ComConsult Research

Der Netzwerk Insider

Oktober 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

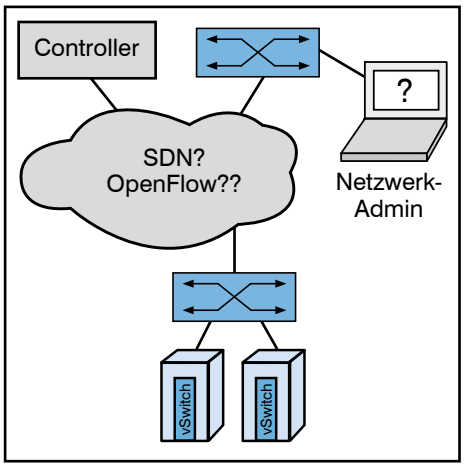
von Dipl.-Inform. Petra Borowka-Gatzweiler

SDN und OpenFlow haben sich zu einem Hype entwickelt. Ist OpenFlow eine Technik, die gekommen ist um zu bleiben? Oder wird sie in den nächsten drei Jahren wieder in der Versenkung der "da war mal was" Technologien verschwinden? Der nachfolgende Beitrag beleuchtet Motivation, Hintergründe, Treiber, Technologie und Erfolgswahrscheinlichkeit von SDN und OpenFlow.

1. Warum SDN und OpenFlow?

1.1 Aktuelle Probleme und Motivation für SDN und OpenFlow

Die Motivation für eine neue Netzwerk-Architektur, wie Software Defined Networking



und OpenFlow sie wollen, liegt in verschiedensten Problembereichen heutiger Netzwerke, die wir nachfolgend näher beleuchtet werden.

Software vs. ASICs: Begeben wir uns einmal zurück in die 70er und 80er Jahre: Damals war ein Router ein Server (typischerweise Unix), der Datenpakete zwischen zwei oder mehreren Netzwerk-Schnittstellen weiterleitete… Später begann die Entwicklung von ASICs mit ständig wachsender Leistung, Kapazität, Komplexität und hoher Funktions-Robustheit, sowie ständig sinkenden Delay-Werten für die switch-interne Paket-Bearbeitung.

weiter auf Seite 14

Zweitthema

UCC gehört ins Internet!

von Dominik Zöller

Unified Communications (& Collaboration!) gehört ins Internet – diese These dürfte so manchem Sicherheitsbeauftragten den wohlverdienten Schlaf rauben. Doch deswegen ist sie nicht weniger wahr. Nur in und mit dem Internet kann UCC seinen Mehrwert voll entfalten. Um diese These zu überprüfen, müssen wir uns zunächst dem Wesen und dem Versprechen von UCC zuwenden.

Betrachten wir zunächst den prototypischen Entstehungsprozess eines UCC-Projektes. In der Mehrzahl aller Fälle wird über eine Investition in eine neue Telefonie-Infrastruktur nachgedacht. Die Gründe sind vielfältig: Erweiterungsbedarf aufgrund von Neubauten, End-of-Life der bestehenden Lösung, Unsicherheit bezüglich der wirtschaftlichen Zukunft des bisherigen Zulieferers, zunehmende Inhomogenität der Infrastruktur aufgrund von M&A. Die Liste ließe sich beliebig fortsetzen. Doch das Ziel ist immer dasselbe: wir wollen morgen noch telefonieren und den Betrieb der Infrastruktur bewältigen können. Bei näherer Beschäftigung mit dem Thema wird sofort klar, dass mit Voice-over-IP aus der Telefonie ein Dienst wird, der sich in die bestehende IT-Landschaft integrieren muss. Und dass vielmehr bedacht werden muss, als nur die Telefonie.

weiter auf Seite 30

Geleit

Intel greift an: ist der RISC-Markt am Ende?

ab Seite 2

Standpunkt

Zertifikatsinsuffizienz: Wenn Informationssicherheit zu kompliziert wird

auf Seite 24

Sonderaktion im Oktober

Wireless-Spezial

auf Seite 13

Aktuelles Intensiv-Seminar

Winterschule 2012

ab Seite 26

Zum Geleit

Intel greift an: ist der RISC-Markt am Ende?

Die letzten Quartalszahlen belegen weitere Marktgewinne für x86-Server, der Anteil der verkauften RISC-Systeme geht mehr und mehr zurück. Stehen HP, IBM und Oracle mit dem Rücken an der Wand und ist es nur noch eine Frage der Zeit, bis sie mit ihren RISC-Systemen aufgeben müssen?

Zur Beantwortung dieser Frage dreht sich alles um Verfügbarkeit und weniger um Leistung. 99,999% und bessere Verfügbarkeiten sind nur noch mit Hardware-Automatisierung in der Reaktion auf Störungen zu erreichen. Damit müssen alle Systemkomponenten wie CPU, DIMMs, Bussysteme, Buskarten und die gesamte I/O redundant ausgelegt sein und es muss Mechanismen für die Erkennung von Fehlern und die Ab- und Umschaltung von Komponenten geben. Für menschliche Interaktion bleibt keine Zeit, lediglich Hot-Swap-Eigenschafen für DIMMs und Buskarten zur Vermeidung einer Server-Abschaltung spielen noch eine Rolle in Bezug auf den menschlichen Eingriff.

Mit dem E7 hat Intel im letzten Jahr eine Server-CPU auf den Markt gebracht, die viele RAS-Eigenschaften (RAS= Reliability, Availability, Serviceability) des Itaniums übernommen hat. Intel greift damit direkt die etablierten RISC-Systeme an. Hardware-Redundanz mit Um-/Abschaltung defekter Busse, CPUs und DIMMs sind damit auch in den E7 x86-Servern vorhanden. Im Jahr 2013 wartet die Branche auf den großen Wurf durch Intel. Bisher hat Intel keine Server-CPU im 22nm-Prozess auf den Markt gebracht. Dafür soll 2013 der große Sprung eventuell sogar mit einer neuen Microarchitektur kommen. 3Gate-Transistoren werden aller Voraussicht nach eine neue Messlatte für den Stromverbrauch von Top-Servern setzen. Gleichzeitig wird die Frage diskutiert, was Intel mit den vielen zusätzlichen Transistoren des 22nm-Prozesses machen wird. Als sicher gilt eine Integration des PCI-Express in den CPU-Chip so wie es in der aktuellen 22nm-Desktop-CPU schon erfolgt ist. Aber geht Intel noch weiter? Denkbar wären vier anstelle von zwei Threads pro Core. Das würde die Lücke zu Oracle/Sun etwas schließen und eine bessere Eignung für hochparallele Anwendungen schaffen. Oder ist sogar die Zeit der Ablösung des PCI-Express gekommen? Seit längerer Zeit wird über eine neue I/O-Konstruktion mit einer Integration eines Netzwerk-Adapters und Switches in die CPU spekuliert. Das Problem dieses Konzepts ist, dass es

nicht wirklich rund ist. Es erfordert einen Systemhersteller, der daraus eine sinnvolle Gesamtarchitektur macht. Aber vielleicht müssen wir darauf noch zwei oder drei Server-Generationen warten. Immerhin haben PCI-Express 3.0 und die zukünftige 4.0 Variante eine erhebliche Leistung mit sehr viel Flexibilität. Der Hauptnachteil ist, dass PCI-Express immer eine lokale Bustechnologie ist. Will man den Systembus weiter ausdehnen, um deutlich mehr CPUs oder weitere Peripherie zu integrieren, dann wäre der Wechsel auf eine neue Technologie angesagt.

Also wird 2013 das Ende des RISC-Marktes einläuten? Die Antwort ist aus meiner Sicht ein klares Jein. Für Anwendungen wie Cloud-Computing reichen x86-Server mit Virtualisierung, Life Migration zwischen Servern und High Availability aus. Hier findet die Redundanz auf Server-Ebene statt und für die meisten Fälle ist das ausreichend. Es gibt also begründeten Anlass, diesen Markt für RISC-Lösungen als verloren anzusehen. Vermutlich wird hier das Thema Performance/Watt, das mit den 22nm-CPUs noch einmal an Marktbedeutung gewinnen wird, einen weiteren Schub in Richtung x86-Server geben.

Für komplexere Datenbank- oder High Performance Computing-Anwendungen reicht das allerdings nicht aus. Intel hat gegenüber der RISC-Konkurrenz einen wesentlichen Nachteil: Hardware, Virtualisierung und Betriebssystem kommen von verschiedenen Herstellern. Eine Machine Check Architecture wie sie der E7 einführt ist ohne eine direkte Unterstützung dieser Eigenschaften im Betriebssystem oder auch der Applikation nutzlos. Abschaltung und Umschaltung von Hardware-Komponenten geht ohne Integration des Betriebssystems und der Anwendungen nicht. Die Serverhardware muss die Alarme und Schaltmechanismen zur Verfügung stellen. Aber die Hardware kann nicht entscheiden, ob und in wie weit ein Komponentenausfall eine Applikation gestört hat und ob ein Zurückgehen auf den letzten Snapshot erforderlich ist. Auch eine Veränderung der Bus- oder I/O-Architektur zu einer weiteren Verbesserung der Systemhardware müsste durch die Betriebssystemhersteller mitgetragen werden. Während der Linux-Markt in sich relativ flexibel ist, muss man bei der

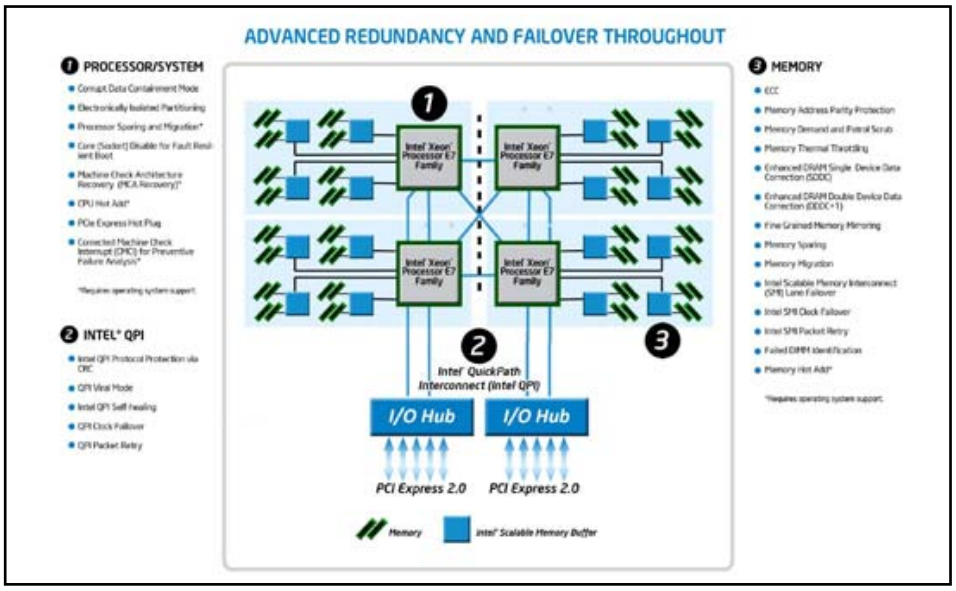


Abbildung 1: Intel E7-RAS-Eigenschaften Quelle Intel

Schwerpunktthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Die ASIC-Technik brachte jedoch auch Nachteile: reduzierte Funktionalität, verlängerte Produktionszyklen, fehlende Änderbarkeit; die Control Plane von Netzwerk-Komponenten, Firmware und auch Software, insbesondere Switches und Routern, ist nun seit vielen Jahren proprietär, gegen einen Zugriff des Betreibers abgeschottet und verbleibt unter der Kontroll-Hoheit der Hersteller. So entstanden Netzwerke mit vertikal integrierter Funktionalität, in denen für jeden Switch dezentral eine umfängliche Konfiguration eingerichtet und aufrecht erhalten bleiben muss. (siehe Abbildung 1.1)

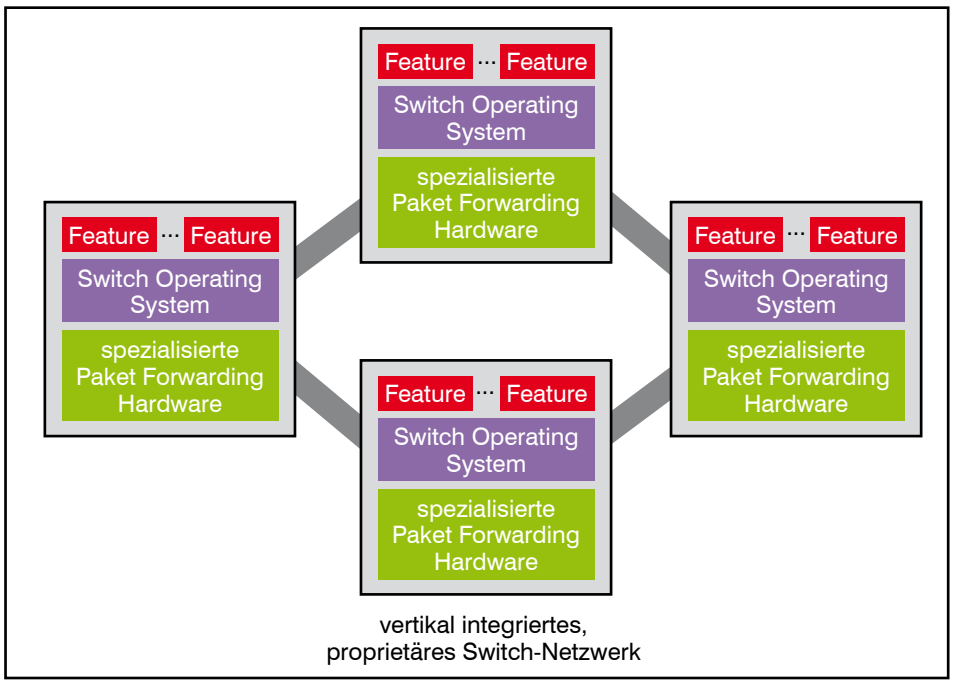


Abbildung 1.1: Vertikale integrierte, proprietäre Switch-Architektur

IP-Prinzip: IP-basierte Netzwerke wurden auf dem Architektur-Prinzip von Autonomen Systemen (AS) gebildet. Dies bedeutet Skalierbarkeit und geografische Ausdehnung durch eine Verbindungslogik, bei der Pakete zu einem Next Hop weitergeleitet werden, der auf der Basis beschränkter Informationen eine vernünftige Zwischenetappe auf dem Weg zum Ziel darstellt. Die zu verwaltenden Informationen sind nach diesem Prinzip auf ein Minimum beschränkt, das mit beschränkten Speichermitteln den Aufbau weltweiter Netze erlaubte. Das IP und AS Prinzip hat aber einen bekannten Nachteil: Die Identität ist immer mit der Topologie verknüpft, ein System kann nicht beliebig von A nach B wandern, ohne die Identität im Sinne der Netzwerk-Adresse zu ändern. Über viele Jahre hinweg wurde versucht, diesen Nachteil mit VPN- und VLAN-Technik zu umgehen. Beides reicht jedoch nicht aus, um die Migrations-Bedarfe virtueller Maschinen in heutigen Data Center Strukturen handhaben zu können.

Robustheit vs. Flexibilität: Während viele Jahre lang der Fokus bei Netzdesigns auf der Robustheit und Fehlervermeidung lag, treten jetzt Anforderungen in den Vordergrund, dynamische Zustandsinformationen an realen oder virtuellen Switchports zu handhaben und spezifische Verkehrslasten flexibel steuern zu können. Videoanwendungen beispielsweise lassen sich bei Überlast durch Drops oder Drosselung der Eingangsrate auffangen, Finanztransaktionen oder Patientenüberwachung nehmen jeden Paketverlust äußerst übel. Hierauf könnten moderne Netze so reagieren, dass sie unterschiedliche Anwendungen über unterschiedliche Wege transportieren. Anforderungen an eine dynamisch angepasste Paketweiterleitung und Wegwahl treten insbesondere im Zusammenhang mit hochdynamischen Verkehrslasten zwischen virtuellen Servern, "Ost-West-Verkehr", Data Center-Flexibilisierung und Cloud Diensten auf. Für solche dynamischen Verkehrslasten ist das klassische dezentrale Hop-by-Hop IP Routing Paradigma jedoch nicht wirklich gut geeignet.

Komplexität vs. Flexibilität: Die aktuelle Netzwerk-Technologie besteht aus mehreren voneinander unabhängigen, standardisierten Layer-2 und Layer-3 Protokollen wie STP, LACP, OSPF, VRRP, BGP, IEEE 802.1X, IPsec etc., die Endsysteme zuverlässig und sicher über beliebige Distanzen, Linkgeschwindigkeiten und Topologien miteinander verbinden. Diese Protokolle arbeiten ohne gegenseitige automatische protokoll-übergreifende Konsistenzprüfung, daher liegt es in der Verantwortung des Netzwerk-Administrators, die Parameter der verschiedenen Protokolle aufeinander abzustimmen. Hinzufü-

gen oder Ändern einzelner Geräte oder Gerätegruppen führt zu Konfigurations-Änderungen in allen Switches, Routern, Firewalls, Web Authentisierungs-Portalen etc., da ACLs, VLANs, QoS Regeln usw. auf Element-Manager-Basis für jede Netzkomponenten-Gruppe geändert werden müssen. Diese mehr oder weniger statische Natur von Netzwerken wird der dynamischen Natur heutiger Server-Umgebungen nicht mehr gerecht, in der einzelne Applikationen über mehrere VMs auf mehrere Hosts verteilt sind und (in großen Cloud Rechenzentren) VMs dynamisch nach Bedarf bereitgestellt oder deaktiviert werden.

Konsistenz und dynamische Skalierbarkeit: Die Konfiguration einer netzweiten Policy erfordert es gegebenenfalls, Hunderte bis Tausende Netzkomponenten anzufassen und z.B. ihre ACL-Konfiguration anzupassen. Dies kann Stunden bis Tage dauern und birgt bei aller Sorgfalt bei großen Netzen ein erhöhtes Risiko für Konfigurations-Inkonsistenzen, da ja keine komponentenübergreifende Konsistenzprüfung gegeben ist. Das heißt, mit traditioneller Netzwerktechnik können Netze einerseits nicht schnell genug erweitert werden, andererseits wächst die Komplexität tausender separat konfigurierter Netzkomponenten so stark an, dass sie kaum noch beherrschbar ist.

Deterministik vs. Dynamik: Die aktuellen Netzwerk-Verfahren sind auf Verkehrsmuster ausgelegt, die sich vergleichsweise langsam ändern, so dass notwendige Erweiterungen, ggf. unterstützt von Trendberechnungen, im Bedarfsfall manuell durchgeführt werden können. In großen Rechenzentren können die Verkehrsmuster jedoch so dynamisch und über so viele VMs verteilt sein, dass eine Vorhersage und Trendberechnung nicht mehr möglich ist. Large-Scale Parallelprozesse und die zugehörigen Datenbanken sind teilweise über einen kompletten Serverpool verteilt, mit steigender Anzahl Endnutzer-Applikationen (ein Beispiel: Durchsuchen und Indizierung des gesamten Webs und sofortige Rückgabe eines Suchergebnisses zum Endnutzer) steigt das Datenvolumen zwischen vernetzten Knoten auf PetaBytes. Solche Netzwerke müssen Hunderttausende bis Millionen Server verbinden, und dies kann eine manuelle Provisionierung und Konfiguration nicht mehr leisten.

VLAN-Grenzen und Mandantenkonzepte: In großen Umgebungen, insbesondere auch bei Mandantenkonzepten, reicht der VLAN-Nummernbereich von 4096 VLANs nicht mehr aus. Wächst ein Mandant so stark, dass er nicht mehr in ein IP Subnetz hineinpasst oder gibt es überlappende IP/VLAN Adressbereiche, so müssen komplexe Mandanten-Techniken wie VRF, NAT, MPLS oder andere Overlay-Netze greifen. Um ein Vielfaches der 4000 VLANs zu betreiben, sind Overlay-Technologien wie VXLAN, NVGRE, MPLS, LISP notwendig. Mit steigender Anzahl Mandanten und VLANs und Overlay-Technologien ergibt sich wiederum der Bedarf nach zentraler, konsistenter Konfiguration und gegebenenfalls zentral gesteuerter dynamischer Anpassung.

Virtuelle Switches: Mit steigender Anzahl virtueller Maschinen auf Hostsystemen steigt auch die Anzahl eingesetzter virtueller Switches (vSwitches). Vielfach werden diese nicht oder nicht ausschließlich vom Netzwerk-Administrator, sondern vom Server-Administrator gehandhabt. Etablierte Switch-Hersteller haben als Antwort darauf eigene Management-Erweiterungen entwickelt, um die Migration von VMs und das Management von vSwitches netzwerkseitig zugreifbar oder einsehbar zu machen. Hier wäre ein deutlicher Fortschritt erreicht, wenn alle vSwitches erstens eine einheitliche Funktionalität hätten (z.B. Open vSwitch) und zweitens mit einem gemeinsamen, vom Server-Management losgelösten Management-Tool provisioniert, administriert und überwacht werden könnten.

Bei all diesen Problemfeldern kommen Software-Defined Networking (SDN) und OpenFlow ins Spiel: Sie wollen die Netzsteuerung auf einen zentralen Controller auslagern und damit vollständig flexibilisieren und dynamisieren.

1.2 Wie hängen ONF, SDN und OpenFlow zusammen?

ONF

Anfang 2011 gründeten die Deutsche Telekom, Facebook, Google, Microsoft, Verizon und Yahoo die Open Networking Foundation als non-Profit Konsortium mit dem Ziel, Software Defined Networking (SDN) nach vorne zu treiben und für die Netzwerk-Technologie im Markt durchzusetzen. Die Standardisierung einer eigenen Netzwerk-Architektur, die Netze weltweit programmierbar macht, soll die Umsetzung von SDN ermöglichen. Später erfolgte der Beitritt von Broadcom, Brocade, Ciena, Cisco, Citrix, Dell, Ericsson, Force10, HP, IBM, Juniper, Marvell, Microsoft, NEC, Netgear, NTT, Oracle, Riverbed Technology und VMware. Aktuell hat die ONF mehr als 70 Mitglieder aus verschiedenen marktrelevanten Technologiebereichen: Provider, Netzwerk-Komponenten-Hersteller, Chip-Hersteller, Software- und System-Hersteller. (siehe Abbildung 1.2)

Eines der Ziele von ONF ist es, OpenFlow zu standardisieren. Hierfür hat sie technische Arbeitsgruppen ins Leben gerufen, die sich um das Protokoll, die Konfiguration und Multivendor Interoperabilitätstests kümmern.

SDN

Begeben wir uns noch einmal zurück in die 70er und 80er Jahre: Damals war ein Router ein Server (typischerweise Unix), der Datenpakete zwischen zwei oder mehreren Netzwerk-Schnittstellen weiterleitete, z.B. X.25… Heute haben wir skalierbare Mehrkern-Prozessoren und handelsübliche Netzwerkprozessoren, die immer mehr Funktionsmöglichkeiten bieten, Programmierwerkzeuge sind weltweit verfügbar. Warum also nicht Software-Entwicklung für Netzwerke etablieren? Was spricht dagegen, in jedem Rechner einen oder mehrere eigene Prozessoren für Netzwerk-Aufgaben abzustellen?

Hier kommt nun Software Defined Networking ins Spiel. SDN ist eine aufkommen-

Abbildung 1.2: Gründungs-Mitglieder der ONF

Zweitthema

UCC gehört ins Internet!

Fortsetzung von Seite 1

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich bereits auf moderne Kommunikationsnetze und Betriebssysteme. Zu seinen Spezialgebieten gehören jetzt u.a. die Konzeption und Ausschreibung professioneller Unified-Communications- und Kollaborations-Systeme sowie Microsoft-Lösungen.

Bald drehen sich die Überlegungen um viele verschiedene Kommunikationskanäle, ihre Integration in das Arbeitsumfeld der Anwender und die hieraus zu generierenden Mehrwerte. Das TK-Projekt wird zum UCC-Projekt. Aus Infrastruktur-Überlegungen werden Prozessbetrachtungen.

Denn Unified Communications & Collaboration hat sich längst von einem Thema der Infrastrukturkonvergenz zu einer Plattform für Anwender und Geschäftsprozesse fortentwickelt: die Rede ist heute von Communications Enabled Business Processes oder eben User-centric Communications. User-centric Communications verspricht dabei:

- ungehinderte Kommunikation zwischen Mitarbeitern, Partnern, Zulieferern und Kunden,
- freie Wahl des Kommunikationskanals vor und während der Kommunikation,
- tiefe Integration in die Applikationswelt und somit die Geschäftsprozesse,
- bessere Erreichbarkeit aller Kommunikationsteilnehmer, sowie orts- und geräteunabhängige Kommunikation und Zusammenarbeit.

Doch was muss gewährleistet sein, damit diese Versprechen eingelöst werden können?

These 1: UCC kennt keine Unternehmensgrenzen

Will man effektiv Prozesse vereinfachen und beschleunigen, so müssen alle Teilnehmer am Prozess Zugriff auf die Plattform erhalten, die den Prozess technisch abbildet. Was das bedeutet, kann man sich anhand der Telefonie vergegenwärtigen: Niemand plant eine TK-Lösung, die nur die Telefonie von Mitarbeitern einer Abteilung untereinander ermöglicht. Die PBX stellt immer die Kommunikation zwischen allen Mitarbeitern eines Unternehmens her. Und ebenso soll das für UCC-Lösungen gelten. Alle Kommunikationsteilnehmer im Unternehmen sollen auf derselben UCC-Plattform aufsetzen. Nur so ist eine medienbruchfreie Kommunikation und Zusammenarbeit möglich.

Aber hier liegt bereits der erste Denkfehler: so wie man früher die PBX – Private Branch Exchange! – als internes Kommunikationssystem angesehen hat, betrachtet man UCC ebenfalls als unternehmensinterne Plattform. Doch das ist falsch. Die Telefonanlage war immer die Verlängerung des öffentlichen Telefonnetzes in das Unternehmen hinein. Der Grund: man benötigte eine Möglichkeit, hunderte und tausende von Kupferdoppeladern an das öffentliche Netz anzukoppeln. Natürlich ermöglichte die TK-Anlage auch gebührenfreie interne Kommunikation und bot zusätzliche Leistungsmerkmale – aber das kompensiert nur Defizite des öffentlichen Telefonnetzes. Im Kern war und ist die PBX der verlängerte Arm des öffentlichen Telefonnetzes – einer standardisierten, globalen Infrastruktur für Sprachkommunikation. Und ohne dieses öffentliche Telefonnetz wären viele Prozesse im Unternehmen undenkbar. Denn die Prozessbeteiligten sind in der absoluten Minderheit innerhalb des Unternehmens angesiedelt. Neben den Mitarbeitern sind Geschäftspartner, Zulieferer und – nicht zuletzt – Kunden involviert. Will man die Mehrwerte von UCC über die gesamte Prozesskette realisieren, muss der Zugriff ALLER auf UCC-Dienste möglich sein. Eine UCC-Lösung an das Telefonnetz zu koppeln ist nur eine unzureichende Krücke, die den Verlust von Leistungsmerkmalen bedeutet und die Dienstvielfalt von UCC auf Sprache beschränkt. Einzig ein weltweites, dienstneutrales Datennetz kann ein geeignetes Interconnect über die Unternehmensgrenzen hinweg bieten.

These 2: UCC lebt vom einfachen Zugriff

Damit UCC seine Wirkung entfalten kann, müssen die Kommunikationskanäle jedem Teilnehmer einfach zugänglich sein. Ein gutes Beispiel sind raumgebundene Videokonferenzlösungen. Die Auslastung vieler derartiger Systeme ist nahe Null. Die Problematik: gerade hochqualitative Systeme, wie z.B. Telepräsenz-Lösungen, werden für einen sehr exklusiven Nutzerkreis eingeführt, der schon aufgrund seiner geringen Teilnehmerzahl nicht für eine angemessene Auslastung der Systeme sorgen kann. Selbst wenn der Teilnehmerkreis nicht auf das Management beschränkt ist, sorgt die Verortung auf der sprichwörtlichen „Chef-Etage“ für Berührungsängste und mangelnde Akzeptanz. Zudem ist die Buchung entweder zu kompliziert oder ohne Zugriff auf das Unternehmensnetz nicht möglich. In dem Moment, wo Videokonferenzsysteme frei zugänglich in regulären Besprechungsräumen verbaut und über ein global zugängliches Buchungssystem von autorisierten Nutzern mit wenigen Klicks reserviert werden können, steigt die Auslastung sprunghaft an.

Doch auch hier sind rein unternehmensinterne Systeme wieder schlechter gestellt. Beschränkt sich die Interkonnektivität auf drei, zehn oder gar zwanzig Telepräsenzsysteme innerhalb des Unternehmens mangelt es oft an Anwendungsfällen für den durchschnittlichen Benutzer. Er muss überlegen, ob das Telepräsenzsystem wirklich das geeignete Kommunikationsmedium ist. Sobald ein externer Kommunikationspartner an Bord ist, kann das Telepräsenzsystem nicht genutzt werden. Das lässt viele Anwender direkt zu einer einfacheren Alternative greifen – zum Beispiel einem öffentlichen Webconferencing- oder Desktopvideo-Dienst. Ob das immer das optimale Kommunikati-

onsmedium ist, darf in Frage gestellt werden. Wie unter Punkt eins bereits diskutiert, braucht es also ein Datennetz, das die Systeme an Standorten in- und außerhalb des Unternehmens miteinander verbindet. Das gilt aber nicht nur für Medienstrom und Signalisierung. Will man einfache Nutzbarkeit erzielen, muss die Buchungsplattform auch externe Raumsysteme einbeziehen können. Das heißt, dass diese mit ihrer öffentlichen Adresse im Buchungssystem registriert oder bei Anfrage durch den Gesprächspartner im Buchungssystem hinterlegt werden können. Ein globales Adressverzeichnis und ein einfaches Adressformat unterstützen hierbei. Unabdingbar ist aber ein gemeinsames Kommunikationsnetz, das für den Austausch dieser Daten geeignet ist.

These 3: Perimeterschutz verhindert globale Kommunikationslösungen

Wir halten fest: UCC benötigt ein weltweites Netz, das für interne wie externe Teilnehmer zugänglich ist, und neben den diversen Medienströmen und der Signalisierung auch Dienste wie Adressbücher und Buchungssysteme miteinander koppeln kann. Innerhalb eines privaten Weitverkehrsnetzes ohne jegliche Sicherheitseinrichtungen ist das leicht vorstellbar. Wer allerdings einmal die Firewall-Regeln für den externen Zugriff auf eine UCC-Lösung konfigurieren musste, der weiß: sollen alle Dienste intern wie extern erreichbar sein, ist das ein kompliziertes Unterfangen, das im Ergebnis zu einer Firewall führt, die alle möglichen Arten von Traffic von und zu allen möglichen Zielen zulässt. Will man zumindest die zulässigen Quellen und Ziele einschränken, so steigt die Komplexität der Regelwerke linear zu deren Anzahl. Tut man dies nicht, wird der Gedanke des Perimeterschutzes ad absurdum geführt. Denn de facto öffnet man vielfältigste Einfalltore für Angreifer.

Angesichts dieser Problematik muss man sich die Frage stellen, was durch den Perimeterschutz erreicht werden soll. IT-Sicherheit hat im Kern zwei Ziele:

- Sicherung der Vertraulichkeit und Integrität von Informationen
- Sicherung der Verfügbarkeit von IT-Diensten

Zu beidem trägt ein effektiver Perimeterschutz wesentlich bei. Aber nur unter der Annahme, dass der Angreifer sich außerhalb des Firmennetzes befindet. Glaubt man diversen Studien zur IT-Sicherheit, so geht die größte Gefahr für die Integrität und Sicherheit der IT-Infrastruktur nicht von externen Angreifern aus, sondern von Innentätern. Von Racheakten frustrierter Mitarbeiter bis hin zur Wirtschaftsspionage – hat der Angreifer autorisierten Zugriff auf Netz und Systeme, nutzt der beste Perimeterschutz nichts. Versagen andere Sicherheitssysteme, wie z.B. der Malware-Schutz, so wird der externe Angreifer via Trojaner zum Innentäter. Und überhaupt: in Zeiten höchster Mobilität befindet sich ein großer Teil der Mitarbeiter schon längst nicht mehr „im“ Unternehmensnetz, sondern wird künstlich und mit hohem Aufwand via VPN in dieses zurückgeholt. Unter diesen Voraussetzungen den Perimeterschutz als Allheilmittel zu betrachten ist kurzsichtig.

Das bedeutet nicht, dass man seine lokalen Netze – oder gar Rechenzentren und produktionskritische Infrastrukturen – schutzlos preisgeben sollte. Die Sicherheit in Zeiten hochkomplexer IT-Systeme muss aber neu gedacht werden. Weg vom Perimeterschutz, hin zum Inhaltsschutz. Auf UCC-Dienste bezogen bedeutet das, dass die Verschlüsselung von Medienströmen und Signalisierung Pflicht sein muss. Andernfalls endet die Integrität der Kommunikation nicht erst beim Übergang in das öffentliche Telefonnetz, sondern schon im lokalen Netzwerk. Die Verfügbarkeit der Dienste darf nicht durch eine Trennung in inneres und äußeres Netz, sondern muss durch mehrfach redundante Auslegung der Systeme, geeignete Lastbalancierung und intelligente Angriffserkennung an Netzübergängen und Clients stattfinden. Was diese Mechanismen angeht, hinkt die Infrastruktur der meisten Unternehmen denen eines einfachen Webhosters hinterher. Und der Netzübergang wird allzu oft zum Single Point of Failure. Was aber nützt hochverfügbare interne Kommunikation, wenn die externe Kommunikation – und damit der Geschäftsprozess – unterbrochen ist? Wie der renommierte Sicherheitsexperte Dan Kaminsky einmal treffend bemerkte, ist Mehrwert das, was in Abwesenheit eines Angreifers erzielt werden kann. Den Mehrwert von UCC einem althergebrachten Sicherheitsverständnis von „drinnen und draußen“ zu opfern ist mit Sicherheit falsch. Und was unterscheidet – geeignete Sicherheitsmechanismen vorausgesetzt – noch das „innere“ vom „äußeren“ Netz, dem Internet?

These 4: UCC braucht öffentlich zugängliche, standardisierte Plattformen

Mit dem Internet steht die größte, standardbasierte Routingplattform aller Zeiten zur Verfügung. Mit den Bordmitteln des Internet ist es problemlos möglich, Punkt-zu-Punkt-Beziehungen zwischen Unternehmenslösungen für Unified Communications aufzubauen. Jedoch mangelt es an der Möglichkeit, solche „Föderationen“ für alle Kommunikationsmedien gleichermaßen aufzubauen. Auch sind diese Föderationen in den vielen Fällen auf Systeme desselben Herstellers begrenzt. Das gewichtigste Argument gegen Föderationen ist aber, dass man aus zwei Insellösungen nur eine neue, größere Insellösung schafft. Man kann durchaus alle Unternehmenslösungen, mit denen man Kommunikationsbeziehungen pflegt, via Föderation ankoppeln. Doch der administrative Aufwand für das einzelne Unternehmen steigt linear mit der Anzahl der Föderationspartner. Und alle anderen bleiben

Kongress

ComConsult TK-, UC- und Videokonferenzforum 2012
19.11. - 22.11.12 in Düsseldorf

Dieses hochaktuelle Forum analysiert aktuelle Trends, neue Technologien und Produkt-/Hersteller-Strategien im Bereich TK, UC und Videokonferenztechnik. Die Kernthemen sind: wie viel UC braucht TK; zukunftsweisende Client-Strategien; User Centric Communications; der Kunde, das unbekannte UC-Wesen; Videokonferenztechnik der Zukunft.

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Dominik Zöller

Kosten:	4-tägige Veranstaltung inkl. Intensiv-Tag	€ 2.490,-- netto
	3-tägige Veranstaltung ohne Intensiv-Tag	€ 2.090,-- netto
	Nur Intensiv-Tag	€ 990,-- netto

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