkt-Verbindungen): kein Spanning Tree, keine Routing Protokolle, kein Shortest-Path-Bridging und ähnliches, keine VLANs

etc. Das Netz (d. h. der Controller) weiß wer mit wem wie kommuniziert und die Pfade durch das Netz können bedarfsgerecht, also zum Beispiel lastabhängig, angepasst werden.

Ein solches flowbasierendes Punkt-zu-Punkt-Layout ist insbesondere deshalb von Bedeutung, weil unsere Anwendungen so arbeiten. Anwendungen versenden in der Regel keine Pakete, sondern Datenströme. Wenn das Netz jetzt ebenfalls auf der Basis von Datenströmen arbeitet, ist das für den Betrieb und das Design des Netzes natürlich vorteilhaft, insbesondere, wenn wir zukünftig Anwendungen in den Fokus unserer Betriebskonzepte stellen wollen (Stichwort Software-Defined Data Center).

Die zentrale Komponente dieses Modells wird der Controller, ohne ihn läuft nichts. Mögliche Controller sollen daher jetzt schon aus Stabilitätsgründen modular aufgebaut werden (siehe Abbildung 2):

1. Die Schnittstelle zur Netzwerk-Hardware mit OpenFlow oder einem vergleichbaren Kommunikationsprotokoll bildet das sogenannte Southbound-Interface.

2. Um den Controller selbst schlank und dynamisch erweiterungsfähig zu machen, wird zusätzlich eine Erweiterungsschnittstelle, das sogenannte Northbound-Interface eingeführt.

3. Auf dieser Schnittstelle setzen alle Anwendungen auf, die Informationen aus dem Netz und anderen relevanten Systemen abrufen, auswerten und die Entscheidungskriterien für den Controller liefern.

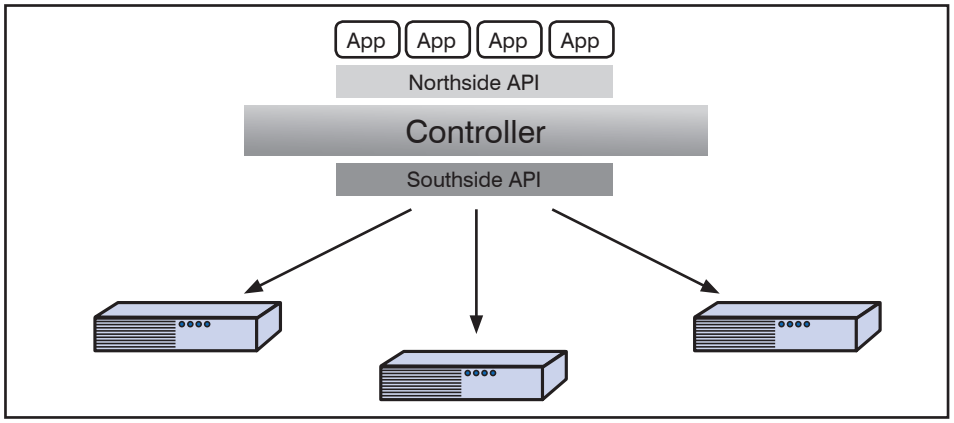

Abbildung 2: Modulare Konzeption des SDN-Controllers

Um die visionäre Kraft dieses Konzepts weiter zu unterstreichen, wird an dieser Stelle gerne der Begriff vom „Netzwerkbetriebssystem“ eingeführt und mehr oder weniger überzeugende Analogien zur klassischen Rechnerarchitektur hergestellt (siehe Abbildung 3).

Der Leistungsumfang dieses Modells wird offensichtlich vom Funktionsumfang des Southbound-Interfaces bestimmt: Nur der Regelsatz, der vom Controller bereitgestellt und auch von den Netzwerkkomponenten unterstützt wird, kann genutzt werden.
Damit kommt dieser Schnittstelle für das betrachtete „One size fits all“-Modell eine erhebliche Bedeutung zu – und zwar nicht nur auf Controller-Seite, sondern auch in den Netzwerkkomponenten.

Das wichtigste Projekt zur Entwicklung einer solchen Schnittstelle ist natürlich OpenFlow.

OpenFlow wird mittlerweile von nahezu allen Herstellern zumindest in Teilen ihres jeweiligen Switch-Portfolios unterstützt, einschließlich einiger Herstellern von virtuellen Switches. Da im betrachteten Modell die Control Plane der Switches auf den Controller ausgelagert ist, hat OpenFlow damit das Potential, den für virtuelle Switche typischen Mangel an Funktionsumfang auszugleichen.

Trotzdem ist OpenFlow nicht das einzige Protokoll zur Realisierung eines Southbound-Interfaces. Die Alternativen reichen von XML über Routingprotokolle wie BGP und IS-IS bis zu ganz proprietären Lösungen.

Kritik am „SDN überall“-Modell

Der entscheidende Punkt bei diesem Modell (ein Controller steuert zumindest alle Layer-2- und Layer-3-Komponenten vollständig) ist, dass es alles im und um das Netzwerk ändert: die Art wie Datenströ-

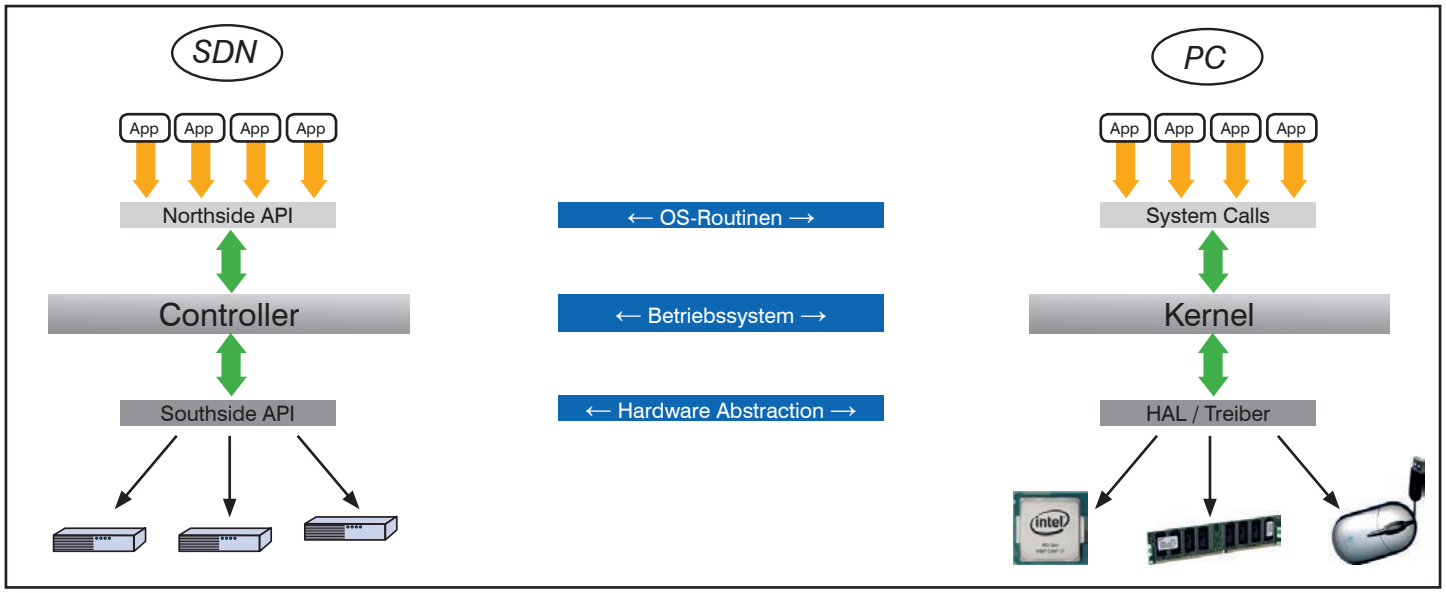

Abbildung 3: Analogie „Netzwerkbetriebssystem“

me durch das Netz geleitet werden, die Konzepte wie Datenströme voneinander getrennt werden, in der Regel müssen alle Komponenten ausgetauscht werden (lediglich in Ausnahmefällen reicht hier und da eine neue Firmware) etc. pp.

Natürlich könnte man argumentieren, dass man ja alle klassischen Netzwerkprotokolle im Controller nachbilden könne, und tatsächlich gibt es Ansätze, zum Beispiel IP-Routing controllerbasierend nachzubauen, inklusive Hop-Count-Reduzierung etc. Aber ernsthaft: Das ist doch absurd. Da wird eine neue Technologie entwickelt, um das Forwarding bedarfs- und anwendungsgerecht zentral steuern zu können, und dann emuliert man über diese zentrale Steuerung die klassischen dezentralen Regelungen? Das kann nicht der richtige Weg sein.

Wir brauchen lösungsorientierte Produkte, die SDN-Konzepte in unsere Netze ***integrieren*** und die Vorteile von SDN nutzen, ohne alles, was gut funktioniert, zu verwerfen.

Doch wo liegt der eigentliche Mehrwert von SDN? Einfach nur Switches und Router zentral steuern zu können, ist ein bisschen wenig, selbst, wenn das mit OpenFlow o. ä. eines Tages herstellerübergreifend möglich wäre.

Der entscheidende Punkt, der SDN zu „Software-Defined“ macht, ist das Northbound-Interface, die Schnittstelle des Controllers zu netzwerkrelevanten Informationen (siehe Abbildung 3)!

Genau das ist der Kern von SDN: Während klassische Netzwerkprotokolle auf dem Prinzip Lernen beruhen und ausschließlich Informationen aus dem Netz selbst zur Entscheidungsfindung heranziehen können, hat SDN zusätzlich Zugriff auf ergänzende Informationen aus weiteren Quellen.

Typische Beispiele hierfür sind:

- das Hypervisor-Management (Wo befindet sich eine virtuelle Maschine? Welche MAC- und IP-Adressen hat sie? Wurde sie gerade bewegt? …),
- das Cloud-Management (Welche Container werden gestartet? Sind andere Clouds angebunden? …),
- Anforderungen der Anwendungen (Der folgende Datenstrom belegt eine bestimmte Bandbreite oder ist abhängig von maximalem Jitter, …).

Lassen Sie uns einen Blick auf solche Produkte werfen.

SDN zur Edge Provisionierung

Ein weiterer Problempunkt des oben diskutierten OpenFlow-Ansatzes ist, dass jedes einzelne Gerät im Netzwerk jedes eintreffende Paket zu den definierten Flows bzw. Regeln zuordnen muss, unabhängig davon wie komplex und aufwändig diese Zuordnung ist. Im Zweifelsfall bedeutet dies den Einsatz teurer ASICs – und zwar in jedem Gerät.

Deutlich einfacher ist dagegen der Ansatz, alle Pakete am Rand des Netzes zu markieren und sie ab dann nur noch anhand dieser Markierung weiterzuleiten. Nutzt man zur „Markierung“ etablierte Methoden wie beispielsweise Tunnelprotokolle, bedeutet das:

- Der SDN-Controller ist ausschließlich für die Provisionierung der Tunnel zuständig.
- Damit hat man eine funktionale Trennung des Netzes in SDN-gesteuerte Ingress-Systeme und ein klassisches Transportnetz.
- Das Forwarding in diesem inneren Transportnetz kann mit Standardverfahren ohne SDN erfolgen.

VMware NSX ist ein Beispiel für den Einsatz einer solchen SDN-gesteuerten Edge

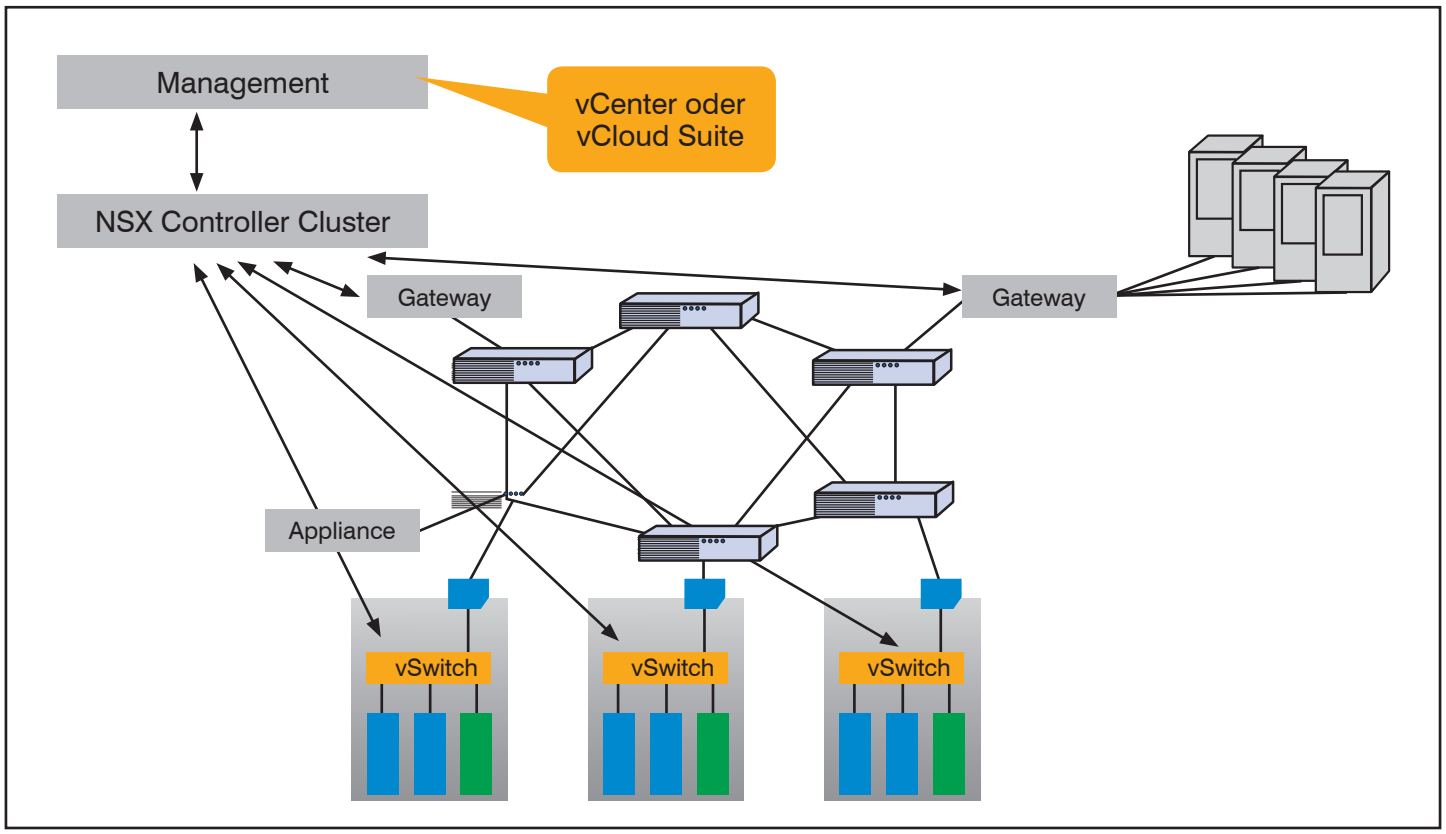

Abbildung 4: VMware NSX

Provisionierung (siehe Abbildung 4). Das Produkt verbindet virtuelle und physische Server durch Layer-2-Tunnel über ein IP-basierendes Transportnetz. Wie immer in einer solchen Umgebung verfügen die Tunnelendpunkte in den Hypervisors der Virtualisierungshosts und den Gateways jeweils über eine Zuordnungstabelle, in der verzeichnet ist, über welchen Tunnelendpunkt welcher Server erreichbar ist.

Wären wir jetzt in einem klassischen Umfeld, könnten sogenannte unknown Unicasts auftreten. Das heißt, der sendende Tunnelendpunkt findet die Zieladresse eines Servers nicht in seiner Zuordnungstabelle, er weiß also nicht welchen Tunnelendpunkt er adressieren muss. Klassisch bleibt dem Host daher nichts Anderes übrig als Broadcasts oder sogar Multicasts (da das Gesamtkonzept mandantenfähig ist) zu nutzen.

Anders im SDN-Umfeld: Hier hat der NSX-Controller eine Schnittstelle zum Hypervisor-Management und kann somit die Tunnelendpunkt bereits proaktiv darüber informieren, wo sich welcher virtuelle Server befindet und wann ein Server zu einem anderen Host verschoben wird (in der ursprünglichen Nicira-Version des Produkts übrigens über OpenFlow). Es gibt keine unknown Unicasts.

SDN zur Sicherstellung von Quality of Service in Voice- und Video-Netzen

Microsoft hat als Teil seiner Skype-for-Business-Architektur eine interessante Schnittstelle geschaffen, die für SDN-Umgebungen genutzt werden kann. Das „Skype for Business SDN Interface“ ist kein Controller sondern im Sinne von Bild 3 eine Anwendung, die über die Northside-Schnittstelle des SDN-Controllers diesen mit netzwerkrelevanten Informationen versorgt (siehe Abbildung 5).

Im konkreten Fall sind dies Informationen über Kommunikationsverbindungen zwischen Skype-Usern, die der SDN-Umgebung in Echtzeit zur Verfügung gestellt werden. Hierzu gehören insbesondere (siehe Abbildung 6):

- die IP-Adressen der Endgeräte,
- die UDP-Ports der Medienströme,
- die Art der Kommunikation (Voice, Video, Chat, Screen-Sharing, File-Transfer etc.),
- Protokoll, Codec, Bandbreite und mehr.

Solche Informationen sind gerade in Netzen wie zum Beispiel WLANs, wo Bandbreite und Delay Störungen verursachen können, hilfreich, da sie zwei Probleme adressieren:

1. Identifizieren von autorisierten Echtzeitverbindungen,

2. Reservieren von Bandbreite.

Und tatsächlich gibt es eine Reihe von Herstellern, die diese SDN-Schnittstelle von Skype for Business abgreifen und die Information zur Steuerung von (Teil-) Netzen nutzen:

- Die Hersteller Aruba Networks, Dell und Meru nutzen die Information in ihrer controllerbasierenden WLAN-Infrastruktur, um Voice- und Video-Ströme sowohl im Funknetz als auch im kabelgebunden Netz zu priorisieren.

- HP hat eine passende Schnittstelle in ihrer „Network Optimizer SDN Application“ und kann via OpenFlow den einzelnen Datenströmen ebenfalls QoS-Policies zuordnen.

Die Forderung nach Standardisierung

In guter(?), alter Netzwerkertradition wird gerne gefordert, beide Controller-Schnittstellen, sowohl Northside als auch Southside, müssten standardisiert werden – und tatsächlich finden sich die bekannten Hersteller reflexartig zusammen, um gemeinsame Verfahren festzuschreiben. Warum eigentlich?

Die böse, wenn auch nicht völlig aus der Luft gegriffene Antwort ist: Weil alle aus Erfahrung wissen, dass ein Standardisierungsprozess das beste Mittel ist, um eine Innovation möglichst lange aufzuhalten.

Ist aber eine Standardisierung dieser Schnittstellen überhaupt nötig oder gar sinnvoll?

Beim Southside-Interface ist man spontan noch am ehesten geneigt, eine stan-

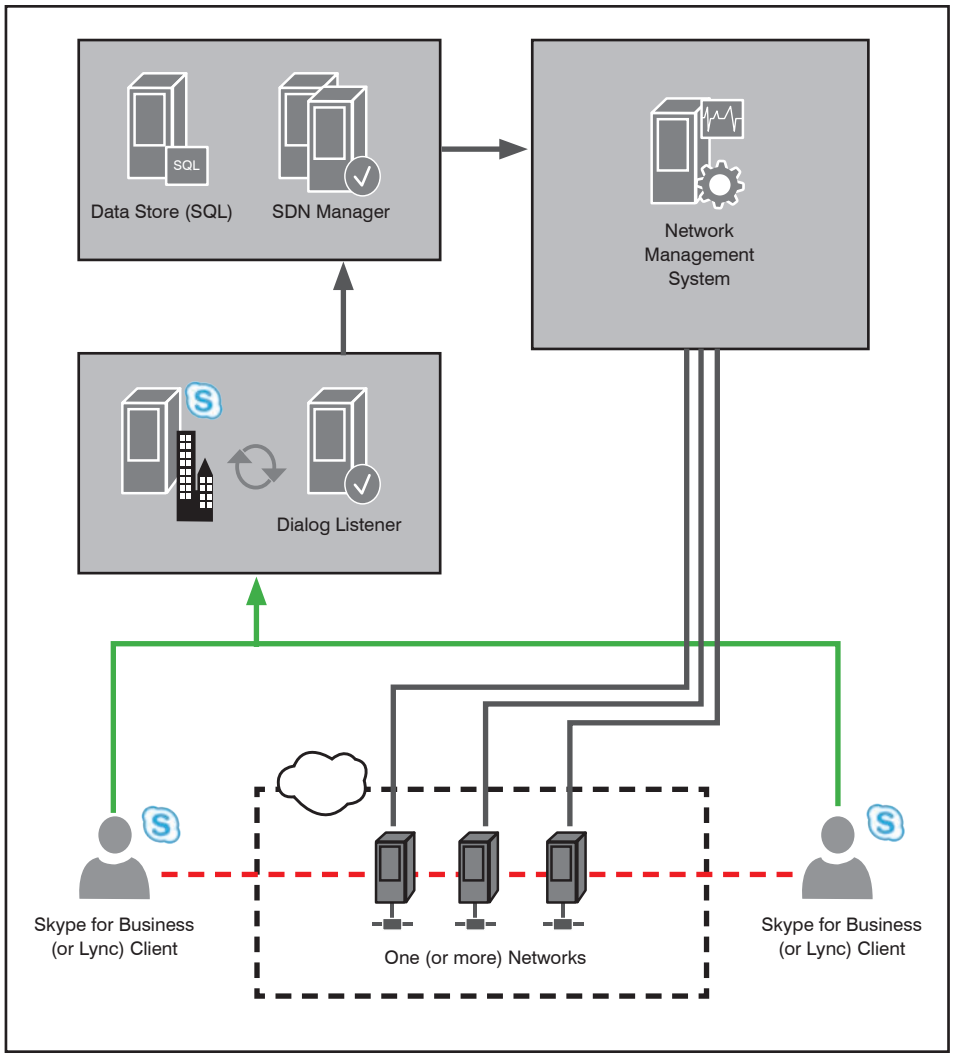

Abbildung 5: Die Architektur des Microsoft Skype for Business SDN Interface

Quelle: Microsoft

dardisierte Schnittstelle zu fordern, um nämlich Interoperabilität mit der Netzwerk-Hardware zu erreichen.

Hier muss man genau hinschauen, wie die SDN-Umgebung ausschaut, welches Konzept umgesetzt werden soll. Denn obwohl die Southside-Schnittstelle von vielen gerne dem Controller zugeordnet wird, geht's im Grunde um eine Schnittstelle in den Netzwerkkomponenten selbst!

Die Frage ist also, ob man über nur einen Controller herstellerübergreifend Netzwerkkomponenten steuern möchte. Wenn man diese Frage mit Ja beantwortet, braucht man natürlich tatsächlich ein standardisiertes Kommunikationsprotokoll wie beispielsweise OpenFlow. Konzeptionell ist es aber völlig überflüssig zu fordern, dass nur gleichartige Systeme über dasselbe Protokoll angebunden werden können. Das Gegenteil würde einen Controller deutlich flexibler machen. Schauen Sie noch einmal auf das obige Beispiel mit dem Skype-SDN-Interface: Warum sollten die genannten WLAN-Hersteller zusätzlich OpenFlow in ihren Access Points und ihren Controllern unterstützen? Klar wäre es nett, wenn man alle WLAN-Controller und Access Points herstellerübergreifend austauschen könnte, aber es ist doch ziemlich unrealistisch, das zu fordern.

Auch bei der nördlichen Schnittstelle bewerte ich eine Standardisierung eher als hinderlich. Natürlich wird man von einem Controller erwarten, dass er eine möglichst große Anzahl von Standardschnittstellen unterstützt. Dazu gehören sicherlich XML, REST u. ä., vermutlich auch BGP und LLDP, aber das heißt doch nicht, dass die Schnittstelle selbst einer aufwändigen Standardisierung unterworfen werden muss. Wir sprechen gerade über Software! Innovation ist hier wichtiger als Interoperabilität. Und wer besser ist, wird sich durchsetzen.

Zusammenfassung

Die Diskussion um SDN wird sehr technokratisch geführt – und meist steht dabei OpenFlow im Zentrum. Diese Fixierung auf OpenFlow verhindert aber den unbelasteten Blick auf SDN. SDN ist nicht gleich OpenFlow!

Die Intension von OpenFlow ist eine hardwareunabhängige Schnittstelle zwischen Controller und standardisierter Hardware (Southbound Interface).

Diese Idee des einen omnipotenten Controllers, der riesige Netze mit gleichartigen, billigen Switches steuert, ist aber

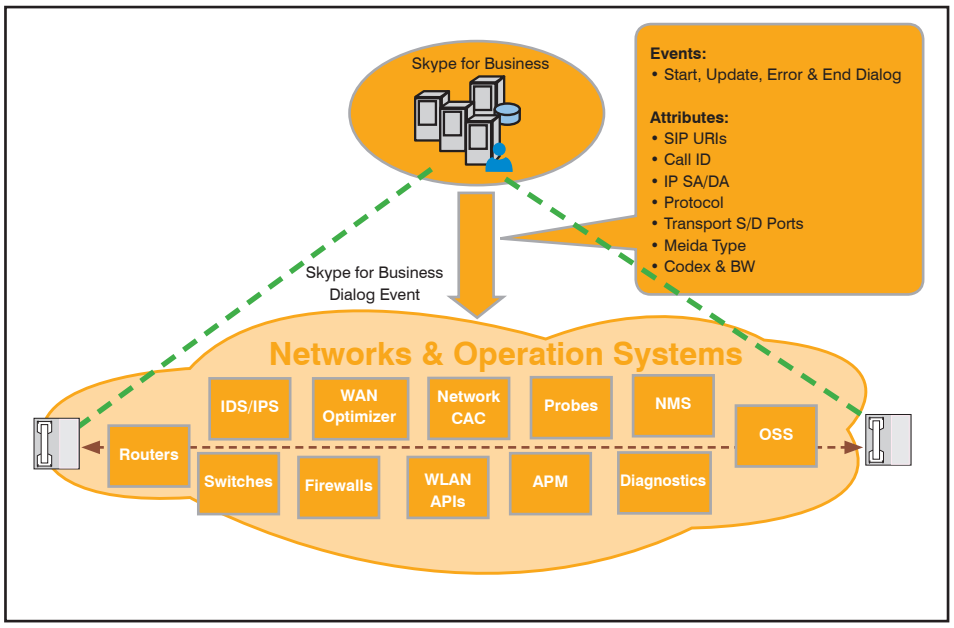

Abbildung 6: Skype for Business Dialog Event Quelle: Aruba Networks

auch zu interessant als dass man sie einfach ignorieren könnte. Ernsthaft umsetzen lässt sie sich aber nur in sehr speziellen Monokulturen, wie sie die sehr großen Provider betreiben. In Unternehmensnetzen ist die Realisierung dieses Konzepts zu aufwändig, mit zu vielen Risiken verbunden und bringt vor allem unter dem Strich zu wenig Mehrwerte.

SDN dagegen (SD steht für Software-Defined!) bezieht sich mehr auf das Norhbound Interface. Hier geht es um ein Konzept, zusätzliche Informationen zur Netzwerksteuerung hinzuzuziehen, auf die klassische Netzwerkprotokolle keinen oder zumindest keinen einfachen Zugriff haben.

Verzichtet man mit Blick auf diese Idee auf den einen Controller und auf die Hardwareunabhängigkeit der südlichen Schnittstelle, wird vieles deutlich einfacher und sinnvoller:

- Der Controller steuert nicht in Alleinverantwortung den gesamten Netzverkehr, sondern greift nur Sonderfällen korrigierend ein. Beispiele sind unknown Unicasts in virtualisierten Serverumgebungen oder Voice-Datenströme, die im WLAN priorisiert werden.

- Es können verschiedene spezialisierte Controller zur Steuerung spezieller, gegebenenfalls auch herstellerspezifischer Umgebungen nebeneinander genutzt werden.

- In Umgebungen, wo es bereits zentrale Systeme zur Steuerung von Netzwerkkomponenten gibt (wie z. B. WLAN-Controller) können diese auch SDN-ähnliche Aufgaben übernehmen.

Die Forderung nach Standardisierung von Northbound Interface, Southbound Interface oder gar des ganzen Controllers erscheint vor diesem Hintergrund wie eine Verhinderungstaktik. Dabei geht es bei allem, was auf uns zukommt (Software-Defined Data Center, Cloud Computing etc.), gerade um das Gegenteil, nämlich um Flexibilität, Dynamik, Agilität.

Es drängt sich natürlich auf, SDN in virtualisierten Umgebungen einzusetzen: Virtuelle Netzwerkkonstrukte sind eh schon Software und es gibt ein übergeordnetes Management, das nahezu alles über die virtuelle Umgebung weiß und damit im SDN-Sinne eine ideale Informationsquelle zur Netzwerksteuerung ist.

Aber SDN ist nicht auf virtualisierte Umgebungen beschränkt. SDN ist der momentan der wichtigste, vermutlich sogar einzige Ansatz, um die Anforderungen von Anwendungen an das Netzwerk dynamisch und automatisiert umzusetzen. Hier geht es nicht um irgendwelche Tunnelprotokolle, es geht noch nicht einmal primär um den Betrieb Ihrer Netze. Es geht um den Betrieb Ihrer IT.

In diesem Sinne ist SDN immanenter Bestandteil jedes anwendungsbewussten (application aware) Netzes und ein wichtiger Baustein des Software-Defined Data Centers. Und hier wird die Zukunft der Unternehmens-IT entschieden – aber das ist ein anderes Thema.

Aktueller Kongress

ComConsult UC-Forum 2016
21.11. - 23.11.16 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 21.11. bis 23.11.16 ihr "ComConsult UC-Forum" in Düsseldorf.

Der VoIP und UC-Markt ist in einer Umbruchsphase wie wir sie in den letzten 5 Jahren nicht erlebt haben. Die weltweiten Ankündigungen zum Thema Ablösung der PSTN Infrastrukturen sowie die neue Dynamik im Cloud Markt durch den Eintritt der VoIP und UC Entwickler als Provider von UCaaS und cPaaS Lösungen zeigt, dass bisherige Denkweisen und Betriebskonzepte überprüft werden müssen.

Gerade die Umbrüche im öffentlichen Telekommunikationsnetz führen zu technologischen Neuausrichtungen. Dienste wie Fax, Modem und Analoganschlüsse sind in einer IP basierten Kommunikationswelt nicht mehr fortzuführen, wie aber können sie ersetzt werden? UC erfährt durch WebRTC eine komplette Umorientierung, gerade im Hinblick auf eine einheitliche,

webbasierte Basistechnologie, die endlich unabhängig ist von Betriebssystemen oder Entwicklungsumgebungen. Was aber bedeutet dies für unsere Unternehmen? Wird jetzt alles einfacher oder gibt es doch noch Einschränkungen?

Aber auch das Thema Betrieb von VoIP und UC Anwendungen steht vor neuen Herausforderungen. Durch den Markteintritt der Hersteller von Kommunikationslösungen in die Welt der Cloud werden klassische On Premise Modelle immer mehr in Frage gestellt. Jedoch muss auch hier hinterfragt werden, für wen sich ein CAPEX orientierter Ansatz lohnt und für wen die OPEX Variante der richtige Weg ist.

Diese und viele weitere Aspekte sind Schwerpunkt unseres diesjährigen UC-Forums. Seien Sie dabei, unsere Top Referenten erläutern Ihnen die wichtigsten Trends und Entwicklungen die für eine zukunftsfähige Unternehmens-IT unabdingbar sind.

Seien Sie dabei und erhalten Sie die aktuellsten Trendanalysen und Informationen von ComConsult Research mit Top-Referenten, Analysen, Projektberichten und Praxiserfahrungen.

Programmübersicht ComConsult UC-Forum 2016

Montag 21.11.2016 - UC 2016 – Cloud und Co.

9:30 - 10:15 Uhr
Keynote
- Wo steht der Markt für UC, Video und Collaboration?
- Was wurde eigentlich aus WebRTC?
- Welche Fragen wirft All-IP auf?
- Gibt es ein Leben ohne die Cloud?
- Welche Trends gestalten den Arbeitsplatz der Zukunft?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
UC goes http:
WebRTC Anwendungen im Vergleich
- Kommunikation ist mehr als telefonieren
- Warum ist Web Technik hierfür ideal
- Wie schlagen sich die Lösungen etablierter Hersteller: Cisco Spark, Unify Circuit, Alcatel Lucent Enterprise Rainbow, ...

Markus Geller, ComConsult Research GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Monitoring für Enterprise VoIP-Dienste
- Warum nicht Wireshark?
- Qualität von VoIP - Woran hakt es?
- Testing vs. Monitoring - ein integrierter Ansatz
- Übersprechen, Fax-Abbrüche - Troubleshooting-Beispiele aus der Praxis

Dr. Michael Wallbaum, VOIPFUTURE GmbH

12:15 - 12:45 Uhr
Wie reif ist Skype for Business als TK-Ersatz
- Wofür braucht man noch TK-Anlagen wenn es Skype-for-Business gibt?
- Wo liegen die Stärken und Schwächen von S4B?
- Wie stellt sich Microsoft die Video-Integration von morgen vor?
- Was ist die Vision hinter „Surface Hub“?
- Ist Skype-for-Business untrennbar mit Office365 verbunden?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

12:45 - 13:00 Uhr
Tour Guide zur Ausstellung
- Welche Aussteller sind im Forum vertreten?
- Welche Trends lassen sich an der Ausstellung ablesen?
- Was sind die persönlichen Highlights?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:15 Uhr
Arbeitsplatz-Optimierung - Office Delve und Office Graph als Fitness App für das Berufsleben
- Finden Sie heraus, wie effizient Sie kommunizieren, um Ihre Leistungsfähigkeit zu steigern
- Das intelligente Werkzeug erkennt, mit wem und woran Sie arbeiten und verbindet Sie mit neuen relevanten Informationen und Kontakten
- Erkennen Sie, womit andere sich momentan beschäftigen, mit wem sie zusammenarbeiten und wo ihre Kompetenzen liegen
- Office Delve zeigt auf, womit Sie Ihren Arbeitstag verbringen (E-Mails, Besprechungen, …) und ermöglicht Ihnen eine bessere Zeiteinteilung
- Sie erfahren, mit wem Sie wie viel Zeit verbringen und wer mehr Aufmerksamkeit benötigt

Christian Sailer, Microsoft Deutschland GmbH

15:15 - 15:45 Uhra
Blick hinter die Kulissen: innovaphone Cloud
- Architekturkomponenten: PBX, Session Border Controller, Reverse Proxy, PSTN Anbindung (ISDN/SIP/Federation)
- Redundanzmöglichkeiten
- Multiservicefunktionen: Videokommunikation, Desktopsharing, WebRTC Toolbox
- Ende zu Ende Sicherheit durch DTLS Verschlüsselung

Lars Dietrichkeit, innovaphone AG

15:45 - 16:15 Uhr Kaffeepause

16:15 - 16:45 Uhr
Liefert die Cloud die bessere UC-Lösung?
- Wie sehen die UC-Angebote in der Cloud aus?
- Werden alle Funktionsbereiche abgedeckt?
- Welche Anforderungen entstehen an die Verbindung zur Cloud?
- Wie wird Video umgesetzt?
- Ist die Cloud als UC-Lösung wirklich preiswerter?
- Wie können Drittprodukte integriert werden, geht das überhaupt?
- Wie sieht der Betrieb aus, ist er mehr oder weniger aufwendig als eine lokale UC-Lösung?

Markus Geller, ComConsult Research GmbH

16:45 - 17:45 Uhr
Podiumsdiskussion: UC aus der Public Cloud, Pro‘s und Con‘s
Mit Herstellern auf dem Podium

ab 18:00 Uhr Happy Hour

Programmübersicht ComConsult UC-Forum 2016

Dienstag 22.11.2016 - All-IP

9:00 - 9:45 Uhr
SIPconnect 2.0: Neuer Standard für SIP Trunking
- SIPconnect 1.1 • SIPconnect 2.0
- Architektur • Voice-LM
- Video-Unterstützung
- IPv6 • Notruf

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

9:45 - 10:30 Uhr
All-IP Migration aus Carrier- und Kundensicht
- Warum überhaupt All-IP?
- Neue Carrier-Infrastuktur, neue SIP- und VPN-Services: Was ändert sich und wann?
- Chancen durch All-IP: Neue Designansätze bei Sprach- und Datennetzen

Dipl.-Ing. Wilfried Meer, T-Systems International GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:30 Uhr
Nicht alles ist Sprache... - was passiert mit den Sonderanschaltungen beim Umstieg auf All-IP
- Was sind Sonderanschaltungen?
- Was passiert da?
- Was sind die Folgen bei der Abschaltung von ISDN
- Vergleich Gateways vs. IP-Migration
- Wie sieht ein Migrationspfad aus?
- Wie ändert sich der Betrieb?

Henry Lakatos, D.I.E. Projekt GmbH

11:30 - 12:00 Uhr
Einsatzszenarien eines Avaya SBC für Enterprise – weit über SIP-Trunking hinaus!
Relevanz eines SBC an der Demarkationslinie zum Unternehmen
- 5 Gründe für einen Avaya SBCE im Unternehmen (Mehr als nur eine Firewall!, Remote-User, WebRTC, Multimedia, Recording)
- Wie sieht eine SIP Connect Zertifizierung aus?

Thomas Römer, Avaya Deutschland GmbH

12:00 - 12:30 Uhr
All-IP in Filialszenarien
- Was unterscheidet All-IP in Filialszenarien von anderen Szenarien?
- Was ist bei Filialszenarien zu beachten? Wo liegen die Fallstricke?
- Wie sehen Architekturen aus und mit welcher Technik setzt man sie um?

Markus Emde, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:30 Uhr
Cisco Collaboration Cloud
- Neue Modelle der Zusammenarbeit unter Berücksichtigung von veränderten betrieblichen Anforderungen
- Integration von interaktiven Hilfsmitteln und Endgeräten in eine gesamtseitliche SaaS Lösung
- Einbindung von Anwendungen über offene APIs
- Wie adressiert die Lösung die Sicherheitsanforderungen und den Schutz der Privatsphäre

Tobias Neumann, Cisco Systems GmbH

14:30 - 15:15 Uhr
Datenschutz bei der Umstellung auf All-IP
- Verschlüsselungsanforderungen und Netztrennung
- SIP-Trunking und Verschlüsselung
- Anforderungen durch das IT-Sicherheitsgesetz und die Cyber-Security-Richtlinie der EU
- Anforderungen durch die EU-Datenschutzverordnung ab Mai 2018

Ulrich Emmert, esb Rechtsanwälte

15:15 - 15:45 Uhr Kaffeepause

15:45 - 16:45 Uhr
Enterprise Session Border Controller: Evaluierung
- Einsatzbereiche: UNI, NNI, E-SBC
- Funktionsbereiche
- ALE, Avaya, Cisco, Mitel, Unify

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

Mittwoch 23.11.2016 - Thementag „Arbeitsplatz der Zukunft“

9:00 - 9:45 Uhr
Einführung zum RfQ „Arbeitsplatz der Zukunft“
- Welche Anforderungen stellen sich an den Arbeitsplatz der Zukunft?
- Welche Szenarien und Use Cases wurden im RfQ angefragt?
- Welche Hersteller und Lieferanten beteiligen sich an der Live-Demo?

Dipl.-Ing. Dominik Zöller, ComConasult Beratung und Planung GmbH

9:45 - 12:00 Uhr (integrierte Kaffeepause)
Live-Demos zum RfQ „Arbeitsplatz der Zukunft“
Referenten der teilnehmenden Hersteller und Lieferanten
- Führung zu den Live-Demo-Stationen der Aussteller
- Präsentation von Use-Cases
- Anschauen und Ausprobieren von realen Arbeitsplatzszenarien

12:00 - 12:45 Uhr
Wieviel Social Collaboration braucht ein Unternehmen?
- Wie relevant ist Social Collaboration für Unternehmen?
- Wann sollte man mit Social Collaboration starten?
- Wie führt man Social Collaboration ins Unternehmen ein?

Dr. Thomas Kreye, CEO, Just Software AG

12:45 - 13:45 Uhr Mittagspause

13:45 - 15:00 Uhr
Diskussionsrunde „Arbeitsplatz der Zukunft“
- Offene Diskussionsrunde mit Ausstellern und Teilnehmern
- Anregungen und Kritik zu den gezeigten Arbeitsplatzkonzepten
- Erfüllen die gezeigten Arbeitsplätze die Teilnehmererwartungen?
- Erfahrungsaustausch

15:00 - 15:45 Uhr
Arbeitsplatztransformation und Change-Management
- Wie führt man neue Technologien am Arbeitsplatz ein?
- Wie wichtig ist Change Management für die Arbeitsplatztransformation?
- Welche CM-Maßnahmen haben sich in der Praxis bewährt?

Johanna Ahrens, avodaq AG

15:45 - 16:00 Uhr
Wrap-up des Tages

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

Anmeldung an kundenservice@comconsult-research.de

ComConsult UC-Forum 2016

Ich buche den Kongress
ComConsult UC-Forum 2016

☐ Kongress mit Thementag
21.11. - 23.11.16 in Düsseldorf - € 2.390,--

☐ Kongress ohne Thementag
21.11. - 22.11.16 in Düsseldorf - € 1.990,--

☐ Thementag am 23.11.16 - € 990,--

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Standpunkt

Universelle Mobilität – ist das gesund?

Der Standpunkt von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Sie haben es vermutlich gelesen: Microsoft hat seine neue Deutschland-Zentrale in München bezogen. Dort erlebt man nun, wie Microsoft sich die Arbeit der Zukunft vorstellt. Es gibt keine festen Arbeitsplätze mehr. Mitarbeiter arbeiten im „Home-Office“ oder nutzen vor Ort einen der zahlreichen „Workspaces“. Da gibt es Think Workspaces, wo Ruhe zum konzentrierten Arbeiten herrscht. Oder Share & Discuss Workspaces für spontane Meetings. Es gibt Converse Workspaces, Accomplish Workspaces und so weiter. Microsoft nennt das „ideale Bedingungen für zeitgemäßes Arbeiten“.

Wahrscheinlich sieht Ihr Arbeitsplatz noch ganz gewöhnlich aus. Tastatur, Bildschirme, Maus und vielleicht ein Laptop in der Docking Station daneben. Aber Hand aufs Herz, ohne Funk geht auch dort fast nichts mehr. Wenn Sie Ihren Arbeitsplatz verlassen und sich in einen Besprechungsraum begeben, erwarten Sie selbstverständlich die Möglichkeit, auf Ihre Daten zugreifen zu können – Präsentationen halten Sie vom Laptop oder vielleicht bereits von einem Tablett. Ob das praktischer ist, sei dahingestellt, leichter ist es allemal. Und selbstverständlich ist Ihr Smartphone immer dabei – und „always on“.

Wie alle diese mobilen Endgeräte kommunizieren, haben Sie an dieser Stelle schon mannigfach gelesen. Im Außenbereich ist es der Mobilfunk, im Büro oder in der Halle das WLAN. Und hohe Bitraten verlangen nach hoher Dichte der Access Points, nach hoher Signalstärke, flächendeckend. Kann das gesund sein?

Zu Anfang des Jahrtausends, als WLAN und Mobilfunk sich gerade zu verbreiten anschickten, herrschte eine große Unsicherheit bezüglich möglicher Gesundheitsrisiken. Ich erinnere mich an ein ComConsult-Forum im Jahre 2002, auf dem wir dieses Thema heiß diskutiert haben. Inzwischen scheint ein wenig Gras über die Sache gewachsen zu sein. Und doch, gerade jetzt werde ich von Zeit zu Zeit wieder danach gefragt.

Die Frage der Unbedenklichkeit von Funkwellen lässt sich nur aus der gesetzlichen Perspektive eindeutig beantworten. Die 26. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes nennt Grenzwerte, die beim Errichten von Funkanlagen zu beachten sind. Diese Grenzwerte schützen uns vor den thermischen Wirkungen von Funkwellen, die Sie vom heimischen Mikrowellenherd kennen. Die Sendeleistungen von WLAN sind jedoch so gering, dass diese Grenzwerte immer eingehalten werden. So weit, so gut. Aber es soll ja auch nicht thermische Wirkungen von Funkwellen geben.

Darüber ist viel geforscht worden, insbesondere eben zu Anfang des Jahrtausends. Industrie-nahe Institutionen verteidigten den gesetzlichen Grenzwert. Bürger-nahe Organisationen gaben Empfehlungen für geringere Grenzwerte heraus, so genannte Vorsorgewerte. Diese Werte liegen im Bereich zwischen einem Hundertstel bis zu einem Hundert-Millionstel (!) des gesetzlichen Grenzwerts – letzterer übrigens für Schlafbereiche.

Diese Schwankungsbreite reflektiert die nach wie vor bestehende Unsicherheit. Inzwischen hat man aber erkannt, dass sich Erkrankungen des Menschen nicht einfach auf eine Ursache zurückführen lassen. Signifikante Zusammenhänge zwischen den allgegenwärtigen Funkwellen – Radio, Fernsehen, Mobilfunk, Schnurlostelephone, WLAN, Bluetooth, um nur einige zu nennen – und zunehmenden Erkrankungen haben sich bisher nicht nachweisen lassen.

Übrigens wird WLAN an Ihrem Arbeitsplatz schwächer sein als ein Zehntausendstel des gesetzlichen Grenzwertes. Und die stärksten Signale stammen von Ihrem eigenen Endgerät, also Laptop oder Smartphone. Da Funksignale mit dem Quadrat des Abstandes abnehmen, wird die WLAN-Basisstation (der Access Point) unter der Decke noch einmal um den Faktor Zehn bis Tausend schwächer sein – selbst wenn die WLAN-Ausleuchtung für höchste Bitraten optimiert wurde.

Wie denken Sie über dieses Thema? Ist die Frage nach der gesundheitlichen Unbedenklichkeit von Funkwellen in Ihrem Unternehmen gestellt worden oder spielt das keine Rolle? Ich freue mich auf die Diskussion mit Ihnen, vielleicht auf der Sonderveranstaltung Wireless und Mobility am 12. und 13. Dezember in Köln.

Aktuelles Intensiv-Seminar

Winterschule 2016 – Intensiv-Update auf den neuesten Stand der Netzwerktechnik 05.12. - 09.12.2016 in Aachen

Die ComConsult Akademie veranstaltet vom 05.12. bis 09.12.2016 ihre "Winterschule 2016 – Intensiv-Update auf den neuesten Stand der Netzwerktechnik" in Aachen.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen.

Architekturen
- Wie ändert sich die IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerkseite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

Rechenzentren: neue Arten von Infrastrukturen gefragt
- Strategien für das Rechenzentrum der Zukunft:
- Software-Defined Networks SDN: Was ist der Kern von SDN? Wo unterscheidet sich SDN von klassischen Netzwerkarchitekturen? OpenFlow, Netzwerkvirtualisierung und weitere Ansätze; Ciscos Sonderweg: ACI und QoS im RZ
- Cloud Computing: Cloud Konzepte: Private, Public oder Hybrid? Was leistet die Cloud heute, welche Anforderungen entstehen bei der Anbindung? Software as a Service: Warum Cloud-Anwendungen anders sind. Hinter den Kulissen: Typische Cloud-Anwendungen im Praxistest

Netzwerk-Technologien: aktuelle Entwicklungen
- Was ist IoT?
- Anwendungsbereiche und Einsatzszenarien
- Infrastrukturen • Roadmap

SDN und NFV in der Analyse
- Wo steht der Markt?
- Was ist NFV und wo setzen wir es wann ein?

- Welchen Stellenwert hat Hardware in den neuen Technologien?
- Wie hängen SDN und NFV zusammen?

Netzwerk-Design-Lösungen im direkten Vergleich
- Layer 3 Design
- Layer 3/4 Design
- Sonderfälle
- Empfehlungen

VMware NSX: Zukunft oder Irrweg?
- Was ist der Bedarf?
- Wie nutzbar ist NSX wirklich?
- Sind die vorhandenen Alternativen besser?
- Gibt es einen mindestens gleichwertigen herstellerneutralen Weg?

Unified Communications, das Ende von ISDN
- Motivation: Warum All-IP? Einführung in das Thema
- SIP Trunking vs. PSTN: Was sind die wesentlichen Unterschiede?
- Standards für Enterprise- und Provider-Peering
- Session Border Controller: Funktionalität und Markt
- Provider-Marktübersicht: Geschäftsmodelle und Angebote
- Was kommt nach 2018?
- Architektur einer globalen All-IP Kommunikation

Sicherheit
- Abwehr zielgerichteter Angriffe: Notwendigkeit system- und anwendungsübergreifender Strategien
- Netzbasierende Sicherheit: Praxiserfahrungen aus den Bereichen Verschlüsselung, Zonenkonzepte, NAC und Testumgebungen
- Sicheres Cloud Computing und sicheres Mobile Computing: Möglichkeiten und Grenzen
- Sicherheit und UC: Immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Underlay – Overlay
- Underlay Design
- VXLAN als De-facto-Standard für Overlay Data Plane
- Overlay Control Plane: Varianten
- BGP als De-facto-Standard für Overlay Control Plane
- Teufel im Detail: redundante Anbindung von Servern

Enterprise WLANs und ihre technologischen Grenzen
- Das Medienzugangsverfahren DCF: Ist es für eine immer größer werdende Anzahl von Teilnehmern pro Zelle geeignet oder laufen wir in ein Problem?
- Schneller, näher, höher: Wie sich WLAN-Technik in Richtung 10 Gigabit entwickelt
- MU-MIMO in der Analyse: Ist dies der Schlüssel zu höherer Performance in der Zelle?
- Wie profitieren Enterprise WLANs von den neuen Technologien?
- Wie sieht der Bedarf konkret aus, brauchen wir Multi-Gigabit und ist diese Entwicklung wirtschaftlich?

Analyse der neuesten Entwicklungen Explosives Wachstum in allen Anforderungsbereichen
- Echte Multi-Gigabit WLANs mit IEEE 802.11ad
- Die nächsten WiFi-Generationen 11ax und 11ay
- Die Entwicklung von LTE
- Problematik von LTE in lizenzfreien Bereichen
- Kommt schneller als man denkt: 5G Mobilfunk
- Anforderungen an unterstützende Infrastrukturen

Programmübersicht Winterschule 2016

Montag, der 05.12.16 - IT-Architekturen und Auswirkungen auf Infrastrukturen

10:00 - 12:30 Uhr

IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand, unsere IT-Landschaft wird in 5 Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

Wir analysieren für Sie:
- Wie ändert sich die IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerkseite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen Sie speziell bei den Planungen für die nächsten Jahre beachtet werden?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:00 - 17:00 Uhr

Rechenzentren: neue Arten von Infrastrukturen gefragt

Rechenzentren sind unter Druck:
- Die Cloud puscht das Thema Wirtschaftlichkeit, Kosten und Transparenz
- Mobile Endgeräte erfordern mindestens eine Private Cloud Infrastruktur und einen Übergang zu benutzerzentrischen Lösungen
- Server- und Speicher-Konsolidierung gehen permanent weiter, hochskalierende Infrastrukturen sind gefordert
- Virtualisierung geht in die nächste Runde und öffnet die Tür zu automatischen Lastausgleichen und Provisionierungen mit erheblichen Anforderungen an Infrastrukturen

Wir analysieren für Sie:
Strategien für das Rechenzentrum der Zukunft:
- Software-Defined Networks SDN: Was ist der Kern von SDN? Wo unterscheidet sich SDN von klassischen Netzwerkarchitekturen? OpenFlow, Netzwerkvirtualisierung und weitere Ansätze; Ciscos Sonderweg: ACI und QoS im RZ
- Cloud Computing: Cloud Konzepte: Private, Public oder Hybrid? Was leistet die Cloud heute, welche Anforderungen entstehen bei der Anbindung? Software as a Service: Warum Cloud-Anwendungen anders sind. Hinter den Kulissen: Typische Cloud-Anwendungen im Praxistest

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

11:00 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, der 06.12.16 - Netzwerk-Technologien: Aktuelle Entwicklungen

9:00 - 10:30 Uhr

Das Internet of Things: Wo stehen wir?

Mehr und mehr Produkte drängen in den Markt. Daraus leitet sich die Frage ab, welche Anforderungen an Infrastrukturen hier auf uns zukommen. Dieser Vortrag zeigt, wo wir stehen und was auf uns zukommt.

Sie lernen in diesem Themenblock:
- Was ist IoT?
- Anwendungsbereiche und Einsatzszenarien
- Infrastrukturen • Roadmap

10:45 - 12:30 Uhr

SDN und NFV in der Analyse
- Wo steht der Markt?
- Was ist NFV und wo setzen wir es wann ein?
- Welchen Stellenwert hat Hardware in den neuen Technologien?
- Wie hängen SDN und NFV zusammen?

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

14:00 - 15:30 Uhr

Netzwerk-Design-Lösungen im direkten Vergleich

Wir haben im Moment wesentliche Design-Entwicklungen, die sich direkt widersprechen. Gleichzeitig sind einige der neuen Ansätze auch sehr komplex. Hier stellt sich die Frage, wie man mit möglichst wenig Aufwand ein maximal gutes Design erreichen kann.

Wir diskutieren mit Ihnen:
- Layer 2 Design
- Layer 3/4 Design
- Sonderfälle
- Empfehlungen

Markus Geller, ComConsult Research GmbH

15:45 - 17:00 Uhr

VMware NSX: Zukunft oder Irrweg?

Immer mehr der traditionellen Anbieter integrieren NSX in ihre Lösungen, zum Teil sogar strategisch und ohne wirkliche Alternative. Cisco grenzt sich dabei klar durch einen eigenen Weg ab.

Wir analysieren:
- Was ist der Bedarf?
- Wie nutzbar ist NSX wirklich?
- Sind die vorhandenen Alternativen besser?
- Gibt es einen mindestens gleichwertigen herstellerneutralen Weg?

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 15:45 Uhr Kaffeepause

Mittwoch, der 07.12.16 - UC, das Ende von ISDN: Wie sieht die Kommunikationslösung der Zukunft aus?

9:00 - 17:00 Uhr

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons. Gleichzeitig ist ISDN am Ende, es wird 2017 abgeschaltet. Dies erfordert eine Neubestimmung des Verständnisses von Kommunikation: Was gehört dazu, wie kommunizieren wir in Zukunft?

Wir analysieren für Sie:
- Motivation: Warum All-IP? Einführung in das Thema
- SIP Trunking vs. PSTN: Was sind die wesentlichen Unterschiede?
- Standards für Enterprise- und Provider-Peering
- Session Border Controller: Funktionalität und Markt
- Provider-Marktübersicht: Geschäftsmodelle und Angebote
- Was kommt nach 2018?
- Architektur einer globalen All-IP Kommunikation

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN
Markus Geller, ComConult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Programmübersicht Winterschule 2016

Donnerstag, der 08.12.16 - Sicherheit / Underlay - Overlay-Design für RZ-Netze

9:00 - 12:30 Uhr

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume, sondern um Informationssicherheit als integraler Bestandteil der IT-Architektur.

Wir analysieren für Sie:

- Abwehr zielgerichteter Angriffe: Notwendigkeit system- und anwendungsübergreifender Strategien
- Netzbasierende Sicherheit: Praxiserfahrungen aus den Bereichen Verschlüsselung, Zonenkonzepte, NAC und Testumgebungen
- Sicheres Cloud Computing und sicheres Mobile Computing: Möglichkeiten und Grenzen
- Sicherheit und UC: Immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:00 - 17:00 Uhr

Viele Rechenzentren bestehen noch aus einer Mischung von **Underlay und Overlay**. Sowohl physische als auch virtuelle Server müssen in solchen RZs angebunden werden. Nachdem einige Standardisierungsansätze wie SPB und TRILL gescheitert sind und es lange Zeit danach aussah, dass proprietäre Fabrics die einzige Lösung sind, zeichnet sich unerwartet ein neuer gemeinsamer Nenner zwischen den Herstellern ab.

Wir analysieren für Sie:

- Underlay Design
- VXLAN als De-facto-Standard für Overlay Data Plane
- Overlay Control Plane: Varianten
- BGP als De-facto-Standard für Overlay Control Plane
- Teufel im Detail: redundante Anbindung von Servern

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Freitag, der 09.12.16 - WLAN und Mobilfunk

Der funkbasierten Kommunikation gehört die Zukunft. Sie wird die kabelgebundene Alternative nicht verdrängen, aber die Zahl der kabellosen Endgeräte wird deutlich überwiegen. Dies betrifft den Bereich innerhalb der Unternehmen ebenso wie die Kommunikation außerhalb. Tatsächlich wird die jetzige klare Trennung zwischen Mobilfunk und WLAN in den nächsten 5 Jahren abgelöst werden durch einen mehr integrierten Ansatz, in dem ein Endgeräte den jeweils optimalen Zugang dynamisch wählt. In Konsequenz benötigen wir Infrastrukturen, die sowohl der Anzahl als auch den qualitativen Anforderungen mobiler Teilnehmer gewachsen sind. Und tatsächlich ermöglicht die neueste Generation von Produkten Lösungen, die so noch vor wenigen Monaten nicht möglich waren.

9:00 - 12:30 Uhr

Enterprise WLANs und ihre technologischen Grenzen

- Das Medienzugangsverfahren DCF: Ist es für eine immer größer werdende Anzahl von Teilnehmern pro Zelle geeignet oder laufen wir in ein Problem?
- Schneller, näher, höher: Wie sich WLAN-Technik in Richtung 10 Gigabit entwickelt
- MU-MIMO in der Analyse: Ist dies der Schlüssel zu höherer Performance in der Zelle?
- Wie profitieren Enterprise WLANs von den neuen Technologien?
- Wie sieht der Bedarf konkret aus, brauchen wir Multi-Gigabit und ist diese Entwicklung wirtschaftlich?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:00 - 16:00 Uhr

Analyse der neuesten Entwicklungen

- Explosives Wachstum in allen Anforderungsbereichen
- Echte Multi-Gigabit WLANs mit IEEE 802.11ad
- Die nächsten WiFi-Generationen 11ax und 11ay
- Die Entwicklung von LTE
- Problematik von LTE in lizenzfreien Bereichen
- Kommt schneller als man denkt: 5G Mobilfunk
- Anforderungen an unterstützende Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

Anmeldung an kundenservice@comconsult-research.de

Winterschule 2016

Ich buche das Seminar
ComConsult Winterschule 2016

☐ 05.12. - 09.12.2016 in Aachen
zum Preis von 2.490,-- € netto

☐ Bitte reservieren Sie mir ein Hotelzimmer

vom_____ bis _____16

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Zweitthema

Internet-DMZ in der Cloud

Fortsetzung von Seite 1

Dr. Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Math. Simon Oberem ist als Berater bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft befasst er sich maßgeblich mit den Aspekten von ISMS nach ISO 27001, auch auf Basis BSI-Grundschutz sowie deren praxistauglicher Umsetzung.

Dieser bewährte Aufbau beginnt sich nun signifikant zur verändern. Zum einen machen Virtualisierung und RZ-Automatisierung auch vor Internet-DMZs nicht halt. Dies ist speziell im der Bereich von Web-Anwendungen und Web-Services der Fall. Zum anderen ist es vom Hosting der Internet-DMZs samt externer Firewall in einem Provider-RZ zu einer Private Cloud bei einem Cloud Provider nicht weit.

2. Cloud Computing und Informationssicherheit

Cloud Computing umfasst als Oberbegriff gemäß einer Definition des BSI (siehe BSI Cloud Computing Eckpunktepapier) „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.“ Die Dienstleistungen umfassen dabei neben Infrastructure as a Service (IaaS), Platform as a Service (PaaS) insbesondere auch Software as a Service (SaaS).

Im Rahmen des Cloud Computing haben sich außerdem unterschiedliche Betreibermodelle etabliert:

- Public Cloud: Hier werden durch einen entsprechenden Anbieter über das Internet Cloud-Ressourcen und Dienste der Allgemeinheit zur Verfügung gestellt.
- Private Cloud: Hierbei wird die Cloud-Infrastruktur dezidiert für eine Organisation betrieben. Sie kann von der Organisation selbst oder einem Dritten organisiert und geführt werden und kann dabei im RZ der eigenen Organisation oder eines Cloud-Dienstleisters stehen.
- Virtual Private Cloud: In einer Public Cloud kann auf Basis der gemeinsam genutzten Infrastruktur mit den Mitteln der Mandantentrennung einem Kunden eine dedizierte virtuelle Landschaft bereitgestellt werden.
- Hybrid Cloud: Diese Cloud-Infrastruktur ist eine Zusammensetzung aus verschiedenen Cloud-Infrastrukturen (Public Cloud oder Private Cloud), die jeweils für sich eigenständig sind und deren Daten bzw. Anwendungen über standardisierte oder proprietäre Technologien gekoppelt werden.

Ein fundamentales Problem des Cloud Computing liegt damit auf der Hand. Außer bei einer Private Cloud im eigenen RZ gilt: Daten verlassen die Institution und neben der Absicherung der Daten beim Transport ist die Kernfrage, wie die Daten beim Cloud Provider abgesichert werden.

Aus dem Blickwinkel der Informationssicherheit handelt es sich beim Cloud Computing tatsächlich zunächst um eine spezielle Form des Outsourcings, d.h. wesentliche Sicherheitsmaßnahmen, wie z.B. Vorgaben an die Verschlüsselung von Daten, können nur noch vertraglich geregelt werden. Die Informationssicherheit und der Datenschutz finden je nach Service-Model (IaaS, PaaS oder SaaS) in einem erheblichen Umfang beim Cloud Provider statt. Im Extremfall ist bei SaaS für die nachhaltige und nachweisliche Absicherung von Anwendungen, Plattformen und Infrastruktur der Cloud Provider zuständig und der Cloud-Nutzer muss sich „nur“ noch um die sichere Nutzung der Cloud-Anwendungen kümmern.

Für die sichere Nutzung und den sicheren Betrieb von Clouds gibt es inzwischen spezifische Anforderungskataloge aus unterschiedlichen Quellen, z.B.:

- NIST, „Guidelines on Security and Privacy in Public Cloud Computing”, 2011
- ISO 27017, “Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, 2015
- BSI, „Anforderungskatalog Cloud Computing - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“, Februar 2016

Außerdem gibt es auch Möglichkeiten, dass ein Cloud-Provider durch ein spezifisches Zertifikat einen Qualitätsnachweis für die Informationssicherheit liefert (z.B. neben einer generischen Zertifizierung nach ISO 27001 auch eine Cloud-spezifische Zertifizierung nach ISO 27017, nach EuroCloud oder nach der Cloud Security Alliance).

Internet-DMZ in der Cloud

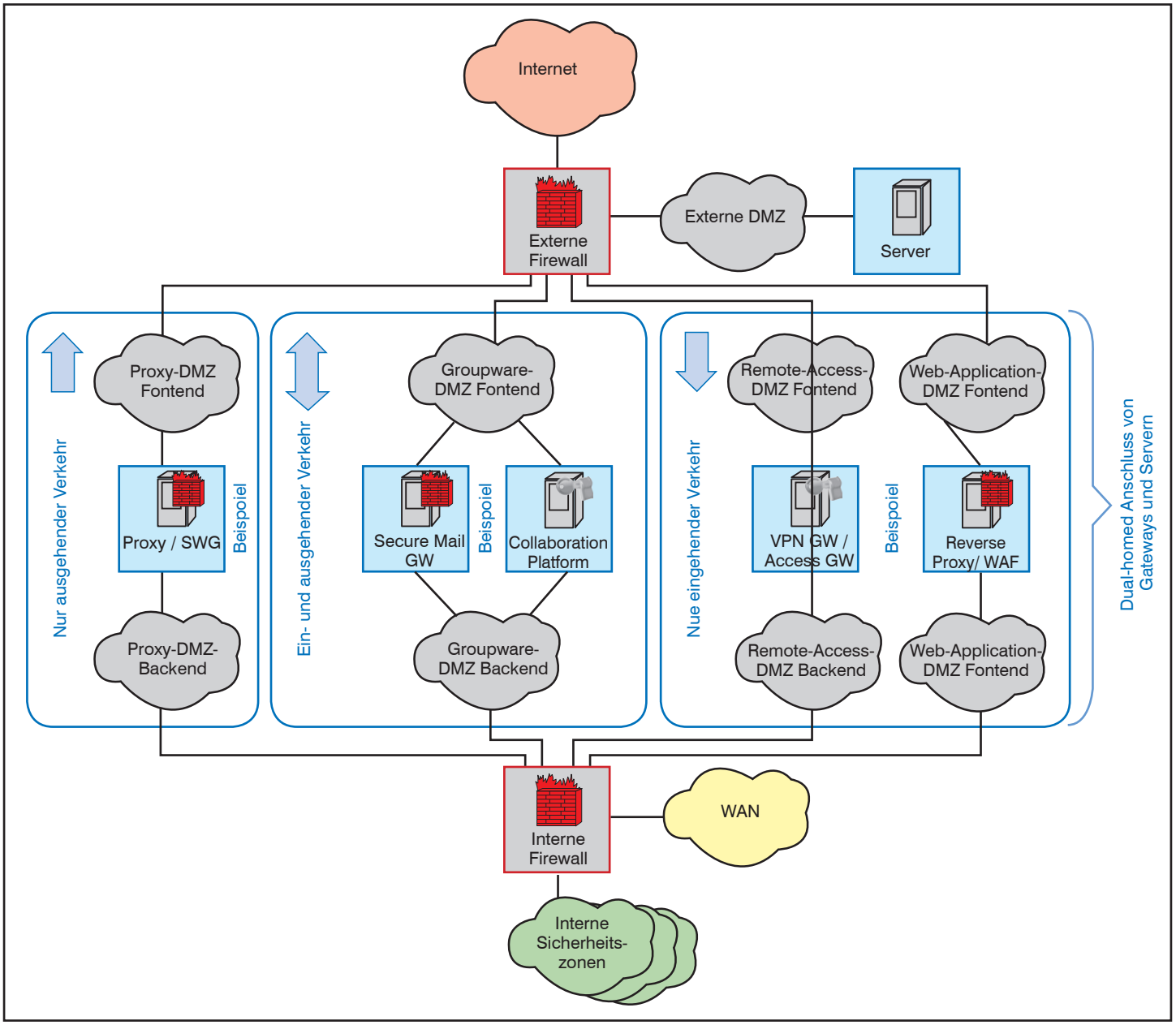

Abbildung 1: Beispiel einer zweistufigen Firewall-Architektur für den Internet-Zugang mit DMZ-Bereich

3. Notwendigkeit von Sicherheitskomponenten in der Cloud

Werden Anwendungen bzw. Anwendungskomponenten in die Cloud verlagert, müssen sich die Maßnahmen der Informationssicherheit automatisch ebenfalls auf die Cloud erstrecken.

Nehmen wir beispielsweise an, dass eine Web-Anwendung in einer Cloud auf Basis von PaaS realisiert werden soll. Der Cloud Provider betreibt die Plattform bestehend aus Web-Servern, Web-Anwendungsservern und Datenbankservern. Hinzu kommen Load Balancer, die ebenfalls Plattformbestandteil sind. Auf diese Plattform wird die Web-Anwendung, inklusive Anwendungs-Code und Datenbankschema auf der Plattform durch den Nutzer über einen gesicherten Kommunikationskanal geladen und eine sichere Mandantentrennung sorgt dafür, dass die Bestandteile der Web-Anwendung und die zugehörigen Daten vor den anderen Nutzern der Systeme geschützt werden. Bei einer 3-Tier-Webanwendung liegt oft vor jedem Tier eine Firewall (ggf. ergänzt um Intrusion-Prevention-Funktionen), welche die Kommunikation filtert. Diese Firewalls müssten dann idealerweise Bestandteil der Gesamtplattform beim Cloud Provider sein. Ähnliches gilt für den Einsatz einer WAF. Für eine Web-Anwendung sind meist auch Authentisierungsdienste erforderlich und selbstverständlich müssen Daten nicht nur beim Transport, sondern auch bei der Ablage geschützt werden. Als Folge ist PaaS ohne Security as a Service in vielen Fällen nur schwer denkbar.

Automatisierung ist ein wesentlicher Kernbestandteil der Cloud-Idee (und moderner Rechenzentren). Die physikalische Infrastruktur muss hierzu von Diensten, Applikationen und damit den logischen Strukturen so weit entkoppelt werden, dass die Einrichtung (das „Provisioning“) von Diensten und Applikationen in der Regel ausschließlich auf der logischen Ebene erfolgt. Dies bedeutet konsequente Virtualisierung auf allen Ebenen der Infrastruktur. Hierzu wird mit Overlay-Techniken gearbeitet, die von der zugrundeliegenden

physischen Netzinfrastruktur durch Tunnelmechanismen abstrahieren und auf Ebene des Hypervisor logische Netzstrukturen für VMs bereitstellen.

Firewalls müssen hier entsprechende Schnittstellen zum Hypervisor haben bzw. (zumindest zu Teilen) Bestandteil des Hypervisor werden, um an den Tunnelendpunkten der Overlay-Struktur den eigentlichen Verkehr filtern zu können. Ein populäres Beispiel ist die VMware NSX Distributed Firewall (DFW), die Bestandteil der VMware NSX Network Virtualization Platform ist. Solche Konzepte sind wichtige Kernelemente eines Software-defined Data Center (SDDC), das seinerseits eine wesentliche Basis für Dienste gleichermaßen in der Private Cloud als auch in der Public Cloud ist.

Unabhängig von dem Trend, Anwendungen aus der Cloud heraus zu beziehen, erfordert die Komplexität der aktuellen Bedrohungslage eine erhebliche Intelligenz und Rechenleistung in Sicherheitskomponenten, die praktisch nur noch über Cloud-Dienste geliefert werden kann. Die notwendige Intelligenz von diversen Security-Lösungen kann nämlich nicht mehr vollständig lokal gehalten werden, sondern muss kontinuierlich über eine Verbindung zur zentralen Infrastruktur eines Herstellers bzw. Dienstleisters aktualisiert, nachgeladen oder bereitgestellt werden. Im Extremfall sind die lokalen Sicherheitskomponenten nur noch „dumme“ Probes und die eigentliche Intelligenz, die Daten analysiert (z.B. hinsichtlich Anomalien, die vielleicht auf einen zielgerichteten Angriff hindeuten), sitzt irgendwo in der Cloud außerhalb der eigenen Infrastruktur.

Zusammengenommen bedeutet dies: Security as a Service ist nicht nur eine Konsequenz aus dem Cloud-Computing-Trend, sondern auch eine unmittelbare Reaktion auf die aktuelle Bedrohungslage. Security as a Service wird alle Bereiche des Cloud Computing von Infrastructure as a Service (IaaS) bis Software as a Service (SaaS), von der Private Cloud bis zur Public Cloud durchdingen und muss integraler Bestandteil des Cloud Computing werden. Dies gilt insbesondere für den Bereich der Internet-Anbindung inklusive aller über das Internet bereitgestellter Dienste.

4. Komponenten einer Cloud-basierten Internet-DMZ

Im Folgenden werden typische DMZ-Komponenten betrachtet, die inzwischen als Cloud Service angeboten werden.

Server

Von den bereits genannten Webauftritten abgesehen, sind immer mehr interne Anwendungen und Services entweder aus dem Internet erreichbar oder bedürfen der Internetkonnektivität um den jeweiligen Dienst vollumfänglich zu leisten. Daher besteht bei vielen Anbietern mittlerweile die Möglichkeit die notwendigen „Schnittstellen-Dienste“, also die Dienste, die man klassischerweise in einer Internet-DMZ abbildet, direkt in der Cloud zu realisieren. Ein Beispiel hierfür wäre in der Microsoft Exchange-Landschaft der Edge Transport Server, der im SaaS-Angebot Office 365 direkt in die Cloud integriert ist.

Aber auch einfach nur das bedarfsweise Hinzuschalten und Parallelisieren von Rechenkapazität durch z.B. eine entsprechende Menge von Applikationsservern wird bei Cloud-Anbietern meist heftig beworben. Das Problem an dem letzteren Einsatzzweck ist allerdings die Anbindung an die Cloud. Denn wenn die zu verarbeitenden Daten nicht schon in der Cloud sind, müssen sie erst einmal einen sicheren Weg dorthin finden und in der Cloud sicher verarbeitet werden.

Secure Web Gateways

Eine klassische Internet-DMZ-Komponente, die inzwischen recht häufig in der Cloud anzutreffen ist, ist das Secure Web Gateway (SWG), d.h. ein um Sicherheitsfunktionen angereicherter Forward-Proxy. Marktstudien zeigen, dass Anbieter einer On-Premises-Lösung inzwischen stark von reinen Cloud-Lösungen und Hybrid-Lösungen in Bedrängnis geraten (siehe z.B. Gartner „Magic Quadrant for Secure Web Gateways“ vom Juni 2016). Das gilt auch für die vormals so etablierten Produkte, wie die von Cisco (WSA / vorher Ironport) und McAfee / Intel (Web Gateway). So hat es Zscaler an allen vorbei innerhalb weniger Jahre geschafft, eine erhebliche Marktpräsenz und Reputation aufzubauen und auch die SWGs von Blue Coat konnten mit ihren Hybrid-Lösungen Marktanteile gewinnen.

Der Unterschied zwischen einem SWG in der Cloud und einer On-Premises-Lösung liegt nun in interessanten Details:

Ein Internetnutzer ruft z.B. eine bestimmte Seite auf. In der On-Premises-Welt weiß der Browser in der Regel über ein PAC-File, dass er zunächst zum SWG muss, wo verschiedenste Sicherheitsfunktionen abgebildet werden und dann die Verbindung zum gewünschten Webserver aufgebaut wird. Wenn sich der Internetnutzer aber jetzt in einem angebundenen Partnerstandort befindet oder mit einen Laptop auf Dienstreise ist, so muss zunächst ein sicherer Weg bis in das RZ zurückgelegt werden, wo sich das SWG befindet. Nur so können alle gewünschten Sicherheitsfunktionen durchgängig abgebildet werden. Und eben dieser Weg ist meist kein günstiger. In einem Fall kostet es z.B. teure WAN-Bandbreite und im anderen Fall muss man wiederum auf eine VPN-Infrastruktur zurückgreifen.

Wenn man hingegen ein Cloud-basiertes SWG nutzt, wird der Verkehr über einen zu spezifizierenden Mechanismus zum nächstgelegenen SWG (bzw. Cloud-Knotenpunkt) des Cloud-Providers geleitet, hier werden die konfigurierten Sicherheitsfunktionen abgebildet und von dort aus wird die Verbindung zum Webserver aufgebaut (siehe Abbildung 2). Das heißt, bei der Auswahl eines Providers für Cloud-SWGs kommt es neben der funktionalen Fähigkeit auf eine weltweit verteilte Marktpräsenz an, damit die Wege zwischen Nutzer, SWG und aufgerufener Webseite möglichst kurz (also schnell) sind. Au-

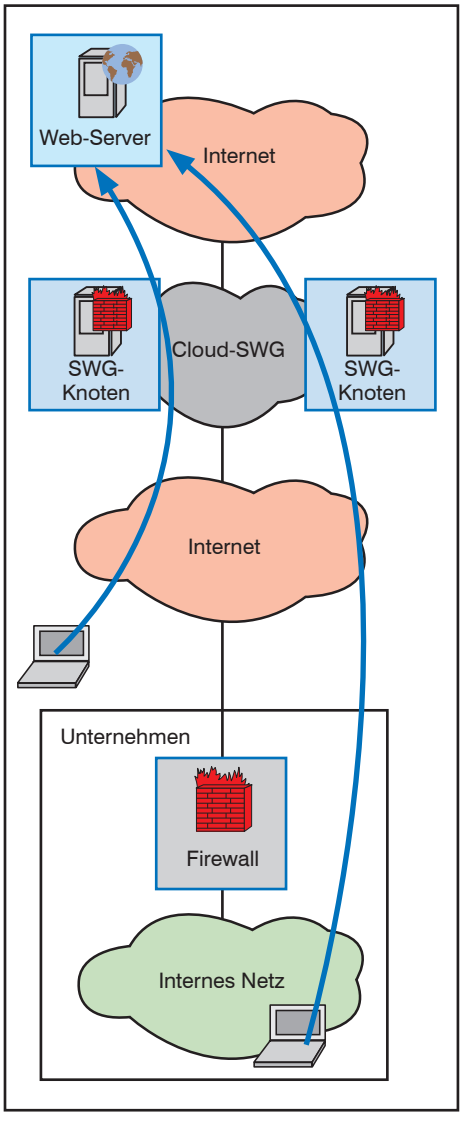

Abbildung 2: Secure Web Gateway in der Cloud

ßerdem muss der vom Provider gewählte Mechanismus zum Auffinden des nächstgelegenen Rechenpunktes unterstützt werden, was eine weitere Anforderung an die Cloud-Anbindung stellt, die später beleuchtet werden soll.

Schutz vor Schadsoftware

Nun zu einem Punkt, der eng mit SWGs zusammenhängt, da beides häufig in einer Komponente realisiert wird, dem Schutz vor Schadsoftware. Unter diesem Begriff sollen an dieser Stelle alle Funktionen zusammengefasst werden, die sich von Anti-Virus über Threat Protection bis hin zu Abwehr vor Advanced Persistent Threats (APTs) nennen lassen. Das Prinzip ist zwar in großen Teilen immer ähnlich: Auf der Basis von Signaturen und / oder statistischen Methoden soll der Netzwerkverkehr (hier Internetverkehr) auf Schadprogramme und Angriffsmuster untersucht werden. Für diesen Zweck werden von verschiedenen Sensoren (zum Beispiel einem SWG) Informationen gesammelt und ausgewertet.

Damit insbesondere anwendungs- und systemübergreifende Angriffe besser erkannt werden können, sind umfangreiche Daten erforderlich und es kommen in 2nd Generation SIEM (Security Information and Event Management) auch Big-Data-Analysetechniken zum Einsatz. Da die Verarbeitung von großen Datenmengen auch immer mit einer entsprechenden Rechenlast verknüpft ist, wird hier oft die Realisierung über eine Hersteller-eigene Cloud angeboten. So müssen die lokalen Systeme nicht überdimensioniert und teuer werden, sondern die Rechenlast kann kundenspezifisch und bedarfsgerecht in der Cloud geleistet werden.

Sandboxing

Viele Angriffe (inklusive APTs) basieren in einem ersten Schritt darauf, dass der Nutzer einen bösartigen Link (z.B. in einer E-Mail) anklickt, über den eine schadenstiftende Software auf den Client heruntergeladen und ausgeführt wird. Die Idee ist nun einfach: Statt die Software im Browser des Client auszuführen, erfolgt dies zunächst in einer isolierten zentralen Umgebung (Sandbox) und das Verhalten der Software wird genau beobachtet. Erst wenn die Software als unbedenklich eingestuft wurde, wird sie auch auf dem Client ausgeführt. In On-Premises-Lösungen ist es hier häufig notwendig, die entsprechend zu untersuchenden Dateien zu dem Anbieter der Sandboxing-Lösung hochzuladen. Wenn die Dateien allerdings bereits in einer Security Cloud als verdächtig erkannt werden, wäre ein zusätzlicher Datei-Upload nicht mehr nötig und es hätte den weiteren Vorteil das potentielle Schadsoftware gar nicht erst in das Netz des Unternehmens kommt.

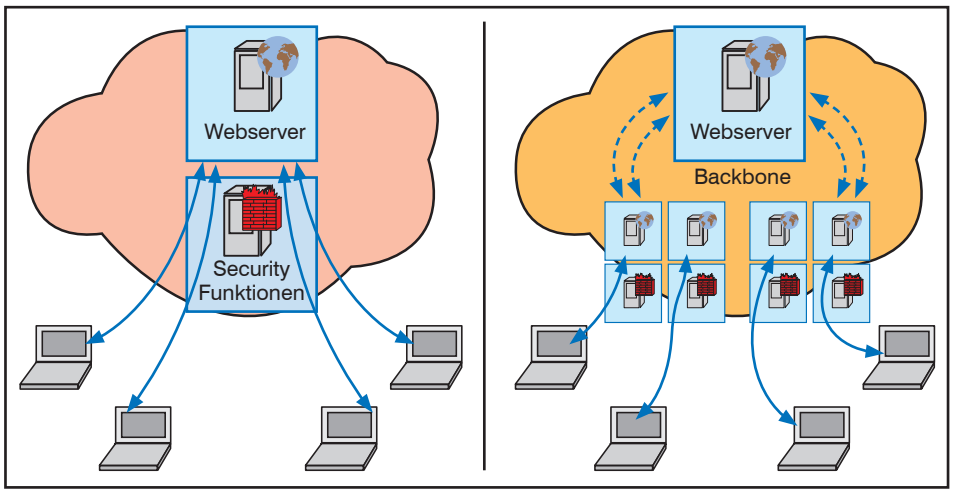

Abbildung 3: Verteilte Bereitstellung von Content und Security durch CDNs

Sandboxes sind in unterschiedlichen Varianten auf dem Markt verfügbar, z.B. als dedizierte Sandbox-Lösung (z.B. FireEye), als Firewall-Komponente (z.B. Check Point Software, Palo Alto Networks, Fortinet) als Bestandteil eines SWG (z.B. Blue Coat, Zscaler) oder eines Secure E-Mail Gateway (SEG) wie z.B. bei Proofpoint.

Reverse Proxys, WAFs und Load Balancer

Die Realisierung von Reverse Proxys in der Cloud ergibt neben dem Schutz vor Schadsoftware spätestens dann Sinn, wenn man auch die eigenen Webserver in der Cloud betreibt. Wäre der Reverse-Proxy lokal und die Webserver in einer Cloud, würde der Traffic zweimal über die eigene Leitung gehen und so die ohnehin schon immer größer werdende benötigte Bandbreite unnötig nach oben schrauben. Da aber der Schritt von einem Reverse Proxy mit Anti-Virus-Funktion und zentralem (Cloud-)Management nicht mehr weit ist zu einer Web Application Firewall (WAF) und einhergehendem Load Balancing, sind es oft eben Hersteller aus diesen Bereichen, die hier eine Gesamtlösung zur Verfügung stellen. Zu nennen sind neben Akamai, Citrix, CloudFlare, F5, Incapsula (zuvor Imperva) und verschiedenen kleineren Anbietern auch die großen drei Cloud-Provider (Amazon Web Services, Google Cloud und Microsoft Azure). All diese stellen nämlich zwei weitere Dienste/Komponenten für die Internet-DMZ in der Cloud bereit. Zum einen ist das die Bereitstellung eines Content Delivery Network (CDN) und zum anderen ist das die Abwehr von Distributed Denial of Service (DDoS) Attacken.

Content Delivery Network (CDN)

Das Konzept von CDNs folgt in etwa dem Konzept des Zugriffs auf ein Cloud-SWG. Zunächst wird dafür gesorgt, dass ein über das Internet erreichbarer Dienst zur Optimierung der Zugriffszeiten und zur Leistungssteigerung auf der Welt verteilt durch verschiedene Systeme abgebildet wird und erreichbar ist. Die dazugehörigen Systeme müssen dann über ein Backbone-Netzwerk miteinander verbunden sein. Wenn ein Nutzer irgendwo auf der Welt versucht diesen Dienst, bzw. den dazugehörigen Webserver, zu erreichen, sorgt ein Mechanismus (vergleichbar mit dem Routing von Load-Balancern) dafür, dass der nächstgelegene CDN-Knotenpunkt die Nutzeranfrage bearbeitet (siehe Abbildung 3). Wieviel Intelligenz nun in einem einzelnen CDN-Knoten steckt, unterscheidet sich je nach Anwendungszweck, zum Beispiel könnte nur das Web-Frontend über ein CDN abgebildet werden und die CDN-Knoten greifen auf zentrale Systeme zurück.

Abwehr von Distributed Denial of Service (DDoS)

Die DDoS-Abwehr und die Notwendigkeit dies als Komponente in der Cloud anzusehen wurde bereits in der Oktober-Ausgabe des Netzwerk Insider besprochen. Kernelemente der DDoS-Abwehr sind:

- Umleitung des Verkehrs zu sogenannten Scrubbing-Centern in der Cloud per DNS-Redirect oder BGP, die den DDoS-Verkehr herausfiltern
- Zusätzliche Abwehr von DDoS auf Anwendungsebene z.B. durch ein Intrusion-Prevention-System (IPS) oder in der (Virtual) Private Cloud oder Public Cloud

Internet-DMZ in der Cloud

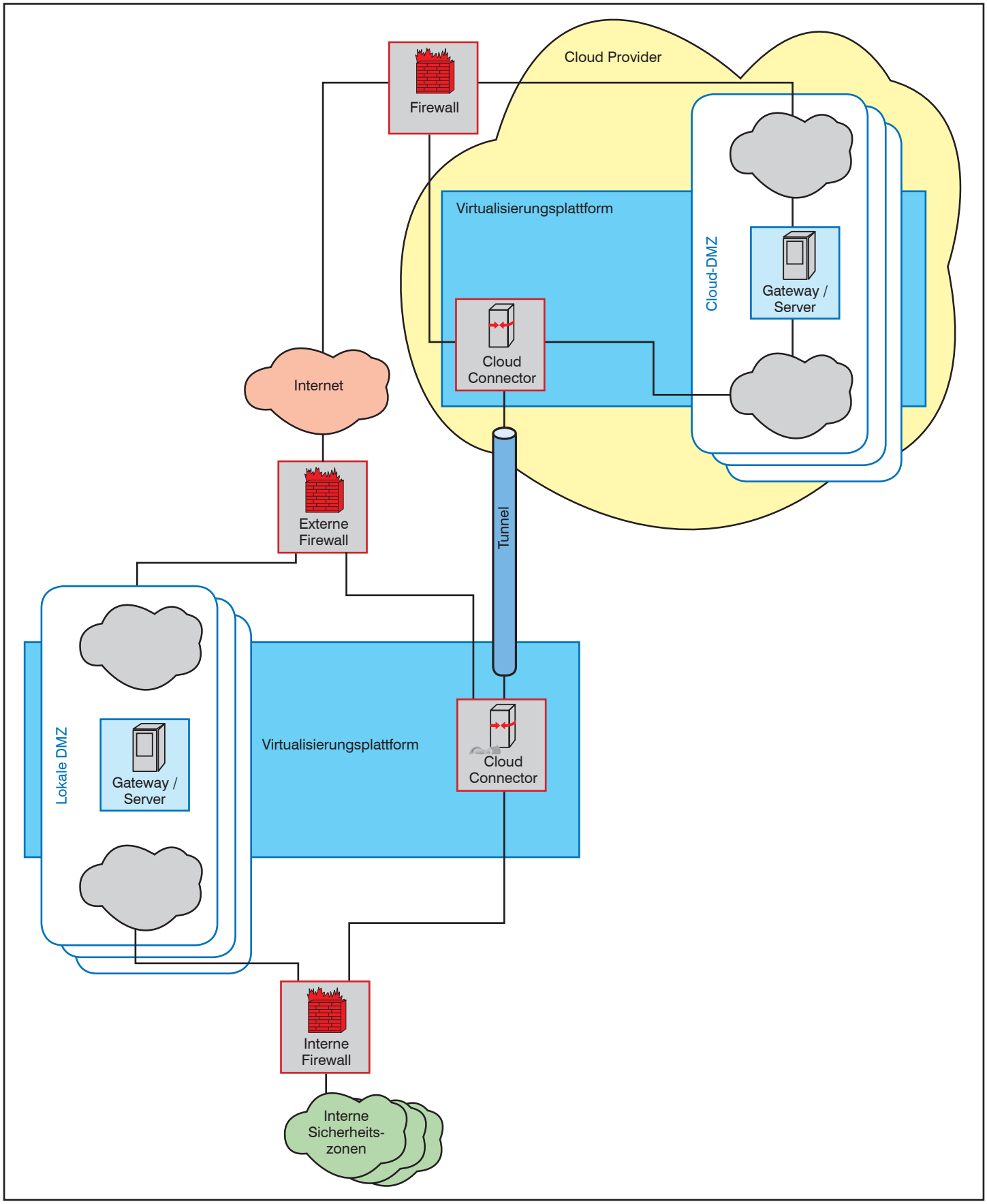

Abbildung 4: Anbindung zwischen eigenem RZ und eines DMZ-Bereichs in der Cloud

Auch CDNs können durch ihre Natur der Lastverteilung einen Beitrag zur (D)DoS-Abwehr auf Ebene der Anwendungen liefern. Auch hier wird über DNS-Redirect oder über BGP der Verkehr an einen Ort in der Cloud geleitet, wird dort mit Lastverteilungsmechanismen auf mehrere Systeme verteilt und darüber hinaus von einer Firewall bzw. einem IPS gefiltert. Es ist daher nicht verwunderlich, dass sich unter den Anbietern von CDNs oft die gleichen Namen finden, wie unter den Anbietern von DDoS-Abwehr-Dienstleistungen.

SSL-Terminierung

Die Analyse des Kommunikationsverkehrs auf Ebene der Anwendungen durch eine Firewall, ein IPS oder eine WAF erfordert, dass vor oder in der jeweiligen Komponente die SSL/TLS-Verschlüsselung, die zum Schutz der Übertragung eingesetzt worden ist, terminiert oder aufgebrochen wird. Die hierzu notwendigen Zertifikate müssen auch in einer klassischen DMZ - soweit möglich - auf die Komponente geladen werden, die die Entschlüsselung und ggf. Wiederverschlüsselung durchführt. Typisches Beispiel ist die SSL-Terminierung in einem Load Balancer oder einer WAF. Dieses Prinzip gilt natürlich grundsätzlich auch für die Internet-DMZ in der Cloud. Hier ist es aber nun so, dass sich größere Dienste-Anbieter alternativ mit einer Zertifizierungsstelle zusammengetan haben. Mit Erlaubnis des Kunden, stellt die Zertifizierungsstelle auch dem Dienste-Anbieter die passenden Zertifikate aus. Das hierzu notwendige Vertrauen in den Dienste-Anbieter muss natürlich gegeben sein!

E-Mail-Gateways

Nun zu einer Internet-DMZ-Komponente, die als Cloud-Komponente scheinbar nur einen kleinen Markt bietet, den E-Mail-Gateways. Bei vielen Institutionen sind die Sicherheitsbedenken, wenn es um E-Mails geht, viel größer als in anderen Bereichen. Andererseits ist der Funktionsumfang, den E-Mail-Gateways abbilden, mit SWGs zu vergleichen. Man untersucht auf Zulässigkeit des Verkehrs und führt Viren-Scanning und gegebenenfalls Sandboxing durch. Allerdings spielt hier sicherlich die immer weiter fortschreitende Homogenisierung der genutzten E-Mail-Plattformen eine Rolle. Das beinahe schon Monopol von Microsoft Exchange hat auch Auswirkungen im Bereich E-Mail-Gateways. Denn je mehr Sicherheitsfunktionen von Microsofts E-Mail-Gateway Exchange Online Protection (EOP), was jetzt schon integraler Bestandteil von Office 365 ist, auch in native Exchange-Server integriert werden, umso weniger Funktionen werden künftig von E-Mail-Gateways verlangt. Ausgenommen werden hierbei wahrscheinlich das korrekte Routing, das etwaige Abtrennen von Anhängen, das Verschieben in Benutzer-Quarantänen und die Verschlüsselung von E-Mails sein.

5. Cloud-Anbindung

Wenn als IaaS Teile oder sogar die vollständige der Internet-DMZ in einer Virtual Private Cloud realisiert ist, könnten z.B. für die Anbindung des eigenen RZs Overlay-Techniken angewendet werden, die dann mit Produkten wie Cisco InterCloud Fabric oder VMware NSX das eigene Netz transparent auf die Cloud erweitern (siehe Abbildung 4).

Werden spezifische DMZ-Komponenten als Managed Service in einer Provider Cloud realisiert, liegen im Detail interessante Probleme bei der Cloud-Anbindung. Im Folgenden wird dies exemplarisch anhand der Anbindung eines Cloud-SWG dargestellt.

Forwarding

Angenommen ein Endpunkt (z.B. ein Browser eines Laptops) ruft die Seite „www.comconsult.com“ auf. Damit die Anfrage das Cloud-SWG erreicht, gibt es drei Möglichkeiten:

Der Browser weiß per PAC-File (das er i.d.R. über das Active Directory bezieht) und DNS-Auflösung die IP-Adresse des Cloud-Proxies und auf diese Weise wird das Forwarding gesteuert. Allerdings gibt es hier direkt zwei Probleme. Einerseits ist es hier entscheidend, wo die PAC-Files bereitgestellt werden. Wenn diese in der Cloud angeboten werden sollen, muss der Client in der Lage sein, direkt die Cloud anzusprechen. Dies kann entweder über eine Default-Route in Richtung Internet ermöglicht werden (was nicht immer gewollt ist) oder über eine der anderen Anbindungsvarianten, die gleich beschrieben werden. Außerdem werden durch die externe PAC-File-Bereitstellung weitere interne Informationen über Anwendungen und Infrastruktur in der Cloud gespeichert. Wenn es nur einen internen PAC-File-Server gibt, müssen Nutzer, die sich nicht im Unternehmensnetz befinden, zunächst eine Verbindung ins interne Netz haben, um den PAC-File-Server zu erreichen und so eine Weiterleitung zum Cloud Proxy geschieht. Ein weiteres Problem kann die DNS-Auflösung sein. Denn im PAC-File stehen ggf. Adressen des Cloud-Proxies, die ein interner DNS nicht auflösen kann. Also muss eine solche DNS-Anfrage an einen externen DNS-Dienst weitergeleitet werden.

Die zweite Möglichkeit der Verkehrsweiterleitung ist der Aufbau eines Tunnels (i.d.R. GRE oder IPsec-VPN Tunnel) durch einen Edge-Router, bzw. eine Firewall. Auf diese Weise wäre keine Default-Route mehr in Richtung Internet (mit etwaiger Einschränkung auf Adressen der Cloud) notwendig, sondern der ausgehende Verkehr würde zunächst immer durch das Cloud-SWG als Cloud-Proxy gehen. Wenn jetzt der Cloud-Knotenpunkt ausfällt, zu dem ein Tunnel konfiguriert ist, muss man gegebenenfalls manuell dafür sorgen, dass ein Tunnel zu einem zweiten Knotenpunkt aufgebaut wird. Wenn zusätzlich vom Edge-Router NAT durchgeführt wird, dann erscheinen außerdem im Logging des Proxies keine internen Adressen, was nicht nur die Fehlersuche komplizierter macht.

Die dritte Möglichkeit der Anbindung des Cloud-SWGs ist das sogenannte Proxy-Chaining. Dabei ist ein interner Proxy so konfiguriert, dass er die gesamte Kommunikation zu einem Cloud-Knotenpunkt weiterleitet. So entstehen Kosten und Betriebsaufwände von zwei Proxy-Systemen. Darüber hinaus müssten Nutzer außerhalb des eigenen Netzwerkes per separatem PAC-File in die Cloud weitergeleitet werden, was wieder neue Unwägbarkeiten mit sich bringt.

Authentisierung

Bei einem Cloud-SWG ist es notwendig, dass Anfragen authentisiert werden, damit überhaupt festgestellt werden kann, ob die angeforderte Kommunikation erlaubt wird oder nicht. Eine Nutzer-Authentisierung kann wie bei jedem beliebigen anderen Dienst mit lokalen Nutzern - hier mit einem Nutzerverzeichnis in der Cloud - erfolgen. Auf eine ähnliche Art und Weise, dem LDAP BIND, können auch bestehende Nutzerverzeichnisse mit der Cloud-Verzeichnis synchronisiert werden. Aus Sicherheitsperspektive sind allerdings beide Varianten nicht sinnvoll. Auch Varianten mit Einmal-Links per Mail oder Einmal-Passwörtern sind praxisfern. Der derzeit eigentlich einzig gangbare Weg für eine sichere Authentisierung mit dem Cloud-Proxy sind Hintergrunddienste wie die aus Sicherheitsgründen und aus Gründen der Verbreitung bei vielen Cloud-Providern zu empfehlende Authentisierung mittels Security Assertion Markup Language (SAML) [1].

Logging

Vom Cloud-SWG werden Nutzeraktionen protokolliert und auf Servern in einem bestimmten Land gespeichert, z.B. bei Zscaler für europäische Kunden in der Schweiz. Die hier gespeicherten Daten unterliegen daher den Schweizer Datenschutzgesetzen. Eine Speicherung nur auf eigenen Servern ist bisher bei keinem der Cloud-SWG-Provider möglich.

Vernetzung von Cloud-Diensten und Cloud-Providern

Üblicherweise lassen sich die in einem Cloud-SWG gewonnen Informationen in

vielen verschiedenen Formaten und Detailtiefen an SIEM-Systeme und andere Überwachungssysteme weiterleiten. Dabei kann natürlich durchaus ein weiterer Cloud-Dienst genutzt werden. Dies deutet auf einen anderen wichtigen Aspekt beim Cloud Computing hin: Institutionen werden nicht nur mehrere Cloud-Dienste simultan verwenden und Daten zwischen Cloud Diensten austauschen, sondern auch die Cloud-Provider werden auf Cloud-Dienste anderer Provider zurückgreifen, es entsteht ein (ggf. sehr dynamisches) Netzwerk von Cloud-Diensten unterschiedlicher Provider. Hierzu ist eine entsprechende Standarisierung, die auch die Informationssicherheit und den Datenschutz angemessen berücksichtigt, zwingend erforderlich. Wie eingangs bereits beschrieben, gibt es zwar verschiedene Zertifizierungsmöglichkeiten für Cloud Provider, jedoch ist man von einheitlichen und international etablierten Standards, die auch den notwendigen Detaillierungsgrad für die Schaffung einer Interoperabilität von Cloud-Diensten liefern, noch recht weit entfernt.

6. Fazit

Wir haben in diesem Artikel anhand der Internet-Anbindung gezeigt, wie heutzutage Cloud-Dienste zur Auslagerung von Diensten und Komponenten einer Internet-DMZ genutzt werden können. Beispielsweise ist PaaS für das Hosting von Web-Anwendungen und Web Services nicht mehr ungewöhnlich und durch Firewalls und WAFs in der Cloud lassen sich Umgebungen analog zur lokalen Internet-DMZ realisieren. Die besondere Stärke von Cloud-Lösungen wird dabei durch die Möglichkeiten von CDNs besonders deutlich und eine sinnvolle Abwehr von DDoS ist ohne Cloud-Dienste praktisch unmöglich. Für die Absicherung des ausgehenden Internet-Verkehrs haben sich Cloud-SWGs inzwischen so stark etabliert, dass reine On-Premises-Lösungen kaum noch Chancen haben.

Technisch hat sich Cloud Computing und insbesondere Security as a Service inzwischen mit einer höchst interessanten Produktpalette materialisiert. Dabei erlaubt insbesondere die Vernetzung von Cloud Services eine extrem schnelle und flexible Entwicklung und Bereitstellung von anspruchsvollen Diensten und ist daher besonders attraktiv. Wenn hierbei eine angemessen sichere Mandantenfähigkeit durch die Provider umgesetzt worden ist, die Daten bei Transport und Ablage angemessen geschützt sind und die Provider nachweislich nachhaltig einen sicheren Betrieb der Infrastruktur gewährleisten, gibt es auf den ersten Blick scheinbar immer weniger Bedenken. Nur fehlt es immer noch an international anerkannten Standards, die auch die Anforderungen der Informationssicherheit so berücksichtigen, dass weltweit vernetzte, interoperable und zertifizierte Trusted Cloud Services möglich sind.

7. Abkürzungen

APT	Advanced Persistent Threat
BGP	Border Gateway Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDN	Content Delivery Network
DDoS	Distributed Denial of Service
DFW	Distributed Firewall
DMZ	Demilitarized Zone
DNS	Domain Name System
EOP	Exchange Online Protection
GW	Gateway
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PAC	Proxy Auto-Configuration
RZ	Rechenzentrum
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDDC	Software-defined Data Center
SEG	Secure E-Mail Gateway
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

8. Verweise

[1] Siehe hierzu „Authentifizierung und Single Sign On in Cloud-Umgebungen“ aus „Der Netzwerk Insider“ vom Oktober 2016

ComConsult Veranstaltungskalender

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 14.11. bis 16.11.2016 in Bonn

Garantietermin

Die IT-Sicherheit für die Internet DMZ und internen Sicherheitszonen werden in diesem Seminar von Experten aus der Praxis vorgestellt und anschaulich erklärt. Verschiedene IT-Architekturen und Konzepte werden analysiert und auf ihre Praxistauglichkeit untersucht. Die Umsetzung anhand konkrete Projektbeispiele runden die Schulung ab.

Preis: € 1.890,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 14.11. bis 16.11.2016 in Bonn

Garantietermin

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: € 1.890,-- netto

Wireless LAN professionell, 14.11. bis 16.11.2016 in Bonn

Garantietermin

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, die Markt- und Produktsituation bewertet, und Empfehlungen für eine optimale Auswahl gegeben. Die für WLAN relevanten technischen Bereiche werden dabei von nachrichtentechnischen Aspekten der Funkübertragung bis hin zur Erstellung eines WLAN-Sicherheitskonzepts vertieft behandelt.

Preis: € 1.890,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 14.11. bis 18.11.2016 in Aachen

Garantietermin

Dieses Seminar vermittelt alles Wichtige, was Sie zum Thema LAN wissen müssen. Es werden unterschiedlichen Einsatzszenarien für Routing und Switching beleuchtet und das notwendige Wissen zur erfolgreichen Planung und dem Betrieb von Netzwerk Infrastrukturen vermittelt. Die Abdeckung der Themen erstreckt sich über Layer 2 Redundanzverfahren, Routing und Tunneltechnologien, sowie Netzwerkmanagement Fragen. Einen weiteren Schwerpunkt bildet das Kapitel Office Network. Hier werden der Aufbau und die Integration von WLAN Strukturen detailliert beleuchtet.

Preis: € 2.490,-- netto

Trouble Shooting für Netzwerk-Anwendungen, 15.11. bis 18.11.2016 in Aachen

Garantietermin

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzten Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.490,-- netto

Verkabelungssysteme für Lokale Netze, 28.11. - 29.11.2016 in Köln

Garantietermin

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen. Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Dabei werden die Normen diskutiert und die praktische Handhabung der Normungsvorgaben erklärt. Der 2. Tag widmet sich der konkreten Durchführung einer Planung in kleinen Übungsgruppen.

Preis: € 1.430,-- netto

Recht und Datenschutz bei Einführung von VoIP, 28.11. - 29.11.2016 in Bonn

Garantietermin

Ziel der Schulung ist es, den Teilnehmern einen Überblick über die aktuelle Situation im Bereich des Datenschutzes im Kommunikationsumfeld zu verschaffen. Datenschutz und Datensicherheit werden zunehmend wichtiger im Umgang mit Kunden und Mitarbeitern. Gerade mit der Einführung von IP basierten Lösungen in den Bereichen Telefonie oder Contact Center, stellen sich neue Herausforderungen in Bezug auf personenbezogene Informationen. Um Ihnen einen Überblick über den rechtlichen Rahmen zu geben beschäftigt sich dieses Seminar u.a. mit Fragen zur Abhörsicherheit, Vorratsdatenspeicherung, Datenverlust und den dazugehörigen Aspekten.

Preis: € 1.590,-- netto

IPv6 Grundlagen, 28.11. - 29.11.2016 in Bonn

Garantietermin

IPv6 betreiben, bedingt IPv6 verstehen. In diesem Seminar werden die Grundlagen des neuen IP Protokolles verständlich und praxisnah vermittelt. Die Schulung richtet sich gleichermaßen an Planer, Betreiber, Administratoren und Software-Entwickler.

Preis: € 1.790,-- netto

Storage: Planung moderner Speicherlandschaften, 28.11. - 29.11.2016 in Bonn

Garantietermin

Hohe Lese-/Schreibraten, niedrige Latenz, revisionssichere Bereitstellung, Skalierbarkeit, Hochverfügbarkeit und nicht zu Letzt niedrige Kosten sind nur einige der teils gegensätzlichen Anforderungen, die an Speicherlandschaften gestellt werden. Moderne Speicherprotokolle und Medien, die Konvergenz von Speicher- und Clientnetzen und die Virtualisierung von Speicher z.B. im virtuellen SAN bieten die Möglichkeit, Speicherlösungen zu entwerfen, die den individuellen Ansprüchen zentraler Rechenzentren oder von Filialen unterschiedlicher Größe und Bedeutung gerecht werden. Im Seminar werden die unterschiedlichen Technologien vorgestellt und, basierend auf einem pragmatischen Best-Practice-Ansatz, Szenarien beschrieben um das persönliche Speicher-Optimum zu erreichen.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen
09.10. - 11.10.17 in Bremen

Internetworking
14.11. - 18.11.16 in Aachen
03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
02.05. - 05.05.17 in Aachen
26.09. - 29.09.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
15.11. - 18.11.16 in Aachen
27.06. - 30.06.17 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf
16.10. - 18.10.17 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt

Umfassende Absicherung von Voice over IP und Unified Communications
28.11. - 30.11.16 in Bonn
08.05. - 10.05.17 in Frankfurt
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf
18.09. - 19.09.17 in Düsseldorf

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: kundenservice@comconsult-research.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie